



Documentación del SnapCenter software

SnapCenter software

NetApp
September 29, 2025

This PDF was generated from <https://docs.netapp.com/es-es/snapcenter-61/index.html> on September 29, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación del SnapCenter software	1
Notas de la versión	2
Notas de la versión	2
Rutas de actualización compatibles con SnapCenter	2
Empezar	3
Obtenga más información sobre el SnapCenter software	3
Descripción general de SnapCenter	3
Funciones de seguridad en SnapCenter	8
Control de acceso basado en roles en SnapCenter	9
Recuperación ante desastres en SnapCenter	14
Licencias requeridas por SnapCenter	15
Sincronización activa de SnapMirror en SnapCenter	18
Conceptos clave de la protección de datos	19
Sistemas de almacenamiento y aplicaciones compatibles con SnapCenter	21
Métodos de autenticación para las credenciales de SnapCenter	21
Operaciones de SnapCenter compatibles con sistemas ASA r2	23
Inicio rápido del SnapCenter software	24
Instalar y configurar SnapCenter Server	26
Prepárese para instalar el servidor SnapCenter	26
Requisitos para instalar SnapCenter Server	26
Regístrese para acceder al SnapCenter software	33
Autenticación multifactor (MFA)	34
Instalar el servidor SnapCenter	44
Instalar el servidor SnapCenter en el host de Windows	44
Instalar el servidor SnapCenter en el host Linux	48
Registrarse en SnapCenter	52
Inicie sesión en SnapCenter mediante la autorización RBAC	52
Configurar el servidor SnapCenter	56
Agregar y aprovisionar el sistema de almacenamiento	56
Agregar licencias basadas en controlador de SnapCenter Standard	77
Configurar alta disponibilidad	82
Configurar el control de acceso basado en roles (RBAC)	86
Configurar los ajustes del registro de auditoría	115
Configurar conexiones MySQL seguras con SnapCenter Server	116
Configurar la autenticación basada en certificados	122
Habilitar la autenticación basada en certificados	122
Exportar certificados de autoridad de certificación (CA) desde SnapCenter Server	123
Importar certificado de CA a los hosts del complemento de Windows	123
Importar certificado CA a los hosts del complemento UNIX	124
Exportar certificados de SnapCenter	126
Configurar el certificado CA para el host de Windows	126
Generar archivo CSR de certificado de CA	126
Importar certificados de CA	127

Obtenga la huella digital del certificado CA	128
Configurar el certificado de CA con los servicios del complemento de host de Windows	128
Configurar el certificado de CA con el sitio de SnapCenter	129
Habilitar certificados CA para SnapCenter	130
Configurar el certificado CA para el host Linux	130
Configurar el certificado nginx	130
Configurar el certificado de registro de auditoría	131
Configurar el certificado de servicios de SnapCenter	131
Configurar y habilitar la comunicación SSL bidireccional en el host de Windows	132
Configurar la comunicación SSL bidireccional en el host de Windows	132
Habilitar la comunicación SSL bidireccional en el host de Windows	134
Configurar y habilitar la comunicación SSL bidireccional en el host Linux	136
Configurar la comunicación SSL bidireccional en el host Linux	136
Habilitar la comunicación SSL en el host Linux	137
Configurar Active Directory, LDAP y LDAPS	138
Registrar dominios de Active Directory que no sean de confianza	138
Configurar los grupos de aplicaciones de IIS para habilitar los permisos de lectura de Active Directory	139
Configurar el certificado de cliente de CA para LDAPS	140
Proteger las bases de datos de Microsoft SQL Server	141
Complemento de SnapCenter para Microsoft SQL Server	141
Descripción general del complemento de SnapCenter para Microsoft SQL Server	141
Qué puede hacer con el complemento SnapCenter para Microsoft SQL Server	141
Funciones del complemento SnapCenter para Microsoft SQL Server	142
Compatibilidad con la asignación asimétrica de LUN en clústeres de Windows	143
Tipos de almacenamiento compatibles con el complemento SnapCenter para Microsoft SQL Server	144
Recomendaciones de diseño de almacenamiento para el complemento SnapCenter para Microsoft SQL Server	147
Privilegios mínimos de ONTAP necesarios para el complemento SQL	149
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el complemento para SQL Server	151
Estrategia de respaldo para recursos de SQL Server	152
Estrategia de restauración para SQL Server	157
Definir una estrategia de clonación para SQL Server	160
Prepárese para instalar el complemento de SnapCenter para Microsoft SQL Server	161
Flujo de trabajo de instalación del complemento SnapCenter para Microsoft SQL Server	161
Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para Microsoft SQL Server	162
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	163
Configurar credenciales para el paquete de complementos de SnapCenter para Windows	164
Configurar credenciales para un recurso individual de SQL Server	166
Configurar gMSA en Windows Server 2016 o posterior	168
Instalar el complemento de SnapCenter para Microsoft SQL Server	169
Configurar el certificado de CA	175
Configurar la recuperación ante desastres	179
Instalar el SnapCenter Plug-in for VMware vSphere	181

Implementar certificado de CA	181
Configurar el archivo CRL	181
Prepárese para la protección de datos	181
Requisitos previos para utilizar el complemento de SnapCenter para Microsoft SQL Server	181
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger SQL Server	182
Realizar una copia de seguridad de la base de datos, instancia o grupo de disponibilidad de SQL Server	183
Flujo de trabajo de respaldo	183
Determinar si hay recursos disponibles para realizar copias de seguridad	185
Migrar recursos al sistema de almacenamiento NetApp	186
Crear políticas de respaldo para bases de datos de SQL Server	188
Crear grupos de recursos y adjuntar políticas para SQL Server	195
Cree grupos de recursos y habilite la protección secundaria para los recursos de Microsoft SQL Server en sistemas ASA r2	198
Requisitos para realizar copias de seguridad de recursos SQL	200
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell	201
Realizar copias de seguridad de los recursos de SQL	202
Realizar copias de seguridad de grupos de recursos de SQL Server	207
Supervisar las operaciones de copia de seguridad de recursos de SQL en la página Trabajos de SnapCenter	208
Cancelar las operaciones de copia de seguridad del complemento SnapCenter para Microsoft SQL Server	209
Ver copias de seguridad y clones de SQL Server en la página Topología	210
Limpiar el recuento de copias de seguridad secundarias mediante cmdlets de PowerShell	212
Restaurar recursos de SQL Server	213
Restaurar flujo de trabajo	213
Requisitos para restaurar una base de datos	213
Restaurar copias de seguridad de bases de datos de SQL Server	214
Restaurar una base de datos de SQL Server desde un almacenamiento secundario	221
Restaurar recursos mediante cmdlets de PowerShell	222
Resembrar bases de datos del grupo de disponibilidad	225
Supervisar las operaciones de restauración de recursos SQL	226
Cancelar operaciones de restauración de recursos SQL	227
Clonar recursos de base de datos de SQL Server	227
Flujo de trabajo de clonación	228
Clonar desde una copia de seguridad de la base de datos de SQL Server	228
Realizar ciclo de vida de clonación	236
Supervisar operaciones de clonación de bases de datos SQL	239
Cancelar operaciones de clonación de recursos SQL	239
Dividir un clon	240
Proteger las bases de datos de SAP HANA	242
Complemento de SnapCenter para bases de datos SAP HANA	242
Descripción general del complemento de SnapCenter para la base de datos SAP HANA	242
Qué puede hacer utilizando el complemento SnapCenter para la base de datos SAP HANA	242
Funciones del complemento SnapCenter para la base de datos SAP HANA	243
Tipos de almacenamiento compatibles con el complemento de SnapCenter para la base de datos	

SAP HANA	243
Privilegios mínimos de ONTAP necesarios para el complemento SAP HANA	244
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para bases de datos SAP HANA	247
Estrategia de respaldo para bases de datos de SAP HANA	247
Estrategia de restauración y recuperación para bases de datos de SAP HANA	251
Prepárese para instalar el complemento de SnapCenter para la base de datos SAP HANA	253
Flujo de trabajo de instalación del complemento de SnapCenter para la base de datos SAP HANA ..	253
Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para la base de datos SAP HANA	254
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	257
Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux	258
Configurar credenciales para el complemento de SnapCenter para la base de datos SAP HANA	259
Configurar gMSA en Windows Server 2016 o posterior	262
Instalar el complemento de SnapCenter para bases de datos SAP HANA	263
Configurar el certificado de CA	269
Instalar el SnapCenter Plug-in for VMware vSphere	277
Implementar certificado de CA	277
Configurar el archivo CRL	277
Prepárese para la protección de datos	277
Requisitos previos para utilizar el complemento de SnapCenter para la base de datos SAP HANA ..	278
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger las bases de datos de SAP HANA	278
Realizar copias de seguridad de los recursos de SAP HANA	279
Realizar copias de seguridad de los recursos de SAP HANA	279
Configurar la clave de almacenamiento de usuarios de 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 multiinquilino para la protección de datos	281
Agregar recursos manualmente al host del complemento	284
Crear políticas de respaldo para bases de datos de SAP HANA	286
Crear grupos de recursos y adjuntar políticas	292
Cree grupos de recursos y habilite la protección secundaria para los recursos de SAP HANA en sistemas ASA r2	296
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos de SAP HANA	299
Realizar copias de seguridad de las bases de datos de SAP HANA	300
Realizar copias de seguridad de grupos de recursos	308
Supervisar las operaciones de copia de seguridad de las bases de datos de SAP HANA	308
Cancelar operaciones de copia de seguridad para SAP HANA	310
Ver copias de seguridad y clones de bases de datos de SAP HANA en la página Topología	310
Restaurar bases de datos de SAP HANA	312
Restaurar flujo de trabajo	312
Restaurar y recuperar una copia de seguridad de un recurso agregado manualmente	313
Restaurar y recuperar una copia de seguridad de una base de datos descubierta automáticamente ..	317

Restaurar recursos mediante cmdlets de PowerShell	322
Supervisar las operaciones de restauración de bases de datos de SAP HANA	324
Clonar copias de seguridad de recursos de SAP HANA	325
Flujo de trabajo de clonación	325
Clonar una copia de seguridad de la base de datos de SAP HANA	326
Supervisar las operaciones de clonación de bases de datos de SAP HANA	330
Dividir un clon.	330
Eliminar o dividir clones de bases de datos de SAP HANA después de actualizar SnapCenter	332
Proteger las bases de datos de Oracle	333
Descripción general del complemento SnapCenter para Oracle Database	333
¿Qué puede hacer con el complemento para Oracle Database?	333
Características del complemento para Oracle Database	333
Tipos de almacenamiento admitidos por el complemento para Oracle Database	335
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el complemento de Oracle	337
Privilegios mínimos de ONTAP necesarios para el complemento de Oracle	337
Instalar el complemento de SnapCenter para la base de datos Oracle	340
Flujo de trabajo de instalación del complemento SnapCenter para Oracle Database	340
Requisitos previos para agregar hosts e instalar el paquete de complementos para Linux o AIX	340
Agregue hosts e instale el paquete de complementos para Linux o AIX mediante GUI	350
Formas alternativas de instalar el paquete de complementos para Linux o AIX	354
Configurar el servicio de Loader de complementos de SnapCenter	357
Configurar el certificado de CA con el servicio SnapCenter Plug-in Loader (SPL) en el host Linux	360
Habilitar certificados CA para complementos	363
Importar datos de SnapManager para Oracle y SnapManager para SAP a SnapCenter	364
Instalar el SnapCenter Plug-in for VMware vSphere	370
Implementar certificado de CA.	370
Configurar el archivo CRL	370
Prepárese para proteger las bases de datos de Oracle	370
Realizar copias de seguridad de bases de datos de Oracle	372
Descripción general del procedimiento de copia de seguridad	372
Información de configuración de la copia de seguridad.	373
Requisitos para realizar una copia de seguridad de una base de datos Oracle	385
Descubra las bases de datos Oracle disponibles para realizar copias de seguridad	386
Crear políticas de respaldo para bases de datos de Oracle	388
Crear grupos de recursos y adjuntar políticas para bases de datos de Oracle	395
Cree grupos de recursos y habilite la protección secundaria para los recursos de Oracle en sistemas ASA r2	397
Realizar copias de seguridad de los recursos de Oracle	400
Realizar copias de seguridad de los grupos de recursos de bases de datos de Oracle	403
Supervisar la copia de seguridad de la base de datos Oracle	404
Otras operaciones de respaldo	405
Montar y desmontar copias de seguridad de bases de datos	409
Montar una copia de seguridad de la base de datos	410
Desmontar una copia de seguridad de la base de datos	411

Restaurar y recuperar bases de datos Oracle	411
Restaurar flujo de trabajo	411
Definir una estrategia de restauración y recuperación para bases de datos Oracle	412
Variables de entorno predefinidas para restaurar prescript y postscript específicos	417
Requisitos para restaurar una base de datos Oracle	418
Restaurar y recuperar la base de datos Oracle	419
Restaurar y recuperar espacios de tabla mediante la recuperación en un punto en el tiempo	425
Restaurar y recuperar bases de datos conectables mediante recuperación en un punto determinado del tiempo	426
Restaurar y recuperar bases de datos Oracle mediante comandos UNIX	429
Supervisar las operaciones de restauración de la base de datos Oracle	429
Cancelar operaciones de restauración de bases de datos de Oracle	430
Clonar base de datos Oracle	431
Flujo de trabajo de clonación	431
Definir una estrategia de clonación para bases de datos Oracle	432
Variables de entorno predefinidas para prescript y postscript específicos de clones	433
Requisitos para clonar una base de datos Oracle	434
Clonar una copia de seguridad de una base de datos Oracle	436
Clonar una base de datos conectable	446
Clonar copias de seguridad de bases de datos de Oracle mediante comandos UNIX	451
Dividir un clon de base de datos Oracle	452
Clon dividido de una base de datos conectable	453
Supervisar las operaciones de clonación de bases de datos de Oracle	453
Actualizar un clon	454
Eliminar el clon de una base de datos conectable	455
Administrar volúmenes de aplicaciones	456
¿Qué son los volúmenes de aplicación?	456
Agregar volúmenes de aplicaciones	456
Volúmenes de aplicaciones de respaldo	457
Copia de seguridad del volumen de la aplicación clonada	460
Proteger los sistemas de archivos de Windows	462
Conceptos del complemento SnapCenter para Microsoft Windows	462
Descripción general del complemento SnapCenter para Microsoft Windows	462
Qué puede hacer con el complemento SnapCenter para Microsoft Windows	462
Características del complemento SnapCenter para Windows	463
Cómo SnapCenter realiza copias de seguridad de los sistemas de archivos de Windows	464
Tipos de almacenamiento compatibles con el complemento SnapCenter para Microsoft Windows	464
Privilegios mínimos de ONTAP necesarios para el complemento de Windows	467
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault	469
Definir una estrategia de respaldo para los sistemas de archivos de Windows	470
Orígenes y destinos de clones para sistemas de archivos de Windows	472
Instalar el complemento SnapCenter para Microsoft Windows	472
Flujo de trabajo de instalación del complemento SnapCenter para Microsoft Windows	472
Requisitos de instalación del complemento SnapCenter para Microsoft Windows	473
Agregar hosts e instalar el complemento SnapCenter para Microsoft Windows	477

Instalar el complemento SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell.	481
Instale el complemento SnapCenter para Microsoft Windows de forma silenciosa desde la línea de comandos.	481
Supervisar el estado de instalación del paquete de complementos de SnapCenter.	483
Configurar el certificado de CA	484
Instalar el SnapCenter Plug-in for VMware vSphere	487
Implementar certificado de CA.	487
Configurar el archivo CRL	487
Realizar copias de seguridad de los sistemas de archivos de Windows.	487
Realizar copias de seguridad de los sistemas de archivos de Windows.	487
Determinar la disponibilidad de recursos para los sistemas de archivos de Windows	489
Crear políticas de respaldo para sistemas de archivos de Windows.	490
Crear grupos de recursos para sistemas de archivos de Windows.	493
Cree grupos de recursos y habilite la protección secundaria para los sistemas de archivos de Windows en sistemas ASA r2	496
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell	498
Realice una copia de seguridad de un único recurso a pedido para los sistemas de archivos de Windows.	499
Realizar copias de seguridad de grupos de recursos para sistemas de archivos de Windows	504
Supervisar las operaciones de copia de seguridad	505
Cancelar operaciones de copia de seguridad	507
Ver copias de seguridad y clones relacionados en la página Topología	507
Limpiar el recuento de copias de seguridad secundarias mediante cmdlets de PowerShell	510
Restaurar sistemas de archivos de Windows	511
Restaurar copias de seguridad del sistema de archivos de Windows.	511
Restaurar recursos mediante cmdlets de PowerShell.	515
Supervisar las operaciones de restauración	518
Cancelar operaciones de restauración	519
Clonar sistemas de archivos de Windows	520
Clonar desde una copia de seguridad del sistema de archivos de Windows	520
Supervisar las operaciones de clonación	526
Cancelar operaciones de clonación.	527
Dividir un clon.	528
Proteger las bases de datos de Microsoft Exchange Server	530
Conceptos del complemento SnapCenter para Microsoft Exchange Server.	530
Descripción general del complemento de SnapCenter para Microsoft Exchange Server.	530
Qué puede hacer con el complemento SnapCenter para Microsoft Exchange Server	531
Tipos de almacenamiento compatibles con el complemento SnapCenter para Microsoft Windows y Microsoft Exchange Server	531
Privilegios mínimos de ONTAP necesarios para el complemento de Exchange.	532
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault.	535
Definir una estrategia de respaldo para los recursos de Exchange Server.	535
Definir una estrategia de restauración para bases de datos de Exchange	538
Instalar el complemento de SnapCenter para Microsoft Exchange Server	539

Flujo de trabajo de instalación del complemento de SnapCenter para Microsoft Exchange Server	539
Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para Microsoft Exchange Server	540
Configurar credenciales para el complemento SnapCenter para Windows	544
Configurar gMSA en Windows Server 2016 o posterior	545
Agregar hosts e instalar el complemento para Exchange	547
Instalar el complemento para Exchange desde el host del servidor SnapCenter mediante cmdlets de PowerShell	552
Instale el complemento de SnapCenter para Exchange de forma silenciosa desde la línea de comandos	553
Supervisar el estado de instalación del paquete de complementos de SnapCenter	554
Configurar el certificado de CA	555
Configurar SnapManager 7.x para que Exchange y SnapCenter coexistan	558
Instalar el SnapCenter Plug-in for VMware vSphere	560
Implementar certificado de CA	560
Configurar el archivo CRL	560
Prepárese para la protección de datos	560
Requisitos previos para utilizar el complemento de SnapCenter para Microsoft Exchange Server	561
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger Exchange Server .	561
Realizar copias de seguridad de los recursos de Exchange	562
Flujo de trabajo de respaldo	562
Verificación de la base de datos y de la copia de seguridad de Exchange	563
Determinar si los recursos de Exchange están disponibles para realizar copias de seguridad	564
Crear políticas de copia de seguridad para bases de datos de Exchange Server	565
Crear grupos de recursos y adjuntar políticas para servidores Exchange	573
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para Exchange Server	576
Realizar copias de seguridad de las bases de datos de Exchange	577
Realizar copias de seguridad de grupos de recursos de Exchange	583
Supervisar las operaciones de copia de seguridad	584
Cancelar operaciones de copia de seguridad de la base de datos de Exchange	585
Ver copias de seguridad de Exchange en la página Topología	586
Restaurar recursos de Exchange	588
Restaurar flujo de trabajo	588
Requisitos para restaurar una base de datos de Exchange	588
Restaurar bases de datos de Exchange	589
Recuperación granular de correos y buzones	593
Restaurar una base de datos de Exchange Server desde un almacenamiento secundario	593
Resembrar una réplica de nodo de Exchange pasivo	594
Resembrar una réplica mediante cmdlets de PowerShell para la base de datos de Exchange	595
Supervisar las operaciones de restauración	596
Cancelar operaciones de restauración de la base de datos de Exchange	596
Proteger IBM Db2	598
Complemento de SnapCenter para IBM Db2	598
Descripción general del complemento SnapCenter para IBM Db2	598

Qué puede hacer utilizando el complemento SnapCenter para IBM Db2	598
Funciones del complemento SnapCenter para IBM Db2	599
Tipos de almacenamiento compatibles con el complemento SnapCenter para IBM Db2	599
Privilegios mínimos de ONTAP necesarios para el complemento IBM Db2	600
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para IBM Db2	603
Estrategia de respaldo para IBM Db2	603
Estrategia de restauración y recuperación para IBM Db2	606
Prepárese para instalar el complemento SnapCenter para IBM Db2	607
Flujo de trabajo de instalación del complemento SnapCenter para IBM Db2	607
Requisitos previos para agregar hosts e instalar paquetes de complementos para Windows, Linux o AIX	607
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	613
Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux	614
Configurar credenciales para el complemento SnapCenter para IBM Db2	615
Configurar gMSA en Windows Server 2016 o posterior	618
Instalar el complemento SnapCenter para IBM Db2	619
Configurar el certificado de CA	625
Prepárese para la protección de datos	633
Requisitos previos para utilizar el complemento SnapCenter para IBM Db2	633
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger IBM Db2	634
Realizar copias de seguridad de los recursos de IBM Db2	634
Realizar copias de seguridad de los recursos de IBM Db2	634
Descubra las bases de datos automáticamente	636
Agregar recursos manualmente al host del complemento	636
Crear políticas de copia de seguridad para IBM Db2	638
Crear grupos de recursos y adjuntar políticas	640
Cree grupos de recursos y habilite la protección secundaria para los recursos de IBM Db2 en sistemas ASA r2	644
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para IBM Db2	647
Realizar copias de seguridad de bases de datos Db2	648
Realizar copias de seguridad de grupos de recursos	655
Supervisar las operaciones de copia de seguridad de IBM Db2	656
Cancelar operaciones de copia de seguridad de IBM Db2	657
Ver copias de seguridad y clones de IBM Db2 en la página Topología	658
Restaurar IBM Db2	660
Restaurar flujo de trabajo	660
Restaurar una copia de seguridad de un recurso agregado manualmente	660
Restaurar y recuperar una copia de seguridad de una base de datos descubierta automáticamente	665
Supervisar las operaciones de restauración de IBM Db2	667
Clonar copias de seguridad de recursos de IBM Db2	667
Flujo de trabajo de clonación	667
Clonar una copia de seguridad de IBM Db2	668
Supervisar las operaciones de clones de IBM Db2	675
Dividir un clon	676

Eliminar o dividir clones de bases de datos de IBM Db2 después de actualizar SnapCenter	677
Proteger PostgreSQL	679
Complemento de SnapCenter para PostgreSQL	679
Descripción general del complemento de SnapCenter para PostgreSQL	679
Qué puede hacer utilizando el complemento SnapCenter para PostgreSQL	679
Funciones del complemento SnapCenter para PostgreSQL	679
Tipos de almacenamiento compatibles con el complemento SnapCenter para PostgreSQL	680
Privilegios mínimos de ONTAP necesarios para el complemento PostgreSQL	681
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para PostgreSQL	684
Estrategia de respaldo para PostgreSQL	684
Estrategia de restauración y recuperación para PostgreSQL	687
Prepárese para instalar el complemento SnapCenter para PostgreSQL	688
Flujo de trabajo de instalación del complemento SnapCenter para PostgreSQL	688
Requisitos previos para agregar hosts e instalar el complemento SnapCenter para PostgreSQL	689
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	692
Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux	693
Configurar credenciales para el complemento SnapCenter para PostgreSQL	694
Configurar gMSA en Windows Server 2016 o posterior	696
Instalar el complemento SnapCenter para PostgreSQL	697
Configurar el certificado de CA	703
Prepárese para la protección de datos	711
Requisitos previos para utilizar el complemento SnapCenter para PostgreSQL	711
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger PostgreSQL	712
Realizar copias de seguridad de los recursos de PostgreSQL	712
Realizar copias de seguridad de los recursos de PostgreSQL	712
Descubra los clústeres automáticamente	714
Agregar recursos manualmente al host del complemento	714
Crear políticas de respaldo para PostgreSQL	716
Crear grupos de recursos y adjuntar políticas	720
Cree grupos de recursos y habilite la protección secundaria para los recursos de PostgreSQL en sistemas ASA r2	724
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para PostgreSQL	727
Realizar una copia de seguridad de PostgreSQL	728
Realizar copias de seguridad de grupos de recursos	734
Supervisar las operaciones de copia de seguridad de PostgreSQL	735
Cancelar operaciones de copia de seguridad para PostgreSQL	736
Ver copias de seguridad y clones de PostgreSQL en la página Topología	737
Restaurar PostgreSQL	739
Restaurar flujo de trabajo	739
Restaurar y recuperar una copia de seguridad de un recurso agregado manualmente	739
Restaurar y recuperar una copia de seguridad de un clúster detectado automáticamente	744
Restaurar recursos mediante cmdlets de PowerShell	747
Supervisar operaciones de restauración de PostgreSQL	749

Clonar copias de seguridad de recursos de PostgreSQL	750
Flujo de trabajo de clonación	750
Clonar una copia de seguridad de PostgreSQL	751
Supervisar operaciones de clonación de PostgreSQL	754
Dividir un clon	755
Eliminar o dividir clones del clúster PostgreSQL después de actualizar SnapCenter	756
Proteger MySQL	758
Complemento de SnapCenter para MySQL	758
Descripción general del complemento SnapCenter para MySQL	758
Qué puede hacer utilizando el complemento SnapCenter para MySQL	758
Funciones del complemento SnapCenter para MySQL	758
Tipos de almacenamiento compatibles con el complemento SnapCenter para MySQL	759
Privilegios mínimos de ONTAP necesarios para el complemento MySQL	760
Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para MySQL ..	763
Estrategia de respaldo para MySQL	763
Estrategia de restauración y recuperación para MySQL	766
Prepárese para instalar el complemento SnapCenter para MySQL	767
Flujo de trabajo de instalación del complemento SnapCenter para MySQL	767
Requisitos previos para agregar hosts e instalar el complemento SnapCenter para MySQL	767
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	771
Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux	772
Configurar credenciales para el complemento SnapCenter para MySQL	773
Instalar el complemento SnapCenter para MySQL	776
Configurar el certificado de CA	781
Prepárese para la protección de datos	789
Requisitos previos para utilizar el complemento SnapCenter para MySQL	789
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger MySQL	789
Realizar copias de seguridad de los recursos de MySQL	790
Realizar copias de seguridad de los recursos de MySQL	790
Descubra las bases de datos automáticamente	792
Agregar recursos manualmente al host del complemento	792
Crear políticas de respaldo para MySQL	793
Crear grupos de recursos y adjuntar políticas	797
Cree grupos de recursos y habilite la protección secundaria para los recursos MySQL en sistemas ASA r2	801
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para MySQL	804
Realizar una copia de seguridad de MySQL	806
Realizar copias de seguridad de grupos de recursos	811
Supervisar las operaciones de copia de seguridad de MySQL	812
Cancelar operaciones de copia de seguridad de MySQL	813
Ver copias de seguridad y clones de MySQL en la página Topología	814
Restaurar MySQL	816
Restaurar flujo de trabajo	816
Restaurar y recuperar una copia de seguridad de un recurso agregado manualmente	816

Restaurar y recuperar una copia de seguridad de una base de datos descubierta automáticamente . .	821
Restaurar recursos mediante cmdlets de PowerShell	823
Supervisar las operaciones de restauración de MySQL	825
Clonar copias de seguridad de recursos de MySQL	826
Flujo de trabajo de clonación	826
Clonar una copia de seguridad de MySQL	827
Supervisar las operaciones de clonación de MySQL	831
Dividir un clon.	832
Eliminar o dividir clones de bases de datos MySQL después de actualizar SnapCenter	833
Proteja las aplicaciones mediante complementos compatibles con NetApp	835
Complementos compatibles con NetApp	835
Descripción general de los complementos compatibles con NetApp	835
Qué puede hacer con los complementos compatibles con NetApp	835
Funciones de los complementos compatibles con NetApp	836
Tipos de almacenamiento compatibles con los complementos de NetApp	837
Privilegios mínimos de ONTAP necesarios para el complemento compatible con NetApp	837
Prepare los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para complementos compatibles con NetApp	840
Definir una estrategia de backup	840
Estrategia de respaldo para complementos compatibles con NetApp	841
Tipos de estrategias de restauración compatibles con recursos de complementos compatibles con NetApp agregados manualmente	842
Prepárese para instalar los complementos compatibles con NetApp	842
Flujo de trabajo de instalación de complementos compatibles con SnapCenter NetApp	842
Requisitos previos para agregar hosts e instalar paquetes de complementos para Windows, Linux o AIX	843
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	847
Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux y AIX	848
Configurar credenciales para complementos compatibles con NetApp	849
Configurar gMSA en Windows Server 2016 o posterior	852
Instalar los complementos compatibles con NetApp	853
Configurar el certificado de CA	859
Prepárese para la protección de datos	867
Requisitos previos para utilizar los complementos compatibles con NetApp	867
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger los recursos de complementos compatibles con NetApp	868
Realizar copias de seguridad de los recursos de complementos compatibles con NetApp	869
Realizar copias de seguridad de los recursos de complementos compatibles con NetApp	869
Agregar recursos a los complementos compatibles con NetApp	870
Crear políticas para recursos de complementos compatibles con NetApp	874
Crear grupos de recursos y adjuntar políticas	878
Cree grupos de recursos y habilite la protección secundaria para los recursos en los sistemas ASA r2	882
Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell	884
Realizar copias de seguridad de recursos de complementos individuales compatibles con NetApp	886
Realizar copias de seguridad de grupos de recursos de complementos compatibles con NetApp	891

Supervisar las operaciones de respaldo de recursos del complemento compatibles con NetApp	892
Cancelar operaciones de copia de seguridad para complementos compatibles con NetApp	893
Vea las copias de seguridad y clones relacionados con los recursos de complementos compatibles con NetApp en la página Topología	894
Restaurar recursos de complementos compatibles con NetApp	896
Restaurar recursos de complementos compatibles con NetApp	896
Restaurar una copia de seguridad de recursos	896
Supervisar las operaciones de restauración de recursos del complemento compatible con NetApp . . .	901
Copias de seguridad de recursos de complementos compatibles con Clonar NetApp	902
Copias de seguridad de recursos de complementos compatibles con Clonar NetApp	902
Clonar desde una copia de seguridad	903
Supervisar las operaciones de clonación de recursos del complemento compatibles con NetApp	909
Proteger los sistemas de archivos Unix	911
Qué puede hacer con el complemento SnapCenter para sistemas de archivos Unix	911
Configuraciones compatibles	911
Limitaciones	912
Funciones	912
Instalar el complemento SnapCenter para sistemas de archivos Unix	912
Requisitos previos para agregar hosts e instalar el paquete de complementos para Linux	912
Agregar hosts e instalar el paquete de complementos para Linux mediante GUI	914
Configurar el servicio de Loader de complementos de SnapCenter	917
Configurar el certificado de CA con el servicio SnapCenter Plug-in Loader (SPL) en el host Linux	920
Habilitar certificados CA para complementos	923
Instalar el SnapCenter Plug-in for VMware vSphere	924
Implementar certificado de CA	924
Configurar el archivo CRL	924
Prepárese para proteger los sistemas de archivos Unix	924
Realizar copias de seguridad de los sistemas de archivos Unix	925
Descubra los sistemas de archivos UNIX disponibles para realizar copias de seguridad	925
Crear políticas de respaldo para sistemas de archivos Unix	925
Crear grupos de recursos y adjuntar políticas para sistemas de archivos Unix	928
Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Unix en sistemas ASA r2	930
Realizar copias de seguridad de los sistemas de archivos Unix	933
Realizar copias de seguridad de los grupos de recursos de los sistemas de archivos Unix	934
Supervisar la copia de seguridad de los sistemas de archivos Unix	935
Ver sistemas de archivos Unix protegidos en la página Topología	936
Restaurar y recuperar sistemas de archivos Unix	939
Restaurar sistemas de archivos Unix	939
Supervisar las operaciones de restauración de sistemas de archivos Unix	941
Clonar sistemas de archivos Unix	941
Copia de seguridad del sistema de archivos clonado de Unix	941
Dividir un clon	943
Supervisar operaciones de clonación de sistemas de archivos Unix	944
Proteger las aplicaciones que se ejecutan en Azure NetApp Files	946

Proteger las aplicaciones que se ejecutan en Azure NetApp Files	946
Limitaciones	946
Instalar SnapCenter y crear credenciales	946
Instalar SnapCenter en una máquina virtual de Azure	946
Crear la credencial de Azure en SnapCenter	948
Configurar la cuenta de almacenamiento de Azure	949
Cree las credenciales para agregar el host del complemento	949
Proteger las bases de datos de SAP HANA	950
Agregar hosts e instalar el complemento de SnapCenter para la base de datos SAP HANA	950
Agregar base de datos SAP HANA	951
Crear políticas de respaldo para bases de datos de SAP HANA	952
Cree grupos de recursos y adjunte políticas de respaldo de SAP HANA	952
Realice una copia de seguridad de las bases de datos de SAP HANA que se ejecutan en Azure NetApp Files	953
Realizar copias de seguridad de los grupos de recursos de SAP HANA	954
Restaurar y recuperar bases de datos de SAP HANA	955
Clonar copia de seguridad de la base de datos de SAP HANA	956
Proteger las bases de datos de Microsoft SQL Server	957
Agregar hosts e instalar el complemento de SnapCenter para la base de datos de SQL Server	957
Crear políticas de respaldo para bases de datos de SQL Server	958
Crear grupos de recursos y adjuntar políticas de respaldo de SQL	959
Realizar copias de seguridad de bases de datos de SQL Server que se ejecutan en Azure NetApp Files	960
Realizar copias de seguridad de grupos de recursos de SQL Server	961
Restaurar y recuperar bases de datos de SQL Server	962
Copia de seguridad de la base de datos de clonación de SQL Server	963
Proteger las bases de datos de Oracle	965
Agregar hosts e instalar el complemento SnapCenter para la base de datos Oracle	965
Crear políticas de respaldo para bases de datos de Oracle	965
Crear grupos de recursos y adjuntar políticas de respaldo de Oracle	966
Realizar copias de seguridad de bases de datos de Oracle que se ejecutan en Azure NetApp Files	967
Realizar copias de seguridad de grupos de recursos de Oracle	968
Restaurar y recuperar bases de datos Oracle	969
Copia de seguridad de la base de datos Clonar Oracle	971
Administrar SnapCenter Server y complementos	975
Ver el panel de control	975
Descripción general del panel de control	975
Cómo ver información en el panel de control	979
Solicitar informes de estado de los trabajos desde el panel de control	979
Solicitar informes del estado de protección desde el panel de control	980
Administrar RBAC	980
Modificar un rol	981
Modificar usuarios y grupos	981
Administrar hosts	982
Actualizar la información de la máquina virtual	984

Modificar los hosts de los complementos	984
Iniciar o reiniciar los servicios del complemento	985
Suspender programaciones para mantenimiento del host	986
Operaciones respaldadas desde la página de Recursos	986
Administrar políticas	987
Modificar políticas	988
Desvincular políticas	988
Eliminar políticas	989
Administrar grupos de recursos	989
Detener y reanudar operaciones en grupos de recursos	990
Eliminar grupos de recursos	990
Administrar copias de seguridad	990
Cambiar el nombre de las copias de seguridad	991
Eliminar copias de seguridad	991
Quitar la protección	992
Eliminar clones	992
Supervisar trabajos, programaciones, eventos y registros	993
Monitorear trabajos	993
Monitorear horarios	994
Monitorear eventos	995
Monitorear registros	995
Eliminar trabajos y registros de SnapCenter	996
Descripción general de las capacidades de generación de informes de SnapCenter	997
Informes de acceso	998
Filtrar su informe	998
Exportar o imprimir informes	999
Configurar el servidor SMTP para notificaciones por correo electrónico	999
Configurar la opción de enviar informes por correo electrónico	1000
Administrar el repositorio de SnapCenter Server	1000
Requisitos previos para proteger el repositorio de SnapCenter	1000
Realice una copia de seguridad del repositorio de SnapCenter	1001
Ver copias de seguridad del repositorio de SnapCenter	1001
Restaurar el repositorio de la base de datos de SnapCenter	1001
Migrar el repositorio de SnapCenter	1002
Restablecer la contraseña del repositorio de SnapCenter	1003
Administrar recursos de dominios no confiables	1003
Modificar dominios no confiables	1004
Anular el registro de dominios de Active Directory que no sean de confianza	1004
Administrar el sistema de almacenamiento	1005
Modificar la configuración del sistema de almacenamiento	1005
Eliminar el sistema de almacenamiento	1007
Compatibilidad con API REST	1008
Gestionar la recopilación de datos de EMS	1008
Detener la recopilación de datos de EMS	1008
Iniciar la recopilación de datos EMS	1009

Cambiar el cronograma de recopilación de datos de EMS y el SVM objetivo	1009
Supervisar el estado de la recopilación de datos de EMS.	1009
Actualizar SnapCenter Server y los complementos	1011
Configurar SnapCenter para buscar actualizaciones disponibles	1011
Actualizar el flujo de trabajo	1011
Rutas de actualización admitidas	1011
Actualizar el servidor SnapCenter en el host de Windows	1012
Actualizar el servidor SnapCenter en el host Linux	1014
Actualice sus paquetes de complementos	1015
Actualización tecnológica	1018
Actualización tecnológica del host del servidor SnapCenter	1018
Actualización tecnológica de un nodo en el clúster F5	1019
Desactivación del antiguo host del servidor SnapCenter	1019
Revertir al antiguo host de SnapCenter Server	1019
Recuperación ante desastres	1019
Actualización tecnológica de los hosts de complementos de SnapCenter	1021
Actualización tecnológica del sistema de almacenamiento	1023
Actualizar las copias de seguridad del almacenamiento principal	1024
Actualizar las copias de seguridad del almacenamiento secundario	1026
Desinstalar SnapCenter Server y sus complementos	1028
Desinstalar los paquetes de complementos de SnapCenter	1028
Requisitos previos para eliminar un host	1028
Eliminar un host	1029
Desinstalar complementos mediante la GUI de SnapCenter	1030
Desinstalar complementos de Windows mediante el cmdlet de PowerShell	1031
Desinstalar complementos localmente en un host	1031
Desinstalar el paquete de complementos para Linux o AIX mediante CLI	1032
Desinstalar el servidor SnapCenter en el host de Windows	1032
Desinstalar el servidor SnapCenter en el host Linux	1032
Automatizar mediante API REST	1034
Automatización de SnapCenter mediante API REST	1034
Cómo acceder a la API REST de SnapCenter de forma nativa	1034
Fundación de servicios web REST	1034
Recursos y representación estatal	1034
Puntos finales URI	1035
Mensajes HTTP	1035
Formato JSON	1035
Características operativas básicas	1035
Transacción de API de solicitud y respuesta	1035
Soporte para operaciones CRUD	1035
Identificadores de objetos	1036
Instancias y colecciones de objetos	1036
Operaciones sincrónicas y asincrónicas	1036
Seguridad	1036
Variables de entrada que controlan una solicitud de API	1037

Métodos HTTP	1037
Encabezados de solicitud	1037
Cuerpo de la solicitud	1037
Filtrado de objetos	1038
Solicitar campos de objeto específicos	1038
Ordenar objetos en el conjunto de salida	1039
Paginación al recuperar objetos de una colección	1039
Propiedades de tamaño	1040
Interpretación de una respuesta de API	1040
Código de estado HTTP	1040
Encabezados de respuesta	1041
Cuerpo de la respuesta	1041
Errores	1042
API REST compatibles con SnapCenter Server y complementos	1043
Autorización	1043
Dominios	1043
Empleos	1043
Configuración	1043
Anfitriones	1044
Recursos	1044
Copias de seguridad	1046
Clones	1046
División de clones	1047
Grupos de recursos	1047
Políticas	1047
Almacenamiento	1047
Compartir	1048
Complementos	1048
Informes	1049
Alertas	1049
Rbac	1049
Configuración	1050
Configuración del certificado	1050
Repositorio	1050
Versión	1050
Cómo acceder a las API REST mediante la página web de la API de Swagger	1050
Comience a utilizar la API REST	1051
Hola Mundo	1051
Avisos legales	1053
Copyright	1053
Marcas comerciales	1053
Patentes	1053
Política de privacidad	1053
Código abierto	1053

Documentación del SnapCenter software

Notas de la versión

Notas de la versión

Obtenga información sobre las funciones nuevas y mejoradas disponibles en SnapCenter 6.1.

Para obtener una lista completa de las nuevas funciones y mejoras, consulte ["Novedades de SnapCenter 6.1"](#).

Para obtener detalles sobre problemas conocidos, limitaciones, problemas solucionados y comandos nuevos y modificados, consulte la ["Notas de la versión 6.1 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 compatibles con SnapCenter

La ruta de actualización le ayuda a comprender desde qué versiones anteriores de SnapCenter puede actualizar a las últimas versiones de SnapCenter y qué versiones de los complementos son compatibles.

Si está en la versión SnapCenter Server...	Puede actualizar directamente SnapCenter Server a...	Versiones de complementos compatibles
5,0	6,0	• 5,0 • 6,0
	6.0.1	• 6.0.1
	6,1	• 6,1
6,0	6.0.1	• 6,0 • 6.0.1
	6,1	• 6,1
6.0.1	6,1	• 6.0.1 • 6,1

Para obtener información sobre cómo actualizar el SnapCenter Plug-in for VMware vSphere, consulte ["Actualizar el SnapCenter Plug-in for VMware vSphere"](#).

Empezar

Obtenga más información sobre el SnapCenter software

Descripción 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:

- Copias de seguridad rápidas, eficientes en cuanto al espacio y consistentes con las aplicaciones basadas en disco
- Restauración rápida y detallada, y recuperación consistente con la aplicación
- Clonación rápida y que ahorra 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 que se encuentran en los sistemas primarios ONTAP FAS, AFF o ASA y se replican en los sistemas secundarios ONTAP FAS, AFF o ASA
 - Datos que se encuentran en los sistemas primarios de ONTAP Select
 - Datos que se encuentran en sistemas primarios y secundarios de ONTAP FAS, AFF o ASA y están protegidos en el almacenamiento de objetos StorageGRID local
 - Datos que se encuentran en los sistemas primarios y secundarios de ONTAP ASA r2
- Local en una nube híbrida para proteger lo siguiente:
 - Datos que se encuentran en los sistemas principales de ONTAP FAS, AFF o ASA y se replican en Cloud Volumes ONTAP
 - Datos que se encuentran en sistemas primarios y secundarios de ONTAP FAS, AFF o ASA y están protegidos en almacenamiento de objetos y archivos en la nube (mediante la integración de BlueXP backup and recovery)
- En una nube pública para proteger lo siguiente:
 - Datos que se encuentran en los sistemas principales de Cloud Volumes ONTAP (anteriormente ONTAP Cloud)
 - Datos que están en Amazon FSX para ONTAP
 - Datos que se encuentran en los Azure NetApp Files (Oracle, Microsoft SQL y SAP HANA)

Características principales

SnapCenter ofrece las siguientes características clave:

- Protección de datos centralizada y consistente para cada aplicación

La protección de datos es compatible con Microsoft Exchange Server, Microsoft SQL Server, bases de datos Oracle en Linux o AIX, bases de datos SAP HANA, IBM Db2, PostgreSQL, MySQL y sistemas de archivos de host de Windows que se ejecutan en sistemas ONTAP . SnapCenter también admite la protección de aplicaciones como MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Copias de seguridad basadas en políticas

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 .

- Restaurar y recuperar

SnapCenter proporciona restauraciones rápidas y granulares de copias de seguridad y una recuperación basada en el tiempo y consistente con las aplicaciones. Puede restaurar desde cualquier destino en la nube híbrida.

- Clonación

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 REST, cmdlets de Windows, comandos de UNIX

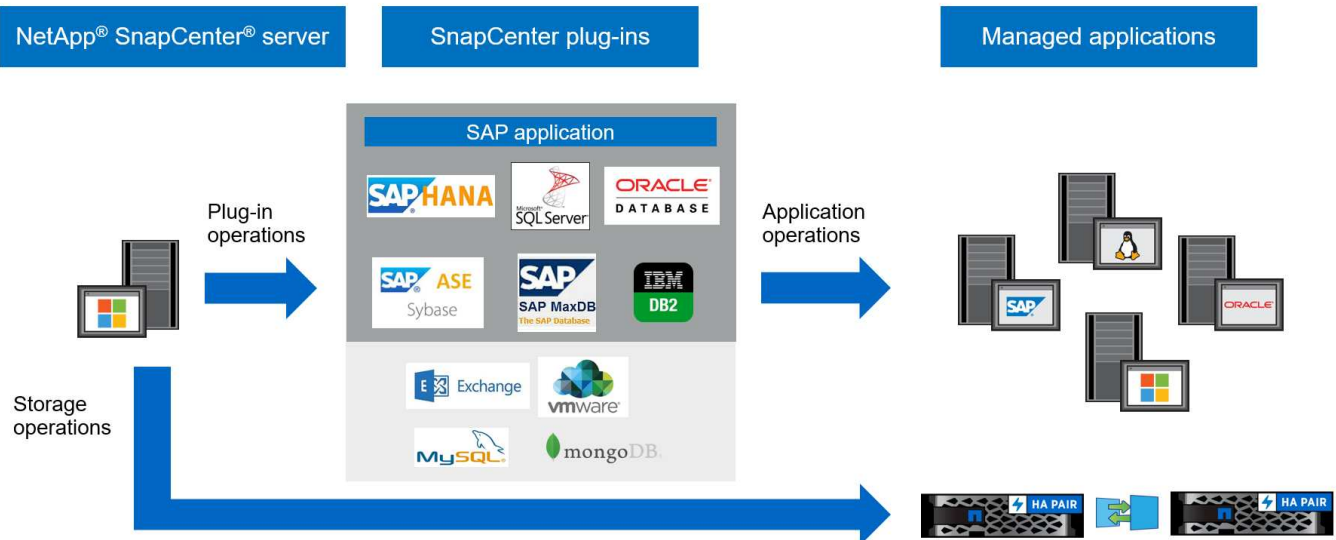
SnapCenter proporciona API REST para la mayoría de las funciones para la integración con cualquier software de orquestación y el uso de cmdlets de Windows PowerShell y la interfaz de línea de comandos.

- Panel de control y generación de informes de protección de datos centralizados
- 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 respaldo
- Instalación push automatizada de complementos
- Alta disponibilidad
- Recuperación ante desastres (DR)
- SnapLock "[Más información](#)"

- Sincronización activa de SnapMirror (inicialmente lanzada como SnapMirror Business Continuity [SM-BC])
- Duplicación sincrónica "[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 SnapCenter Server, el paquete de complementos de SnapCenter para Windows y el paquete de complementos de SnapCenter para Linux. Cada paquete contiene complementos para diversas aplicaciones y componentes de 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 REST y el repositorio de SnapCenter .

SnapCenter almacena información sobre sus operaciones en el repositorio de SnapCenter .

Complementos de SnapCenter

Cada complemento de SnapCenter admite entornos, bases de datos y aplicaciones específicos.

Nombre del complemento	Incluido en el paquete de instalación	Requiere otros complementos	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para Microsoft SQL Server	Paquete de complementos para Windows	Complemento para Windows	Host de SQL Server	Ventanas
Complemento de SnapCenter para Windows	Paquete de complementos para Windows		Host de Windows	Ventanas

Nombre del complemento	Incluido en el paquete de instalación	Requiere otros complementos	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para Microsoft Exchange Server	Paquete de complementos para Windows	Complemento para Windows	Host del servidor Exchange	Ventanas
Complemento de SnapCentre para Oracle Database	Paquete de complementos para Linux y paquete de complementos para AIX	Complemento para UNIX	Host de Oracle	Linux o AIX
Complemento de SnapCenter para la base de datos SAP HANA	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host del cliente HDBSQL	Linux o Windows
Complemento de SnapCenter para IBM Db2	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de Db2	Linux, AIX o Windows
Complemento de SnapCenter para PostgreSQL	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de PostgreSQL	Linux o Windows
Complemento SnaoCenter para MySQL	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host MySQL	Linux o Windows
Complemento de SnapCenter para MongoDB	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de MongoDB	Linux o Windows
Complemento de SnapCenter para ORASCPM (aplicaciones Oracle)	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de Oracle	Linux o Windows

Nombre del complemento	Incluido en el paquete de instalación	Requiere otros complementos	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para SAP ASE	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host SAP	Linux o Windows
Complemento de SnapCenter para SAP MaxDB	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de SAP MaxDB	Linux o Windows
Complemento de SnapCenter para almacenamiento	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento 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 SnapCenter Plug-in for VMware vSphere"](#) .

Repositorio de SnapCenter

El repositorio de SnapCenter , a veces denominado base de datos NSM, almacena información y metadatos para cada operación de 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:

- Copia de seguridad, clonación, restauración y verificación de metadatos
- Información de informes, trabajos y eventos
- Información del host y del complemento
- Detalles de rol, usuario y permisos
- Información de conexión del sistema de almacenamiento

Funciones de seguridad en SnapCenter

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

SnapCenter incluye las siguientes funciones de seguridad:

- Toda comunicación con SnapCenter utiliza HTTP sobre SSL (HTTPS).
- Todas las credenciales en SnapCenter están protegidas mediante el cifrado Estándar de cifrado avanzado (AES).
- Admite algoritmos de seguridad que cumplen con el Estándar Federal de Procesamiento de Información (FIPS).
- Admite el uso de los certificados CA autorizados proporcionados por el cliente.
- Admite seguridad de la capa de transporte (TLS) 1.3 para la comunicación con ONTAP. También puede utilizar TLS 1.2 para la comunicación entre clientes y servidores.
- Admite un determinado conjunto de suites de cifrado SSL para proporcionar seguridad en las comunicaciones de red. ["Más información"](#) .
- SnapCenter se instala dentro del firewall de su empresa para permitir el acceso al servidor SnapCenter y para permitir la comunicación entre el servidor SnapCenter y los complementos.
- El acceso a la API y a las operaciones de SnapCenter utiliza tokens cifrados con cifrado AES, que caducan después de 24 horas.
- SnapCenter se integra con Windows Active Directory para el inicio de sesión y el control de acceso basado en roles (RBAC) que rigen los permisos de acceso.
- IPsec es compatible con SnapCenter en ONTAP para máquinas host de Windows y Linux. ["Más información"](#) .
- Los cmdlets de PowerShell de SnapCenter están protegidos por sesión.
- Después de un período predeterminado de 15 minutos de inactividad, SnapCenter le advierte que se cerrará su sesión en 5 minutos.

Después de 20 minutos de inactividad, SnapCenter cerrará su sesión y deberá iniciar sesión nuevamente. Puede modificar el período de cierre de sesión.

- El inicio de sesión se deshabilita temporalmente después de 5 intentos de inicio de sesión incorrectos.
- Admite la autenticación de certificados CA entre SnapCenter Server y ONTAP. ["Más información"](#) .
- Integrity Verifier se agrega al servidor SnapCenter y a los complementos y valida todos los binarios enviados durante las operaciones de instalación y actualización nuevas.

Descripción general del certificado CA

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

Debe implementar certificados CA después de instalar SnapCenter Server y los complementos respectivos. Para obtener más información, consulte ["Generar archivo CSR de certificado de CA"](#) .

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

Comunicación SSL bidireccional

La comunicación SSL bidireccional asegura la comunicación mutua entre SnapCenter Server y los complementos.

Descripción general de la autenticación basada en certificados

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

Autenticación multifactor (MFA)

MFA utiliza un proveedor de identidad (IdP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para administrar las sesiones de usuario. Esta funcionalidad mejora la seguridad de la autenticación al tener la opción de utilizar múltiples factores como TOTP, biometría, notificaciones push, etc. junto con el nombre de usuario y la contraseña existentes. Además, permite al cliente utilizar sus propios proveedores de identidad de usuario para obtener un inicio de sesión de usuario unificado (SSO) en toda su cartera.

MFA solo se aplica para iniciar sesión en la interfaz de usuario de SnapCenter Server. Los inicios de sesión se autentican a través del IdP Servicios de federación de Active Directory (AD FS). Puede configurar varios factores de autenticación en AD FS. SnapCenter es el proveedor de servicios y debe SnapCenter como parte confiable en AD FS. Para habilitar MFA en SnapCenter, necesitará los metadatos de AD FS.

Para obtener información sobre cómo habilitar MFA, consulte ["Habilitar 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 delegar el control de los recursos de SnapCenter a diferentes usuarios o grupos de usuarios. Este acceso administrado centralmente permite a los administradores de aplicaciones trabajar de forma segura dentro de entornos delegados.

Puede crear y modificar roles y agregar acceso a recursos a los usuarios en cualquier momento. Sin embargo, cuando configure SnapCenter por primera vez, deberá al menos agregar usuarios o grupos de Active Directory a los roles y luego agregar acceso a recursos a esos usuarios o grupos.



No puede utilizar SnapCenter para crear cuentas de usuario o grupo. Debe crear cuentas de usuario o grupo en Active Directory del sistema operativo o la base de datos.

Tipos de RBAC en SnapCenter

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

- RBAC de SnapCenter
- RBAC a nivel de aplicación
- Complemento de SnapCenter para VMware vSphere RBAC
- Permisos de ONTAP

RBAC de SnapCenter

SnapCenter tiene roles predefinidos y usted puede asignar usuarios o grupos de usuarios a estos roles. Los roles predefinidos son:

- Rol de administrador de SnapCenter
- Rol de administrador de copias de seguridad y clonación de aplicaciones
- Función de visor de copias de seguridad y clones
- Rol de administrador de infraestructura

Cuando asigna un rol a un usuario, solo los trabajos que son relevantes para ese usuario son visibles en la página Trabajos, a menos que le asigne el rol SnapCenterAdmin.

También puede crear nuevos roles y administrar permisos y usuarios. Puede asignar permisos a usuarios o grupos para acceder a objetos de SnapCenter , como hosts, conexiones de almacenamiento y grupos de recursos.

Puede asignar permisos RBAC a usuarios y grupos dentro del mismo bosque y a usuarios que pertenecen a diferentes bosques. No se pueden asignar permisos RBAC a usuarios que pertenecen a grupos anidados en distintos bosques.



Si crea un rol personalizado, debe contener todos los permisos del rol SnapCenterAdmin. Si solo copia algunos de los permisos, por ejemplo, agregar host o quitar host, no podrá realizar esas operaciones.

Los usuarios deben proporcionar autenticación durante el inicio de sesión, a través de la interfaz gráfica de usuario (GUI) o utilizando cmdlets de PowerShell. Si los usuarios son miembros de más de un rol, después de ingresar las credenciales de inicio de sesión, se les solicita que especifiquen el rol que desean usar. Los usuarios también deben proporcionar autenticación para ejecutar las API.

RBAC a nivel de aplicación

SnapCenter utiliza credenciales para verificar que los usuarios autorizados de SnapCenter también tengan permisos a nivel de aplicación.

Por ejemplo, si desea realizar operaciones de protección de datos en un entorno de SQL Server, debe configurar las credenciales con las credenciales de Windows o SQL adecuadas. El servidor SnapCenter autentica las credenciales establecidas utilizando cualquiera de los métodos. 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.

SnapCenter Plug-in for VMware vSphere RBAC

Si utiliza el complemento VMware de SnapCenter para la protección de datos consistente con la máquina virtual, vCenter Server proporciona un nivel adicional de RBAC. El complemento VMware de SnapCenter admite tanto vCenter Server RBAC como ONTAP RBAC. ["Más información"](#)

Mejor práctica: 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, debe asignar el permiso StorageConnection para habilitar la comunicación de la máquina virtual de almacenamiento (SVM) o asignar una SVM al usuario para habilitar el permiso para usar la SVM. El permiso de Conexión de almacenamiento permite a los usuarios crear conexiones SVM.

Por ejemplo, un usuario con el rol de administrador de SnapCenter puede crear conexiones SVM y asignarlas a un usuario con el rol de administrador de copias de seguridad y clones de aplicaciones, que de manera predeterminada no tiene permiso para crear o editar conexiones SVM. Sin una conexión SVM, los usuarios no pueden completar ninguna operación de copia de seguridad, clonación o restauración.

Rol de administrador de SnapCenter

El rol de administrador de SnapCenter tiene todos los permisos habilitados. No puedes modificar los permisos para este rol. Puede agregar usuarios y grupos al rol o eliminarlos.

Rol de administrador de copias de seguridad y clonación de aplicaciones

El rol de administrador de copias de seguridad y clones de aplicaciones tiene los permisos necesarios para realizar acciones administrativas para copias de seguridad de aplicaciones y tareas relacionadas con clones. Esta función no tiene permisos para administración de host, aprovisionamiento, administración de conexión de almacenamiento o instalación remota.

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	Sí	Sí	Sí	Sí
Respaldo	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	No	Sí	No	No
Clon	No aplicable	Sí	Sí	Sí	Sí
Disposición	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Informes	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 complementos	No	No aplicable		No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montar	Sí	Sí	No aplicable	No aplicable	No aplicable
Desmontar	Sí	Sí	No aplicable	No aplicable	No aplicable
Restauración de volumen completo	No	No	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajo	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Función de visor de copias de seguridad y clones

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	Habilitado	Crear	Leer	Actualizar	Borrar
Grupo de recursos	No aplicable	No	Sí	No	No
Política	No aplicable	No	Sí	No	No
Respaldo	No aplicable	No	Sí	No	No
Host	No aplicable	No	Sí	No	No
Conexión de almacenamiento	No aplicable	No	Sí	No	No

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Clon	No aplicable	No	Sí	No	No
Disposición	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Informes	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	No	No	No aplicable	No aplicable	No aplicable
Recurso	No	No	Sí	Sí	No
Instalar/desinstalar complementos	No	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restauración de volumen completo	No	No aplicable	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No aplicable	No aplicable	No aplicable	No aplicable
Monitor de trabajo	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Rol de administrador de infraestructura

El rol de administrador de infraestructura tiene permisos habilitados para la administración de host, administración de almacenamiento, aprovisionamiento, grupos de recursos, informes de instalación remota y acceso al Panel de control.

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	No	Sí	Sí	Sí

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Respaldo	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	Sí	Sí	Sí	Sí
Clon	No aplicable	No	Sí	No	No
Disposición	No aplicable	Sí	Sí	Sí	Sí
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Informes	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 complementos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montar	No	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	No	No aplicable	No aplicable	No aplicable	No aplicable
Restauración de volumen completo	No	No	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajo	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 corrupción de recursos o fallas del servidor. Ayuda a restaurar el repositorio de SnapCenter , las programaciones del servidor, los componentes de

configuración y el complemento de SnapCenter para SQL Server y su almacenamiento.

Esta sección explica los dos tipos de DR en SnapCenter:

Recuperación ante desastres del servidor SnapCenter

- Los datos de SnapCenter Server se respaldan y se pueden recuperar sin necesidad de agregar ni administrar ningún complemento a SnapCenter Server.
- El servidor SnapCenter secundario debe instalarse en el mismo directorio de instalación y en el mismo puerto que el servidor SnapCenter principal.
- Para la autenticación multifactor (MFA), durante la recuperación ante desastres de SnapCenter Server, cierre todas las pestañas del navegador y vuelva a abrir un navegador para iniciar sesión nuevamente. 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 API REST para realizar copias de seguridad del servidor SnapCenter . Ver ["Flujos de trabajo de API REST para la recuperación ante desastres de SnapCenter Server"](#) .
- El archivo de configuración relacionado con la configuración de auditoría no se respalda en la copia de seguridad de DR ni en el servidor de DR después de la operación de restauración. Debe repetirse manualmente la configuración del registro de auditoría.

Complemento de SnapCenter y recuperación ante desastres de almacenamiento

DR solo está disponible para el complemento SnapCenter para SQL Server. Si el complemento no funciona, cambie a otro host SQL y recupere los datos siguiendo unos pocos pasos. Ver ["Recuperación ante desastres del complemento SnapCenter para SQL Server"](#) .

SnapCenter utiliza ONTAP SnapMirror para replicar datos, que pueden usarse para recuperación ante desastres manteniendo los datos sincronizados en un sitio secundario. Para iniciar la conmutación por error, interrumpa la replicación de SnapMirror . Durante la recuperación, invierta la sincronización para replicar los datos desde el sitio de recuperación ante desastres a la ubicación principal.

Licencias requeridas por SnapCenter

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

Licencia	Cuando sea necesario
SnapCenter Standard basado en controlador	Requerido para FAS, AFF, ASA La licencia estándar de SnapCenter es una licencia basada en controlador y se incluye como parte de NetApp ONTAP One. Si tiene la licencia de SnapManager Suite, también obtendrá el derecho de licencia de SnapCenter Standard. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS, AFF o ASA , puede obtener una licencia de evaluación de NetApp ONTAP One comunicándose 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 modelo A400 o posterior, deberá adquirir el paquete de protección de datos.
SnapMirror o SnapVault	ONTAP Se requiere una licencia de SnapMirror o SnapVault si la replicación está habilitada en SnapCenter.
SnapRestore	Necesario para restaurar y verificar copias de seguridad. Sobre los sistemas de almacenamiento primario • Requerido en los sistemas de destino SnapVault para realizar la verificación remota y restaurar desde una copia de seguridad. • Requerido en los sistemas de destino SnapMirror para realizar la verificación remota.

Licencia	Cuando sea necesario
FlexClone	Necesario para clonar bases de datos y realizar operaciones de verificación. Sobre sistemas de almacenamiento primario y secundario • Requerido en los sistemas de destino SnapVault para crear clones a partir de una copia de seguridad de la bóveda secundaria. • Requerido en los sistemas de destino SnapMirror para crear clones a partir de una copia de seguridad secundaria de SnapMirror .
Licencias de protocolo	• Licencia iSCSI o FC para LUN • Licencia CIFS para acciones SMB • Licencia NFS para VMDK de tipo NFS • Licencia iSCSI o FC para VMDK de tipo VMFS Obligatorio en los sistemas de destino SnapMirror para servir datos si un volumen de origen no está disponible.
Licencias estándar de SnapCenter (opcionales)	Destinos secundarios  Se recomienda, aunque no es obligatorio, que agregue licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter no están habilitadas en destinos secundarios, no podrá usar SnapCenter para realizar copias de seguridad de recursos en el destino secundario después de realizar una operación de conmutación por error. Sin embargo, se requiere una licencia FlexClone en destinos secundarios para realizar operaciones de clonación y verificación.

Licencia	Cuando sea necesario
Licencias de recuperación de buzón único (SMBR)	Si utiliza el complemento SnapCenter para Exchange para administrar las bases de datos de Microsoft Exchange Server y Single Mailbox Recovery (SMBR), necesitará una licencia adicional para SMBR que debe comprarse por separado según el buzón del usuario. NetApp® Single Mailbox Recovery llegó al final de su disponibilidad (EOA) el 12 de mayo de 2023. Para obtener más información, consulte "CPC-00507" . NetApp seguirá brindando soporte a los clientes que hayan adquirido capacidad de buzón, mantenimiento y soporte a través de los números de pieza de marketing introducidos el 24 de junio de 2020, mientras dure el derecho de soporte. NetApp Single Mailbox Recovery es un producto asociado proporcionado por Ontrack. Ontrack PowerControls ofrece capacidades similares a las de NetApp Single Mailbox Recovery. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls de Ontrack (a través de licensingteam@ontrack.com) para la recuperación granular del buzón después de la fecha de fin de operación del 12 de mayo de 2023.



Las licencias de SnapCenter Advanced y SnapCenter NAS File Services están obsoletas y ya no están disponibles. La licencia estándar y la licencia basada en capacidad ya no son necesarias para Amazon FSx for 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 ["Agregar licencias basadas en controlador de SnapCenter Standard"](#) .

Sincronización activa de SnapMirror en SnapCenter

La sincronización activa de SnapMirror permite que los servicios empresariales sigan funcionando incluso en caso de una falla total del sitio, permitiendo 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 conmutación por error con la sincronización activa de SnapMirror .

Para obtener más información sobre la sincronización activa de SnapMirror , consulte ["Descripción general de la sincronización activa de SnapMirror"](#) .

Para la sincronización activa de SnapMirror , asegúrese de cumplir con los distintos requisitos de configuración de hardware, software y sistema. Para obtener información, consulte ["Prerrequisitos"](#)

Los complementos compatibles con esta función son el complemento de SnapCenter para SQL Server, el

complemento de SnapCenter para Windows, el complemento de SnapCenter para la base de datos Oracle, el complemento de SnapCenter para la base de datos SAP HANA, el complemento de SnapCenter para Microsoft Exchange Server y el complemento de SnapCenter para Unix.



Para admitir la proximidad del iniciador del host en SnapCenter, su valor, ya sea de origen o de destino, debe configurarse en ONTAP.

Los casos de uso no compatibles con SnapCenter:

- Si convierte las cargas de trabajo de sincronización activa asimétrica de SnapMirror existentes en simétricas al cambiar la política en las relaciones de sincronización activa de SnapMirror de *automatedfailover* a *automatedfailoverduplex* en ONTAP, lo mismo no será compatible en SnapCenter.
- Si hay copias de seguridad de un grupo de recursos (ya protegido en SnapCenter) y luego se cambia la política de almacenamiento en las relaciones de sincronización activa de SnapMirror de *automatedfailover* a *automatedfailoverduplex* en ONTAP, lo mismo no se admite en SnapCenter.

Conceptos clave de la protección de datos

Antes de utilizar SnapCenter, comprenda los conceptos clave de copia de seguridad, clonación y restauración.

Recursos

Los recursos incluyen bases de datos, sistemas de archivos de Windows o recursos compartidos de archivos respaldados o clonados con SnapCenter. Según su entorno, los recursos también podrían ser instancias de base de datos, grupos de disponibilidad de SQL Server, bases de datos Oracle, bases de datos RAC o grupos de aplicaciones personalizados.

Grupo de recursos

Un grupo de recursos es una colección de recursos en un host o clúster, potencialmente de múltiples hosts y clústeres. Las operaciones realizadas en un grupo de recursos se aplican a todos sus recursos según la programación especificada. Puede realizar copias de seguridad programadas o a pedido para recursos individuales o grupos.



Si un host de un grupo de recursos compartidos ingresa al modo de mantenimiento, todas las operaciones programadas para ese grupo se suspenderán en todos los hosts.

Utilice complementos relevantes para realizar copias de seguridad de recursos específicos: complementos de base de datos para bases de datos, complementos de sistema de archivos para sistemas de archivos y SnapCenter Plug-in for VMware vSphere para máquinas virtuales y almacenes de datos.

Políticas

Las políticas especifican la frecuencia de las copias de seguridad, la retención de copias, la replicación, los scripts y otras características de las operaciones de protección de datos.

Se pueden seleccionar una o más políticas al crear un grupo de recursos o al realizar una copia de seguridad a pedido.

Un grupo de recursos define qué necesita protegerse y cuándo debe protegerse en términos de día y hora. Una política describe cómo se llevará a cabo la protección. Por ejemplo, si es necesario realizar una copia de seguridad de todas las bases de datos o sistemas de archivos de un host, se podría crear un grupo de

recursos que incluya todas las bases de datos o sistemas de archivos del host. Luego se podrían asociar dos políticas al grupo de recursos: una política diaria y una política por hora.

Al crear el grupo de recursos y adjuntar las políticas, es posible configurarlo para realizar una copia de seguridad completa diariamente y otra programación para copias de seguridad de registros cada hora.

Se pueden utilizar prescripciones y posdatas personalizadas 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 sobre fallas o advertencias en tareas de protección de datos. Comprender los requisitos para crear estos guiones es fundamental antes de configurar prescriptos y posscriptos.

Uso de prescriptos y posscriptos

Las prescripciones y posdatas personalizadas pueden automatizar sus tareas de protección de datos antes o después del trabajo. Por ejemplo, puede agregar un script para notificarle sobre fallas o advertencias en el trabajo. Antes de configurarlos, asegúrese de comprender los requisitos para estos scripts.

Tipos de scripts admitidos

Los siguientes tipos de scripts son compatibles con Windows:

- Archivos por lotes
- Scripts de PowerShell
- Scripts de Perl

Los siguientes tipos de scripts son compatibles con UNIX:

- Scripts de Perl
- Scripts de Python
- Scripts de shell



Además del shell bash predeterminado, también se admiten otros shells como sh-shell, k-shell y c-shell.

Ruta de script

Todos los prescripts y posscripts que se ejecutan como parte de las operaciones de SnapCenter en sistemas de almacenamiento virtualizados y no virtualizados se ejecutan en el host del complemento.

- Los scripts de Windows deben estar ubicados en el host del complemento.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a `SCRIPTS_PATH`.

- Los scripts de UNIX deben estar ubicados en el host del complemento.



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

Dónde especificar scripts

Los scripts se especifican en las políticas de copia de seguridad. Cuando se inicia un trabajo de respaldo, la

política asocia automáticamente el script con los recursos que se están respaldando. Al crear una política de respaldo, puede especificar los argumentos prescript y postscript.



No se pueden especificar varios scripts.

Tiempos de espera de script

El tiempo de espera está establecido en 60 segundos, de manera predeterminada. Puede modificar el valor del tiempo de espera.

Salida del script

El directorio predeterminado para los archivos de salida de prescripts y postscripts de Windows es Windows\System32.

No existe una ubicación predeterminada para los prescripts y postscripts de UNIX. Puede redirigir el archivo de salida a cualquier ubicación preferida.

Sistemas de almacenamiento y aplicaciones compatibles con SnapCenter

Debe conocer los sistemas de almacenamiento, las aplicaciones y las bases de datos compatibles con SnapCenter.

Sistemas de almacenamiento compatibles

- NetApp ONTAP 9.12.1 y posteriores
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

Admite memoria no volátil expresa (NVMe) a través del Protocolo de control de transporte (TCP).

Para obtener información sobre Amazon FSx for NetApp ONTAP, consulte ["Documentación de Amazon FSx for NetApp ONTAP"](#).

- Sistemas NetApp ASA r2 que ejecutan NetApp ONTAP 9.16.1.

Aplicaciones y bases de datos compatibles

SnapCenter admite la protección de diferentes aplicaciones y bases de datos. Para obtener información detallada sobre las aplicaciones y bases de datos compatibles, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#).

SnapCenter admite la protección de 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 diferentes métodos de autenticación 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 complementos y otro para las operaciones de protección de datos.

Autenticación de Windows

El método de autenticación de Windows se autentica contra Active Directory. Para la autenticación de Windows, Active Directory se configura fuera de SnapCenter. SnapCenter se autentica sin configuración adicional. Necesita una credencial de Windows para agregar hosts, instalar paquetes de complementos y programar trabajos.

Autenticación de dominio no confiable

SnapCenter permite que los usuarios y grupos que pertenecen a dominios no confiables creen credenciales de Windows. Para que la autenticación sea exitosa, debes registrar los dominios no confiables con SnapCenter.

Autenticación de grupo de trabajo local

SnapCenter permite la creación de credenciales de Windows con usuarios y grupos de trabajo locales. La autenticación de Windows para usuarios y grupos de grupos de trabajo locales no ocurre durante la creación de credenciales de Windows, sino que se pospone hasta que se realizan el registro del host y otras operaciones del host.

Autenticación de SQL Server

El método de autenticación SQL se autentica contra una instancia de SQL Server. Esto significa que se debe descubrir una instancia de SQL Server en SnapCenter. Por lo tanto, antes de agregar una credencial SQL, debe agregar un host, instalar paquetes de complementos y actualizar los recursos. Necesita la autenticación de SQL Server para realizar operaciones como programar en SQL Server o descubrir recursos.

Autenticación de Linux

El método de autenticación de Linux se autentica contra un host Linux. Necesita autenticación de Linux durante el paso inicial de agregar el host Linux e instalar el paquete de complementos de SnapCenter para Linux de forma remota desde la GUI de SnapCenter .

Autenticación AIX

El método de autenticación AIX se autentica contra un host AIX. Necesita autenticación AIX durante el paso inicial de agregar el host AIX e instalar el paquete de complementos de SnapCenter para AIX de forma remota desde la GUI de SnapCenter .

Autenticación de base de datos de Oracle

El método de autenticación de base de datos de Oracle se autentica contra una base de datos de Oracle. Necesita una autenticación de base de datos Oracle para realizar operaciones en la base de datos Oracle si la autenticación del sistema operativo (SO) está deshabilitada en el host de la base de datos. Por lo tanto, antes de agregar una credencial de base de datos Oracle, debe crear un usuario Oracle en la base de datos Oracle con privilegios sysdba.

Autenticación de Oracle ASM

El método de autenticación de Oracle ASM se autentica contra una instancia de Oracle Automatic Storage Management (ASM). Se requiere autenticación de Oracle ASM si necesita acceder a una instancia de Oracle ASM y la autenticación del sistema operativo está deshabilitada en el host de la base de datos. Antes de agregar una credencial de Oracle ASM, cree un usuario de Oracle con privilegios de sistema en la instancia de ASM.

Autenticación del catálogo RMAN

El método de autenticación del catálogo RMAN se autentica contra la base de datos del catálogo de Oracle Recovery Manager (RMAN). Si ha configurado un mecanismo de catálogo externo y ha registrado su base de datos en la base de datos del catálogo, debe agregar la autenticación del catálogo 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 ASA r2"](#)

SnapCenter aprovecha las API REST para realizar todas las operaciones en sistemas ASA r2, que no admiten ZAPI.

Operaciones compatibles con SnapCenter para sistemas ASA r2

- Creación de copias de seguridad primarias de aplicaciones a través de VMDK
- Transferencia de instantáneas del grupo de consistencia al sistema de almacenamiento secundario
- Restaurar las copias de seguridad de los sistemas de almacenamiento primario y secundario al host original o al host 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

SnapCenter puede descubrir o crear grupos de consistencia ONTAP . También puede aprovisionar e inicializar relaciones de SnapMirror con el clúster de destino para protección secundaria.

Para obtener información sobre 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

- Mapeo de dispositivos sin procesar (RDM)
- Volúmenes de aplicaciones para Oracle
- SAP HANA NDV

- Bóveda de bloqueo
- Instantáneas a prueba de manipulaciones
- Volúmenes de FlexGroup
- Grupo de consistencia jerárquica
- Migración de sistemas de almacenamiento ASA, AFF o FAS a sistemas de almacenamiento ASA r2
- Protección de bases de datos que tienen una combinación de recursos ASA, AFF o FAS y recursos ASA r2
- Cambio de nombre de instantáneas
- Aprovisionamiento secundario del directorio de registro del host del complemento SQL

Inicio rápido del SnapCenter software

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

1

Prepárese para instalar SnapCenter Server

Debe asegurarse de que se cumplan todos los requisitos para instalar SnapCenter Server.

- ["Requisitos"](#)
- ["Regístrese para acceder al SnapCenter software"](#)
- ["Habilitar la autenticación multifactor"](#)

2

Instalar SnapCenter Server

El servidor SnapCenter se puede instalar en hosts Windows o Linux. Descargue el paquete de instalación de SnapCenter Server desde ["Sitio de soporte de NetApp"](#) y ejecutar el instalador.

- ["Instalar el servidor SnapCenter en Windows"](#)
- ["Instalar SnapCenter Server en Linux"](#)

3

Configurar el servidor SnapCenter

Después de instalar SnapCenter Server, debe configurarlo según su entorno.

4

Instale el complemento para su aplicación

Asegúrese de que se cumplan todos los requisitos para instalar el complemento específico de la aplicación en uso y luego proceda con la instalación del complemento correspondiente.

5

Proteja su aplicación

Después de instalar exitosamente SnapCenter Server y los complementos necesarios, puede iniciar la creación de copias de seguridad de la aplicación. Estas copias de seguridad se pueden utilizar posteriormente

para fines de restauración y clonación cuando sea necesario.

Instalar y configurar SnapCenter Server

Prepárese para instalar el servidor SnapCenter

Requisitos para instalar SnapCenter Server

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

Requisitos de dominio y grupo de trabajo para el host de Windows

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

El usuario con privilegios de administrador puede instalar el servidor SnapCenter .

- Dominio de Active Directory: debe utilizar un usuario de dominio con derechos de administrador local. El usuario del dominio debe ser miembro del grupo de administradores locales en el host de Windows.
- Grupos de trabajo: debe utilizar una cuenta local que tenga derechos de administrador local.

Si bien se admiten las confianzas de dominio, los bosques multidominio y las confianzas entre dominios, no se admiten los dominios entre bosques. La documentación de Microsoft sobre dominios y confianzas de Active Directory contiene más información.



Después de instalar SnapCenter Server, no debe cambiar el dominio en el que se encuentra el host de SnapCenter . Si elimina el host de SnapCenter Server del dominio en el que se encontraba cuando se instaló SnapCenter Server y luego intenta desinstalar SnapCenter Server, la operación de desinstalación falla.

Requisitos de espacio y tamaño

Debe estar familiarizado con los requisitos de espacio y tamaño.

Artículo	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 https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT [Herramienta de matriz de interoperabilidad de NetApp] .	• Red Hat Enterprise Linux (RHEL) 8 y 9 • Servidor empresarial SUSE Linux (SLES) 15 Para obtener la información más reciente sobre las versiones compatibles, consulte https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT [Herramienta de matriz de interoperabilidad de NetApp] .

Artículo	Requisitos del host de Windows	Requisitos del host Linux
Cantidad mínima de CPU	4 núcleos	4 núcleos
RAM mínima	8 GB  El grupo de búfer del servidor MySQL utiliza el 20 por ciento de la RAM total.	8 GB
Espacio mínimo en el disco duro para el software y los registros de SnapCenter Server	7 GB  Si tiene el repositorio de SnapCenter en la misma unidad donde está instalado SnapCenter Server, se recomienda tener 15 GB.	15 GB
Espacio mínimo en el disco duro para el repositorio de SnapCenter	8 GB  NOTA: Si tiene el servidor SnapCenter en la misma unidad donde está instalado el repositorio de SnapCenter , se recomienda tener 15 GB.	No aplicable

Artículo	Requisitos del host de Windows	Requisitos del host Linux
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell 7.4.2 o posterior Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en 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 (Módulos de autenticación conectables) es una herramienta de seguridad del sistema que permite a los administradores del sistema establecer políticas de autenticación sin tener que volver a compilar los programas que realizan la autenticación.



ASP.NET Core necesita IIS_IUSRS para acceder al sistema de archivos temporal en SnapCenter Server en Windows.

Requisitos del host SAN

SnapCenter no incluye utilidades de host ni un DSM. Si el host de SnapCenter es parte de un entorno SAN (FC/iSCSI), es posible que deba instalar y configurar software adicional en el host del servidor SnapCenter .

- Utilidades de host: las utilidades de host admiten FC e iSCSI y le permiten utilizar MPIO en sus servidores Windows. ["Más información"](#) .
- Microsoft DSM para Windows MPIO: este software funciona con controladores MPIO de Windows para administrar múltiples rutas entre NetApp y computadoras host de Windows. Se requiere un DSM para configuraciones de alta disponibilidad.



Si estaba utilizando ONTAP DSM, debería migrar a Microsoft DSM. Para obtener más información, consulte ["Cómo migrar de ONTAP DSM a Microsoft DSM"](#) .

Requisitos del navegador

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

Requisitos del puerto

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

- Las aplicaciones no pueden compartir un puerto.

- Para puertos personalizables, puede seleccionar un puerto personalizado durante la instalación si no desea utilizar el puerto predeterminado.
- Para puertos fijos, debe aceptar el número de puerto predeterminado.
- Cortafuegos
 - Los firewalls, servidores proxy u otros dispositivos de red no deben interferir con las conexiones.
 - Si especifica un puerto personalizado al instalar SnapCenter , debe agregar una regla de firewall en el host del complemento para ese puerto para el Loader de complementos de SnapCenter .

La siguiente tabla enumera los diferentes puertos y sus valores predeterminados.

Nombre del puerto	Números de puerto	Protocolo	Dirección	Descripción
Puerto de SnapCenter	8146	HTTPS	Bidireccional	Este puerto se utiliza para la comunicación entre el cliente de SnapCenter (el usuario de SnapCenter) y el servidor de SnapCenter y también se utiliza para la comunicación desde los hosts del complemento al servidor de SnapCenter . Puede personalizar el número de puerto.
Puerto de comunicación SMCORE de SnapCenter	8145	HTTPS	Bidireccional	Este puerto se utiliza para la comunicación entre el servidor SnapCenter y los hosts donde están instalados los complementos de SnapCenter . Puede personalizar el número de puerto.

Nombre del 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 complementos administrados dentro del host del servidor SnapCenter de manera centralizada. Puede personalizar el número de puerto.
Puerto RabbitMQ	5672	TCP		Este es el puerto predeterminado que RabbitMQ escucha y se utiliza para la comunicación del modelo de publicador-suscriptor entre el servicio Scheduler 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. "Más información"

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

Nombre del puerto	Números de puerto	Protocolo	Dirección	Descripción
Complemento de SnapCenter para bases de datos de Exchange	909			El complemento para Windows utiliza el puerto NET.TCP predeterminado 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 ONTAP o SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidireccional	El puerto es utilizado por SAL (capa de abstracción de almacenamiento) para la comunicación entre el host que ejecuta SnapCenter Server y SVM. Actualmente, el puerto también lo utiliza el SAL en los hosts del complemento SnapCenter para Windows para la comunicación entre el host del complemento SnapCenter y SVM.

Nombre del puerto	Números de puerto	Protocolo	Dirección	Descripción
Complemento de SnapCenter para la base de datos SAP HANA	3instance_number13 3instance_number15	- HTTPS - HTTP	Bidireccional	Para un contenedor de base de datos multiinquilino (MDC) de un solo inquilino, el número de puerto termina con 13; para un contenedor que no es MDC, el número de puerto termina con 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 complemento PostgreSQL con el clúster PostgreSQL. Puede personalizar el número de puerto.

Regístrese para acceder al SnapCenter software

Debe registrarse para acceder al SnapCenter software 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 a la ID de correo electrónico corporativa.
- Si usa Azure NetApp Files, debe tener el identificador de suscripción de Azure.
- Si está utilizando Amazon FSx for 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 demorar hasta un día para confirmar y actualizar la nueva cuenta del Sitio de soporte de NetApp (NSS) a acceso **completo** desde acceso **de invitado**.

Pasos

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

- a. Seleccione **Cliente de NetApp /Usuario final**.
- b. En el campo NÚMERO DE SERIE, ingrese el ID de suscripción de Azure si usa Azure NetApp Files o el ID del sistema de archivos si usa Amazon FSx for NetApp ONTAP.



Puedes generar un ticket en <https://mysupport.netapp.com/site/help> Si enfrenta algún problema durante el registro o para conocer el estado.

Autenticación multifactor (MFA)

Administrar 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 en el servidor de SnapCenter .

Habilitar la autenticación multifactor (MFA)

Puede habilitar la funcionalidad MFA para SnapCenter Server mediante 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 ciertas configuraciones de AD FS, SnapCenter podría requerir autenticación de usuario por razones de seguridad dependiendo de la persistencia de la sesión de AD FS.
- La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name` . Alternativamente, también puedes ver "[Guía de referencia de cmdlets del software SnapCenter](#)" .

Antes de empezar

- El Servicio de federación de Active Directory (AD FS) de Windows debe estar en funcionamiento en el dominio respectivo.
- Debe tener un servicio de autenticación multifactor compatible con AD FS, como Azure MFA, Cisco Duo, etc.
- La marca de tiempo de SnapCenter y del servidor AD FS deben ser las mismas independientemente de la zona horaria.
- Obtenga y configure el certificado CA autorizado para SnapCenter Server.

El certificado CA es obligatorio por las siguientes razones:

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

Para obtener información sobre el certificado CA, consulte "[Generar archivo CSR de certificado de CA](#)" .

Pasos

1. Conectarse al host de Servicios de federación de Active Directory (AD FS).

2. Descargar el archivo de metadatos de federación de AD FS desde "<https://<host Nombre de dominio completo>/FederationMetadata/2007-06/FederationMetadata.xml>".
3. Copie el archivo descargado en SnapCenter Server para habilitar la función MFA.
4. Inicie sesión en SnapCenter Server como usuario administrador de SnapCenter a través de PowerShell.
5. Mediante la sesión de PowerShell, genere el archivo de metadatos MFA de SnapCenter mediante el cmdlet *New-SmMultiFactorAuthenticationMetadata -path*.

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

6. Copie el archivo generado en el host de AD FS para configurar SnapCenter como entidad cliente.
7. Habilite MFA para SnapCenter Server mediante el *Set-SmMultiFactorAuthentication* cmdlet.
8. (Opcional) Verifique el estado y la configuración de MFA mediante *Get-SmMultiFactorAuthentication* cmdlet.
9. Vaya a la consola de administración de Microsoft (MMC) y realice los siguientes pasos:
 - a. Haga clic en **Archivo > Agregar o quitar complemento**.
 - b. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
 - c. En la ventana del complemento Certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
 - d. Haga clic en **Raíz de consola > Certificados – Equipo local > Personal > Certificados**.
 - e. Haga clic con el botón derecho en el certificado de CA vinculado a SnapCenter y luego 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 del objeto, ingrese 'IIS_IUSRS' y haga clic en **Verificar nombres** y haga clic en **Aceptar**.

Si la comprobación es exitosa, haga clic en **Aceptar**.

10. En el host de AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
 - a. Haga clic derecho en **Confianzas de usuario autenticado > Agregar confianza de usuario autenticado > Iniciar**.
 - b. Seleccione la segunda opción y busque el archivo de metadatos MFA de SnapCenter y haga clic en **Siguiente**.
 - c. Especifique un nombre para mostrar y haga clic en **Siguiente**.
 - d. Seleccione una política de control de acceso según sea necesario y haga clic en **Siguiente**.
 - e. Seleccione la configuración en la siguiente pestaña para establecerla como predeterminada.
 - f. Haga clic en **Finalizar**.

SnapCenter ahora se refleja como una parte confiable con el nombre para mostrar proporcionado.

11. Seleccione el nombre y realice los siguientes pasos:

- a. Haga clic en **Editar política 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 **User-Principal-Name** y el tipo de reclamo saliente como **Name-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 importaron correctamente.
 - a. Haga clic con el botón derecho en la cuenta de confianza del usuario confiante y seleccione **Propiedades**.
 - b. Asegúrese de que los campos Puntos finales, Identificadores y Firma estén completos.
14. Cierre todas las pestañas del navegador y vuelva a abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

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

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

Actualizar metadatos de MFA de AD FS

Debe actualizar los metadatos de MFA de AD FS en SnapCenter siempre que haya alguna modificación en el servidor de AD FS, como una actualización, una renovación del certificado de CA, una recuperación ante desastres, etc.

Pasos

1. Descargar el archivo de metadatos de federación de AD FS desde "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. Copie el archivo descargado en SnapCenter Server 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 abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Actualizar metadatos de MFA de SnapCenter

Debe actualizar los metadatos de MFA de SnapCenter en AD FS siempre que haya alguna modificación en el servidor ADFS, como reparación, renovación de certificado de CA, DR, etc.

Pasos

1. En el host de AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
 - a. Seleccione **Fideicomisos de terceros que confían**.
 - b. Haga clic con el botón derecho en la relación de confianza creada para SnapCenter y seleccione **Eliminar**.

Se mostrará el nombre definido por el usuario de la parte confiable.

- c. Habilitar la autenticación multifactor (MFA).

Ver "[Habilitar la autenticación multifactor](#)".

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

Deshabilitar la autenticación multifactor (MFA)

Pasos

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

Administrar la autenticación multifactor (MFA) mediante Rest API, PowerShell y SCCLI

El inicio de sesión MFA es compatible con el navegador, la API REST, PowerShell y SCCLI. MFA se admite a través de un administrador de identidad AD FS. Puede habilitar MFA, deshabilitar MFA y configurar MFA desde GUI, API REST, PowerShell y SCCLI.

Configurar AD FS como OAuth/OIDC

Configurar AD FS mediante el asistente de GUI de Windows

1. Vaya a **Panel del administrador del servidor > Herramientas > Administración de ADFS**.
2. Vaya a **ADFS > Grupos de aplicaciones**.
 - a. Haga clic derecho en **Grupos de aplicaciones**.
 - b. Seleccione **Agregar grupo de aplicaciones** e ingrese **Nombre de la aplicación**.
 - c. Seleccione **Aplicación de servidor**.
 - d. Haga clic en **Siguiente**.
3. Copiar **Identificador de cliente**.

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

4. Seleccione **Generar secreto compartido**.

Copiar el valor secreto. Éste es el secreto del cliente. .. Haga clic en **Siguiente**.

5. En la página **Resumen**, haga clic en **Siguiente**.
 - a. En la página **Completa**, haga clic en **Cerrar**.

6. Haga clic derecho en el **Grupo de aplicaciones** recién agregado y seleccione **Propiedades**.
7. Seleccione **Agregar aplicación** en Propiedades de la aplicación.
8. Haga clic en **Agregar aplicación**.

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

9. En la página Configurar API web, ingrese la URL del servidor SnapCenter y el identificador de cliente creado 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**, seleccione la política de control según sus requisitos (por ejemplo, Permitir a todos y requerir MFA) y haga clic en **Siguiente**.
11. En la página **Configurar permiso de aplicación**, de manera predeterminada se selecciona openid como alcance; haga clic en **Siguiente**.
12. En la página **Resumen**, haga clic en **Siguiente**.

En la página **Completa**, haga clic en **Cerrar**.

13. En la página **Propiedades de la aplicación de muestra**, haga clic en **Aceptar**.
14. Token JWT emitido por un servidor de autorización (AD FS) y destinado a ser consumido por el recurso.

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

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

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

16. Abra la herramienta **Administración de AD FS** ubicada en el menú **Herramientas** 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. Ir a la pestaña Reglas de transformación de emisión

17. Haga clic en **Agregar regla**.
 - a. Seleccione **Enviar atributos LDAP como reclamos** en el menú desplegable Plantilla de regla de reclamo.
 - b. Haga clic en **Siguiente**.
18. Introduzca el nombre de la **regla de reclamación**.
 - a. Seleccione **Active Directory** en el menú desplegable Almacén de atributos.
 - b. Seleccione **Nombre principal del usuario** en el menú desplegable **Atributo LDAP** y **UPN** en el menú desplegable **Tipo de reclamación saliente**.
 - c. Haga clic en **Finalizar**.

Crear un grupo de aplicaciones mediante comandos de PowerShell

Puede crear el grupo de aplicaciones, la API web y agregar el alcance y las notificaciones mediante comandos de PowerShell. Estos comandos están disponibles en formato de script automatizado. Para obtener más información, consulte el <enlace al artículo de Knowledge Base>.

1. Cree el nuevo grupo de aplicaciones en AD FS utilizando el siguiente comando.

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

`ClientRoleIdentifier` nombre de su grupo de aplicaciones

`redirectURL` URL válida para redirección después de la autorización

2. Cree la aplicación de servidor 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 del cliente y el secreto del cliente de la salida de los siguientes comandos porque solo se muestran 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. Nombre la aplicación de API web y defina sus reglas de transformación de emisión utilizando un archivo externo.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Actualizar el tiempo de expiración del token de acceso

Puede actualizar el tiempo de expiración del token de acceso mediante el comando de 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 expiración de un token de acceso es de 60 minutos. Este tiempo mínimo de expiración es suficiente y escalable. Debe proporcionar valor suficiente para evitar que se realicen trabajos críticos para el negocio.

Paso

Para actualizar el tiempo de vencimiento del token de acceso para un grupo de aplicaciones WebApi, use el siguiente comando en el servidor AD FS.

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

Obtener el token portador de AD FS

Debe completar los parámetros mencionados a continuación en cualquier cliente REST (como Postman) y le solicitará que complete las credenciales del usuario. Además, debes ingresar la autenticación de segundo factor (algo que tienes y algo que eres) para obtener el token de portador.

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

Campo	Valor

Tipo de subvención	Código de autorización
URL de devolución de llamada	Ingrese la URL base de su aplicación si no tiene una URL de devolución de llamada.
URL de autorización	[nombre-de-dominio-adfs]/adfs/oauth2/authorize
URL del token de acceso	[nombre-de-dominio-adfs]/adfs/oauth2/token
ID de cliente	Introduzca el ID del cliente de AD FS
Secreto del cliente	Ingrese el secreto del cliente de AD FS
Alcance	OpenID
Autenticación del cliente	Enviar como encabezado de autenticación básico
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.

Configurar MFA en SnapCenter Server mediante PowerShell, SCCLI y API REST

Puede configurar MFA en SnapCenter Server mediante PowerShell, SCCLI y API REST.

Autenticación CLI de MFA de SnapCenter

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

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

Después de ejecutar el cmdlet anterior, se crea una sesión para que el usuario respectivo ejecute otros cmdlets de SnapCenter .

Autenticación de API Rest de MFA de SnapCenter

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

Flujo de trabajo de la API Rest de MFA

Cuando MFA está configurado con AD FS, debe autenticarse usando un token de acceso (portador) para acceder a la aplicación SnapCenter mediante cualquier API Rest.

Acerca de esta tarea

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

Pasos

Para autenticarse a través de AD FS MFA

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

Cuando presione el botón para obtener un token de acceso para una aplicación, será redirigido a la página SSO de AD FS donde deberá 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 tener el formato usuario@dominio o dominio\usuario.

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

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

6. En la API Rest, debes pasar el token de acceso y el nombre del 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. Utilizando el nombre de usuario y el nombre del rol, SnapCenter autentica al usuario para una ejecución de API.

Si la autenticación tiene éxito, SnapCenter devuelve el resultado; de lo contrario, se muestra un mensaje de error.

Habilitar o deshabilitar la funcionalidad MFA de SnapCenter para API Rest, CLI y GUI

GUI

Pasos

1. Inicie sesión en el servidor SnapCenter como administrador de SnapCenter .
2. Haga clic en **Configuración > Configuración global > Configuración de autenticación multifactor (MFA)**

3. Seleccione la interfaz (GUI/RST API/CLI) para habilitar o deshabilitar el inicio de sesión MFA.

Interfaz de PowerShell

Pasos

1. Ejecute los comandos de PowerShell o CLI para habilitar MFA para GUI, API Rest, PowerShell y SCCLI.

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

El parámetro de ruta especifica la ubicación del archivo XML de metadatos de AD FS MFA.

Habilita MFA para la GUI de SnapCenter , la API Rest, PowerShell y SCCLI configurados con la ruta de archivo de metadatos de AD FS especificada.

2. Verifique el estado y la configuración de MFA mediante el `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 de publicación para habilitar MFA para GUI, API Rest, PowerShell y SCCLI.

Parámetro	Valor
URL solicitada	/api/4.9/configuraciones/authenticación multifactor
Método HTTP	Correo
Cuerpo de la solicitud	{ "IsGuiMFAEnabled": falso, "IsRestApiMFAEnabled": verdadero, "IsCliMFAEnabled": falso, "ADFSConfigFilePath": "C:\ADFS_metadata\abc.xml" }
Cuerpo de respuesta	{ "Configuración MFAC": { "IsGuiMFAEnabled": falso, "RutaDeArchivoDeConfigADFS": "C:\ADFS_metadata\abc.xml", "RutaDeArchivoDeConfigSC": nulo, "IsRestApiMFAEnabled": verdadero, "IsCliMFAEnabled": falso, "NombreDeHostADFS": "win-adfs-sc49.winscedom2.com" } }

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

Parámetro	Valor
URL solicitada	/api/4.9/configuraciones/autenticación multifactor
Método HTTP	Conseguir
Cuerpo de respuesta	{ "Configuración MFAC": { "IsGuiMFAEnabled": falso, "RutaDeArchivoDeConfigADFS": "C:\\ADFS_metadata\\abc.xml", "RutaDeArchivoDeConfigSC": nulo, "IsRestApiMFAEnabled": verdadero, "IsCliMFAEnabled": falso, "NombreDeHostADFS": "win-adfs-sc49.winscedom2.com" } }

Instalar el servidor SnapCenter

Instalar el servidor SnapCenter en el host de Windows

Puede ejecutar el ejecutable del instalador de SnapCenter Server para instalar SnapCenter Server.

Opcionalmente, puede realizar varios 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 del servidor SnapCenter debe estar actualizado con las actualizaciones de Windows y sin reinicios del sistema pendientes.
- Debería asegurarse de que MySQL Server no esté instalado en el host donde planea instalar SnapCenter Server.
- Deberías haber habilitado la depuración del instalador de Windows.

Consulte el sitio web de Microsoft para obtener información sobre cómo habilitar "[Registro del instalador de Windows](#)".



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

Pasos

1. Descargue el paquete de instalación de SnapCenter Server desde "[Sitio de soporte de NetApp](#)".
2. Inicie la instalación de SnapCenter Server haciendo doble clic en el archivo .exe descargado.

Después de iniciar la instalación, se realizan todas las comprobaciones previas y, si no se cumplen los requisitos mínimos, se muestran mensajes de error o advertencia correspondientes.

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

3. Revise los valores previamente completados necesarios para la instalación de SnapCenter Server y modifíquelos si es necesario.

No es necesario especificar la contraseña para la base de datos del repositorio del servidor MySQL. Durante la instalación de SnapCenter Server, 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 algún valor que no es válido, se mostrarán los mensajes de error correspondientes. Debe volver a ingresar los valores y luego iniciar la instalación.



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

Sin embargo, si hace clic en **Cancelar** cuando se realizan las operaciones "Reinicio del sitio de SnapCenter Server" o "Esperando a que se inicie SnapCenter Server", la instalación continuará sin cancelar la operación.

Los archivos de registro siempre se enumeran (el más antiguo primero) en la carpeta %temp% del usuario administrador. Si desea redirigir las ubicaciones de los registros, inicie la instalación de SnapCenter Server 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 y roles de Windows en su host de Windows durante la instalación. Estos podrían ser de interés para solucionar problemas y realizar mantenimiento al sistema host.

Categoría	Característica
Servidor web	• Servicios de información de Internet • Servicios de la World Wide Web • Características comunes de HTTP ◦ Documento predeterminado ◦ Navegación por directorios ◦ Errores HTTP ◦ Redirección HTTP ◦ Contenido estático ◦ Publicación WebDAV • Salud y Diagnóstico ◦ Registro personalizado ◦ Registro HTTP ◦ Herramientas de registro ◦ Monitor de solicitudes ◦ Rastreo • Características de rendimiento ◦ Compresión de contenido estático • Seguridad ◦ Seguridad IP ◦ Autenticación básica ◦ Soporte centralizado de certificados SSL ◦ Autenticación mediante mapeo de certificados de cliente ◦ Autenticación mediante asignación de certificados de cliente de IIS ◦ Restricciones de IP y dominio ◦ Filtrado de solicitudes ◦ Autorización de URL ◦ Autenticación de Windows • Características del desarrollo de aplicaciones ◦ Extensibilidad de .NET 4.5 ◦ Inicialización de la aplicación ◦ Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) ◦ Incluye del lado del servidor ◦ Protocolo WebSocket Herramientas de gestión Consola de administración de IIS

Categoría	Característica
Scripts y herramientas de administración de IIS	• Servicio de administración de IIS • Herramientas de gestión web
Características de .NET Framework 8.0.12	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • Activación HTTP de Windows Communication Foundation (WCF)⁴⁵ ◦ Activación de TCP ◦ Activación HTTP Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conectividad a Internet" .
Cola de mensajes	• Servicios de cola de mensajes  Asegúrese de que ninguna otra aplicación utilice el servicio MSMQ que SnapCenter crea y administra. • RabbitMQ • Erlang
Servicio de activación de procesos de Windows	• Modelo de proceso
API de configuración	Todo

Instalar el servidor SnapCenter en el host Linux

Puede ejecutar el ejecutable del instalador de SnapCenter Server para instalar SnapCenter Server.

Antes de empezar

- Si desea instalar SnapCenter Server utilizando un usuario que no sea root y que no tenga privilegios suficientes para instalar SnapCenter, obtenga el archivo de suma de comprobación de sudoers del sitio de soporte de NetApp . Debe utilizar el archivo de suma de comprobación apropiado según la versión de Linux.
- Si el paquete sudo no está disponible en SUSE Linux, instálelo para evitar errores de autenticación.
- Para SUSE Linux, configure el nombre de host para evitar errores de instalación.
- Compruebe el estado seguro de Linux ejecutando el comando `sestatus` . Si el *estado de SELinux* está "habilitado" y el *modo actual* está "aplicando", 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 donde tiene permiso de lectura y escritura:

- `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

Si el comando devuelve "no hay nada que hacer", vuelva a ejecutarlo 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 utilizada para el directorio PID de MySQL es */var/opt/mysqld*. Ejecute los siguientes comandos para configurar 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 de datos MySQL es */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Ejecute los siguientes comandos para establecer los permisos para el directorio de datos 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 SnapCenter Server se instala en el host Linux, se instalan servicios de terceros como MySQL, RabbitMq y Erlang. No debes desinstalarlos.
- El servidor SnapCenter instalado en el host Linux no admite:
 - Alta disponibilidad
 - complementos de Windows
 - Active Directory (solo admite usuarios locales, tanto usuarios root como no root con credenciales)
 - Autenticación basada en clave para iniciar sesión en SnapCenter
- Durante la instalación del entorno de ejecución de .NET, si la instalación no logra resolver las dependencias de la biblioteca *libicu*, instale *libicu* ejecutando el comando: `yum install -y libicu`
- Si la instalación de SnapCenter Server falla debido a la falta de disponibilidad de *Perl*, instale *Perl* ejecutando el comando: `yum install -y perl`

Pasos

1. Descargue lo siguiente desde ["Sitio de soporte de NetApp"](#) al directorio `/home`.
 - Paquete de instalación de SnapCenter Server: **snapcenter-linux-server-(el8/el9/sles15).bin**
 - Archivo de clave pública - **snapcenter_public_key.pub**
 - Archivo de firma respectivo: **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. Validar 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 por parte de usuarios no root, agregue el contenido de visudo especificado en **snapcenter_server_checksum_(el8/el9/sles15).txt** disponible junto con el instalador .bin.
4. Asignar 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 SnapCenter Server.

Si quieres realizar...	Haz esto...
Instalación interactiva	<pre>./snapcenter-linux-server-(el8/el9/sles15).bin</pre> Se le pedirá que ingrese los siguientes detalles: • El puerto externo de la aplicación web que se utiliza para acceder a SnapCenter Server fuera del host Linux. El valor predeterminado es 8146. • El usuario de SnapCenter Server que instalará SnapCenter Server. • El directorio de instalación donde se instalarán los paquetes.

Si quieres realizar...	Haz esto...
Instalación no interactiva	<pre> sudo ./snapcenter-linux-server- (e18/e19/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> </pre> Ejemplo: <code>sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log</code> Los registros se almacenarán en <code>/var/opt/snapcenter/logs</code>. Parámetros que se deben pasar para instalar SnapCenter Server: • DWEBAPP_EXTERNAL_PORT: Puerto externo de la aplicación web que se utiliza para acceder a SnapCenter Server fuera del host Linux. El valor predeterminado es 8146. • DWEBAPP_INTERNAL_PORT: Puerto interno de la aplicación web que se utiliza para acceder a SnapCenter Server 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 de SnapCenter Server que instalará SnapCenter Server. Para <code>DSNAPCENTER_SERVER_USER</code>, el valor predeterminado es el usuario que ejecuta el instalador. • DUSER_INSTALL_DIR: Directorio de instalación donde se instalarán los paquetes. Para <code>DUSER_INSTALL_DIR</code>, el directorio de instalación predeterminado es <code>/opt</code>. • 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

¿Que sigue?

- Si el estado *SELinux* está "habilitado" y el *modo actual* está "aplicando", el servicio **nginx** no se puede iniciar. Debes ejecutar los siguientes comandos:
 - a. Ir al directorio de inicio.
 - b. Ejecute el comando: `journalctl -x|grep nginx`.
 - c. Si el puerto interno de la aplicación web (8147) no puede escuchar, ejecute los siguientes comandos:
 - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
 - `semodule -i my-nginx.pp`
 - d. Correr `setsebool -P httpd_can_network_connect`.
- DSELINUX: Si el estado *SELinux* está "habilitado", el *modo actual* está "aplicando" 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 distinto de 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

Registrarse en SnapCenter

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

Pasos

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

Inicie sesión en SnapCenter mediante la autorización RBAC

SnapCenter admite el control de acceso basado en roles (RBAC). El administrador de SnapCenter asigna roles y recursos a través de SnapCenter RBAC a un usuario en un grupo de trabajo o directorio activo, o a grupos en el directorio activo. El usuario 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 el Administrador de servidor de Windows.
- Si desea utilizar Internet Explorer como navegador para iniciar sesión en el servidor SnapCenter , debe asegurarse de que el Modo protegido en Internet Explorer esté deshabilitado.
- Si SnapCenter Server está instalado en un host Linux, debe iniciar sesión con la cuenta de usuario que se utilizó para instalar SnapCenter Server.

Acerca de esta tarea

Durante la instalación, el asistente de instalación de SnapCenter Server crea un acceso directo y lo coloca en el escritorio y en el menú Inicio del host donde está instalado SnapCenter . Además, al final de la instalación, el asistente de instalación muestra la URL de SnapCenter basada en la información que proporcionó durante la instalación, que puede copiar si desea iniciar sesión desde un sistema remoto.



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

Mejores prácticas: Por razones de seguridad, se recomienda que no habilite su navegador para guardar su contraseña de SnapCenter .

La URL de la GUI predeterminada es una conexión segura al puerto predeterminado 8146 en el servidor donde está instalado SnapCenter Server (<https://server:8146>). Si proporcionó un puerto de servidor diferente durante la instalación de SnapCenter , se utilizará ese puerto en su lugar.

Para una 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 cuando navega a https://Virtual_Cluster_IP_or_FQDN:8146 en Internet Explorer (IE), debe agregar la dirección IP o el FQDN del clúster virtual como un sitio confiable en IE en cada host de complemento, o debe deshabilitar la seguridad mejorada de IE en cada host de complemento. Para obtener más información, consulte ["No se puede acceder a la dirección IP del clúster desde la red externa"](#) .

Además de utilizar la GUI de SnapCenter , puede usar cmdlets de PowerShell para crear scripts para realizar operaciones de configuración, copia de seguridad y restauración. Es posible que algunos cmdlets hayan cambiado con cada versión de SnapCenter . El ["Guía de referencia de cmdlets del software SnapCenter"](#) Tiene los detalles.



Si está iniciando sesión en SnapCenter por primera vez, debe iniciar sesión con las credenciales que proporcionó durante el proceso de instalación.

Pasos

1. Inicie SnapCenter desde el acceso directo ubicado en el escritorio del host local, o desde la URL proporcionada al final de la instalación, o desde la URL proporcionada por su administrador de SnapCenter .
2. Introduzca las credenciales del usuario.

Para especificar lo siguiente...	Utilice uno de estos formatos...
Administrador de dominio	• NetBIOS\Nombre de usuario • Sufijo UserName@UPN Por ejemplo, nombreusuario@netapp.com • FQDN de dominio\Nombre de usuario
Administrador local	Nombre de usuario

3. Si tiene asignado más de un rol, en el cuadro Rol, seleccione el rol que desea utilizar para esta sesión de inicio de sesión.

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

Resultado

Se muestra la página del Panel de Control.

Si el registro falla con el error de que no se puede acceder al sitio, debe asignar el certificado SSL a SnapCenter. ["Más información"](#)

Después de terminar

Después de iniciar sesión en SnapCenter Server como usuario 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 los roles para los usuarios en dominios que no son de confianza. ["Más información"](#) .

Si desea agregar el host del complemento en SnapCenter ejecutándose en el host 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 un acceso directo para SnapCenter PowerShell en el escritorio. Puede acceder directamente a los cmdlets de PowerShell de SnapCenter mediante el acceso directo.

Inicie sesión en SnapCenter mediante la autenticación multifactor (MFA)

SnapCenter Server admite MFA para cuentas de dominio, que son parte del directorio activo.

Antes de empezar

Deberías haber habilitado MFA. Para obtener información sobre cómo habilitar MFA, consulte ["Habilitar la autenticación multifactor"](#)

Acerca de esta tarea

- Solo se admite FQDN
- Los usuarios de grupos de trabajo y dominios cruzados no pueden iniciar sesión mediante MFA

Pasos

1. Inicie SnapCenter desde el acceso directo ubicado en el escritorio del host local, o desde la URL proporcionada al final de la instalación, o desde la URL proporcionada por su administrador de SnapCenter .
2. En la página de inicio de sesión de AD FS, ingrese el nombre de usuario y la contraseña.

Cuando se muestra el mensaje de error de nombre de usuario o contraseña no válidos en la página de AD FS, debe verificar lo siguiente:

- Si el nombre de usuario o la contraseña son válidos

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

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

Modificar el tiempo de espera de la sesión GUI predeterminada de SnapCenter

Puede modificar el período de tiempo de espera de la sesión de la GUI de SnapCenter para que sea menor o mayor que el período de tiempo de espera predeterminado de 20 minutos.

Como característica de seguridad, después de un período predeterminado de 15 minutos de inactividad, SnapCenter le advierte que se cerrará su sesión de GUI en 5 minutos. De forma predeterminada, SnapCenter cierra la sesión de la GUI después de 20 minutos de inactividad y debe iniciar sesión nuevamente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración > Configuración global**.
2. En la página Configuración global, haga clic en **Configuración**.
3. En el campo Tiempo de espera de la sesión, ingrese el nuevo tiempo de espera de la sesión en minutos y luego haga clic en **Guardar**.

Proteja el servidor web de SnapCenter deshabilitando SSL 3.0

Por motivos de seguridad, debe deshabilitar el protocolo Secure Socket Layer (SSL) 3.0 en Microsoft IIS si está habilitado en su servidor web SnapCenter .

Existen fallas en el protocolo SSL 3.0 que un atacante puede utilizar para provocar fallas de conexión o realizar ataques de intermediario 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 de SnapCenter , haga clic en **Inicio > Ejecutar** y luego ingrese regedit.
2. En el Editor del Registro, navegue a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\`.
 - Si la clave del servidor ya existe:
 - i. Seleccione el DWORD habilitado y luego haga clic en **Editar > Modificar**.
 - ii. Cambie el valor a 0 y luego haga clic en **Aceptar**.

- Si la clave del servidor no existe:
 - i. Haga clic en **Editar > Nuevo > Clave** y luego nombre la clave Servidor.
 - ii. Con la nueva clave de servidor seleccionada, haga clic en **Editar > Nuevo > DWORD**.
 - iii. Nombre el nuevo DWORD Habilitado y luego ingrese 0 como valor.

3. Cerrar el Editor del Registro.

Configurar el servidor SnapCenter

Agregar y aprovisionar el sistema de almacenamiento

Añadir sistemas de almacenamiento

Debe configurar el sistema de almacenamiento que le otorga a SnapCenter acceso al almacenamiento ONTAP , a los sistemas ASA r2 o a Amazon FSx for NetApp ONTAP para realizar operaciones de aprovisionamiento y protección de datos.

Puede agregar un SVM independiente o un clúster compuesto por varios SVM. Si está utilizando Amazon FSx for NetApp ONTAP, puede agregar un LIF de administrador de FSx que comprenda múltiples SVM mediante la cuenta fsxadmin o agregar 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de datos única.

Acerca de esta tarea

- Al configurar sistemas de almacenamiento, también puede habilitar las funciones del Sistema de administración de eventos (EMS) y AutoSupport . La herramienta AutoSupport recopila datos sobre el estado de su sistema y envía automáticamente dichos datos al soporte técnico de NetApp , lo que les permite solucionar problemas de su sistema.

Si habilita estas funciones, SnapCenter envía información de AutoSupport al sistema de almacenamiento y mensajes EMS al syslog del sistema de almacenamiento cuando un recurso está protegido, una operación de restauración o clonación finaliza correctamente o una operación falla.

- Si planea replicar instantáneas a un destino SnapMirror o SnapVault , debe configurar conexiones del sistema de almacenamiento para la SVM o el clúster de destino, así como para la SVM o el clúster de origen.



Si cambia la contraseña del sistema de almacenamiento, es posible que fallen los trabajos programados, las copias de seguridad a pedido y las operaciones de restauración. Después de cambiar la contraseña del sistema de almacenamiento, puede actualizarla haciendo clic en **Modificar** en la pestaña Almacenamiento.

Pasos

- 1. En el panel de navegación izquierdo, haga clic en **Sistemas de almacenamiento**.
- 2. En la página Sistemas de almacenamiento, haga clic en **Nuevo**.
- 3. En la página Agregar sistema de almacenamiento, proporcione la siguiente información:

Para este campo...	Haz esto...
Sistema de almacenamiento	Introduzca el nombre del sistema de almacenamiento o la dirección IP. Los nombres de los sistemas de almacenamiento, sin incluir el nombre de dominio, deben tener 15 caracteres o menos y deben poder resolverse. Para crear conexiones del sistema de almacenamiento con nombres que tengan más de 15 caracteres, puede usar el cmdlet Add-SmStorageConnectionPowerShell. Para los sistemas de almacenamiento con configuración MetroCluster (MCC), se recomienda registrar clústeres locales y pares para operaciones sin interrupciones. SnapCenter no admite varias SVM con el mismo nombre en diferentes clústeres. Cada SVM compatible con SnapCenter debe tener un nombre único. Después de agregar la conexión de almacenamiento a SnapCenter, no debe cambiar el nombre de la SVM o el clúster mediante ONTAP. Si se agrega SVM con un nombre corto o FQDN, debe poder resolverse tanto desde SnapCenter como desde el host del complemento.

Para este campo...	Haz esto...
Nombre de usuario/Contraseña	Ingrese las credenciales del usuario de almacenamiento que tiene los privilegios necesarios para acceder al sistema de almacenamiento.
Configuración del sistema de gestión de eventos (EMS) y AutoSupport	Si desea enviar mensajes EMS al syslog del sistema de almacenamiento o si desea que se envíen mensajes de AutoSupport al sistema de almacenamiento para protección aplicada, operaciones de restauración completadas u operaciones fallidas, seleccione la casilla de verificación correspondiente. Cuando selecciona la casilla de verificación Enviar notificación de AutoSupport para operaciones fallidas al sistema de almacenamiento, la casilla de verificación Registrar eventos del servidor SnapCenter en syslog también se selecciona porque se requieren mensajes EMS para habilitar las notificaciones de 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 el SVM es el sistema de almacenamiento secundario en una relación de respaldo, seleccione la casilla de verificación **Secundario**. Cuando se selecciona la opción **Secundaria**, SnapCenter no realiza una verificación de licencia inmediatamente.

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

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

El puerto predeterminado 443 normalmente funciona.

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

El valor predeterminado es 60 segundos.

- d. Si el SVM tiene múltiples interfaces de administración, seleccione la casilla de verificación **IP preferida** y luego ingrese la dirección IP preferida para las conexiones SVM.

- e. Haga clic en **Guardar**.

5. Haga clic en **Enviar**.

Resultado

En la página Sistemas de almacenamiento, desde el menú desplegable **Tipo**, realice una de las siguientes acciones:

- Seleccione * ONTAP SVMs* si desea ver todas las SVM que se agregaron.

Si ha agregado SVM de FSx, estos se enumeran aquí.

- Seleccione * Clústeres ONTAP * si desea ver todos los clústeres que se agregaron.

Si ha agregado clústeres FSx mediante fsxadmin, los clústeres FSx se enumeran aquí.

Al hacer clic en el nombre del clúster, todas las SVM que forman parte del clúster se muestran en la sección Máquinas virtuales de almacenamiento.

Si se agrega una nueva SVM al clúster ONTAP mediante la GUI de ONTAP , haga clic en **Redescubrir** para ver la SVM recién agregada.

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 SnapCenter tiene acceso, ejecutando 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 la máquina virtual de almacenamiento (SVM) no tiene acceso a AutoSupport.

Conexiones de almacenamiento y credenciales

Antes de realizar operaciones de protección de datos, debe configurar las conexiones de almacenamiento y agregar las credenciales que usarán SnapCenter Server y los complementos de SnapCenter .

Conexiones de almacenamiento

Las conexiones de almacenamiento brindan a SnapCenter Server y a los complementos de SnapCenter acceso al almacenamiento de ONTAP . La configuración de estas conexiones también implica configurar las funciones de AutoSupport y del Sistema de gestión de eventos (EMS).

Cartas credenciales

- Administrador del dominio o cualquier miembro del grupo de administradores

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

- *NetBIOS\Nombre de usuario*
- *Dominio FQDN\Nombre de usuario*

- *Nombre de usuario@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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host.

El formato válido para el campo Nombre de usuario es: *NombreDeUsuario*

- Credenciales para grupos de recursos individuales

Si configura 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 de respaldo al nombre de usuario.

Aprovisionar almacenamiento en hosts de Windows

Crear y administrar igroups

Crea grupos de iniciadores (igroups) para especificar qué hosts pueden acceder a un LUN determinado en el sistema de almacenamiento. Puede utilizar SnapCenter para crear, cambiar el nombre, modificar o eliminar un igroup en un host de Windows.

Crear un igroup

Puede utilizar SnapCenter para crear un igroup en un host de Windows. El igroup estará disponible en el asistente Crear disco o Conectar disco cuando asigne el igroup a un LUN.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Igroup**.
3. En la página Grupos de iniciadores, haga clic en **Nuevo**.
4. En el cuadro de diálogo Crear igroup, defina el igroup:

En este campo...	Haz esto...
Sistema de almacenamiento	Seleccione la SVM para el LUN que asignará 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 esté satisfecho con sus entradas, haga clic en **Aceptar**.

SnapCenter crea el igroup en el sistema de almacenamiento.

Cambiar el nombre de un igroup

Puede utilizar SnapCenter para cambiar el nombre de un igroup existente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Igroup**.
3. En la página Grupos de iniciadores, haga clic en el campo **Máquina virtual de almacenamiento** para mostrar una lista de las SVM disponibles y, a continuación, seleccione la SVM para el igroup que desea cambiar de nombre.
4. En la lista de igroups del SVM, seleccione el igroup que desea cambiar de nombre y haga clic en **Cambiar nombre**.
5. En el cuadro de diálogo Cambiar nombre de igroup, ingrese el nuevo nombre para el igroup y haga clic en **Cambiar nombre**.

Modificar un igroup

Puede utilizar SnapCenter para agregar iniciadores de igroup a un igroup existente. Al crear un igroup solo puedes agregar un host. Si desea crear un igroup para un clúster, puede modificar el igroup para agregar otros nodos a ese igroup.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Igroup**.
3. En la página Grupos de iniciadores, haga clic en el campo **Máquina virtual de almacenamiento** para mostrar una lista desplegable de las SVM disponibles, luego seleccione la SVM para el igroup que desea modificar.
4. En la lista de igroups, seleccione un igroup y haga clic en **Agregar iniciador al igroup**.
5. Seleccione un host.
6. Seleccione los iniciadores y haga clic en **Aceptar**.

Eliminar un igroup

Puedes usar SnapCenter para eliminar un igroup cuando ya no lo necesites.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Igroup**.
3. En la página Grupos de iniciadores, haga clic en el campo **Máquina virtual de almacenamiento** para mostrar una lista desplegable de las SVM disponibles, luego seleccione la SVM para el igroup que desea eliminar.

4. En la lista de igroups del SVM, seleccione el igroup que desea eliminar y haga clic en **Eliminar**.
5. En el cuadro de diálogo Eliminar igroup, haga clic en **Aceptar**.

SnapCenter elimina el igroup.

Crear y administrar discos

El host de Windows ve los LUN en su sistema de almacenamiento como discos virtuales. Puede utilizar SnapCenter para crear y configurar un LUN conectado a FC o a iSCSI.

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



SnapCenter no admite el cambio de nombre de un disco. Si se cambia el nombre de un disco administrado por SnapCenter, las operaciones de SnapCenter no se realizarán correctamente.

Ver los discos en un host

Puede ver los discos en cada host de Windows que administra con SnapCenter.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.
3. Seleccione el host de la lista desplegable **Host**.

Se enumeran los discos.

Ver discos agrupados

Puede ver los discos agrupados en el clúster que administra con SnapCenter. Los discos agrupados se muestran solo cuando selecciona el clúster en el menú desplegable Hosts.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.
3. Seleccione el clúster de la lista desplegable **Host**.

Se enumeran los discos.

Establecer una sesión iSCSI

Si está utilizando iSCSI para conectarse a un LUN, debe establecer una sesión iSCSI antes de crear el LUN para habilitar la comunicación.

Antes de empezar

- Debe haber definido el nodo del sistema de almacenamiento como un destino iSCSI.
- Debe haber iniciado el servicio iSCSI en el sistema de almacenamiento. ["Más información"](#)

Acerca de esta tarea

Puede establecer una sesión iSCSI solo entre las mismas versiones de IP, ya sea de IPv6 a IPv6 o de IPv4 a IPv4.

Puede utilizar una dirección IPv6 de enlace local para la gestión de sesiones iSCSI y para la comunicación entre un host y un destino solo cuando ambos estén en la misma subred.

Si cambia el nombre de un iniciador iSCSI, el acceso a los objetivos iSCSI se verá afectado. Después de cambiar el nombre, es posible que deba reconfigurar los objetivos a los que accede el iniciador para que puedan reconocer el nuevo nombre. Debe asegurarse de reiniciar el host después de cambiar el nombre de un iniciador iSCSI.

Si su host tiene más de una interfaz iSCSI, una vez que haya establecido una sesión iSCSI en SnapCenter usando una dirección IP en la primera interfaz, no podrá establecer una sesión iSCSI desde otra interfaz con una dirección IP diferente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Sesión iSCSI**.
3. En la lista desplegable **Máquina virtual de almacenamiento**, 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 muestra el asistente para establecer sesión.

6. En el asistente Establecer sesión, identifique el objetivo:

En este campo...	Ingresar...
Nombre del nodo de destino	El nombre del nodo del objetivo iSCSI Si 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 sus entradas, haga clic en **Conectar**.

SnapCenter establece la sesión iSCSI.

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

Crear LUN o discos conectados mediante FC o iSCSI

El host de Windows ve los LUN de su sistema de almacenamiento como discos virtuales. Puede utilizar SnapCenter para crear y configurar un LUN conectado a FC o a iSCSI.

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

Antes de empezar

- Debe haber creado un volumen para el LUN en su sistema de almacenamiento.

El volumen debe contener únicamente LUN, y únicamente LUN creados con SnapCenter.



No se puede crear un LUN en un volumen clonado creado por SnapCenter a menos que el clon ya se haya dividido.

- Debe haber iniciado el servicio FC o iSCSI en el sistema de almacenamiento.
- Si está utilizando iSCSI, debe haber establecido una sesión iSCSI con el sistema de almacenamiento.
- El paquete de complementos de SnapCenter para Windows debe instalarse únicamente en el host en el que está creando 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 es compartido por hosts en un clúster de conmutación por error de Windows Server que usa CSV (volúmenes compartidos de clúster), debe crear el disco en el host que posee el grupo de clústeres.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.
3. Seleccione el host de la lista desplegable **Host**.
4. Haga clic en **Nuevo**.

Se abre el asistente para crear disco.

5. En la página Nombre de LUN, identifique el LUN:

En este campo...	Haz esto...
Sistema de almacenamiento	Seleccione el SVM para el LUN.
Ruta LUN	Haga clic en Explorar para seleccionar la ruta completa de la carpeta que contiene el LUN.
Nombre LUN	Introduzca el nombre del LUN.

En este campo...	Haz esto...
Tamaño del clúster	Seleccione el tamaño de asignación del bloque LUN para el clúster. El tamaño del clúster depende del sistema operativo y las aplicaciones.
Etiqueta LUN	Opcionalmente, ingrese un texto descriptivo para el LUN.

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

Seleccionar...	Si...
Disco dedicado	Sólo un host puede acceder al LUN. Ignore el campo Grupo de recursos.
Disco compartido	El LUN es compartido por los hosts en un clúster de conmutación por error de Windows Server. Ingrese el nombre del grupo de recursos del clúster en el campo Grupo de recursos. Debe crear el disco solo en un host en el clúster de conmutación por error.
Volumen compartido de clúster (CSV)	El LUN es compartido por los hosts en un clúster de conmutación por error de Windows Server que utiliza CSV. Ingrese el nombre del grupo de recursos del clúster en el campo Grupo de recursos. Asegúrese de que el host en el que está creando el disco sea el propietario del grupo de clústeres.

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

Propiedad	Descripción
Asignar automáticamente el punto de montaje	SnapCenter asigna automáticamente un punto de montaje de volumen según la unidad del sistema. Por ejemplo, si la unidad de su sistema es C:, la asignación automática crea un punto de montaje de volumen debajo de su unidad C: (C:\scmnpt\). La asignación automática no es compatible con discos compartidos.

Propiedad	Descripción
Asignar letra de unidad	Monte el disco en la unidad que seleccione en la lista desplegable adyacente.
Usar punto de montaje de volumen	Monte el disco en la ruta de la unidad que especifique en el campo adyacente. La raíz del punto de montaje del volumen debe ser propiedad del host en el que está creando el disco.
No asigne letra de unidad ni punto de montaje de volumen	Elija esta opción si prefiere montar el disco manualmente en Windows.
Tamaño de LUN	Especifique el tamaño del LUN; 150 MB mínimo. Seleccione MB, GB o TB en la lista desplegable adjunta.
Utilice aprovisionamiento fino para el volumen que aloja este LUN	Aprovisione con thin provisioning el LUN. El aprovisionamiento fino asigna solo la cantidad de espacio de almacenamiento que se necesita en un momento dado, lo que permite que el LUN crezca de manera eficiente hasta alcanzar la máxima capacidad disponible. Asegúrese de que haya suficiente espacio disponible en el volumen para acomodar todo el almacenamiento LUN que cree que necesitará.
Elija el tipo de partición	Seleccione la partición GPT para una tabla de particiones GUID o la partición MBR para un registro de arranque maestro. Las particiones MBR pueden causar problemas de desalineación en los clústeres de conmutación por error de Windows Server.  Los discos de partición de interfaz de firmware extensible unificada (UEFI) no son compatibles.

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

En este campo...	Haz esto...
Host	Haga doble clic en el nombre del grupo de clústeres para mostrar una lista desplegable que muestra los hosts que pertenecen al clúster y luego seleccione el host para el iniciador. Este campo solo se muestra si el LUN es compartido por hosts en un clúster de conmutación por error de Windows Server.
Elija el iniciador del host	Seleccione Fibre Channel o iSCSI y, a continuación, seleccione el iniciador en el host. Puede seleccionar varios iniciadores FC si está utilizando FC con E/S de múltiples rutas (MPIO).

9. En la página Tipo de grupo, especifique si desea asignar un igroup existente al LUN o crear un nuevo igroup:

Seleccionar...	Si...
Crear un nuevo igroup para los iniciadores seleccionados	Desea crear un nuevo igroup para los iniciadores seleccionados.
Elija 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 nombre del igroup . Escriba las primeras letras del nombre del igroup existente para completar automáticamente el campo.

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

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

Cambiar el tamaño de un disco

Puede aumentar o disminuir el tamaño de un disco según cambien las necesidades de su sistema de almacenamiento.

Acerca de esta tarea

- Para LUN con aprovisionamiento fino, el tamaño de la geometría del LUN de ONTAP se muestra como el tamaño máximo.
- Para LUN con aprovisionamiento grueso, el tamaño expandible (tamaño disponible en el volumen) se muestra como el tamaño máximo.
- Los LUN con particiones estilo MBR tienen un límite de tamaño de 2 TB.

- Los LUN con particiones de estilo GPT tienen un límite de tamaño del sistema de almacenamiento de 16 TB.
- Es una buena idea hacer una instantánea antes de cambiar el tamaño de una LUN.
- Si necesita restaurar un LUN a partir de una instantánea realizada antes de cambiar el tamaño del LUN, SnapCenter cambia automáticamente el tamaño del LUN al tamaño de la instantánea.

Después de la operación de restauración, los datos agregados al LUN después de su cambio de tamaño se deben restaurar desde una instantánea realizada después de su cambio de tamaño.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.
3. Seleccione el host de la lista desplegable Host.

Se enumeran los discos.

4. Seleccione el disco que desea redimensionar y luego haga clic en **Cambiar tamaño**.
5. En el cuadro de diálogo Cambiar tamaño de disco, utilice la herramienta deslizante para especificar el nuevo tamaño del disco o ingrese el nuevo tamaño en el campo Tamaño.



Si ingresa el tamaño manualmente, deberá hacer clic fuera del campo Tamaño antes de que el botón Reducir o Expandir se habilite correctamente. Además, debe hacer clic en MB, GB o TB para especificar la unidad de medida.

6. Cuando esté satisfecho con sus entradas, haga clic en **Reducir** o **Expandir**, según corresponda.

SnapCenter cambia el tamaño del disco.

Conectar un disco

Puede utilizar el asistente Conectar disco para conectar un LUN existente a un host o para volver a conectar un LUN que se haya desconectado.

Antes de empezar

- Debe haber iniciado el servicio FC o iSCSI en el sistema de almacenamiento.
- Si está utilizando 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 es compartido por hosts en un clúster de conmutación por error de Windows Server que usa CSV (volúmenes compartidos de clúster), entonces debe conectar el disco en el host que posee el grupo de clústeres.
- El complemento para Windows debe instalarse únicamente en el host en el que está conectando el disco.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.

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

4. Haga clic en **Conectar**.

Se abre el asistente Conectar disco.

5. En la página Nombre de LUN, identifique el LUN al que conectarse:

En este campo...	Haz esto...
Sistema de almacenamiento	Seleccione el SVM para el LUN.
Ruta LUN	Haga clic en Explorar para seleccionar la ruta completa del volumen que contiene el LUN.
Nombre LUN	Introduzca el nombre del LUN.
Tamaño del clúster	Seleccione el tamaño de asignación del bloque LUN para el clúster. El tamaño del clúster depende del sistema operativo y las aplicaciones.
Etiqueta LUN	Opcionalmente, ingrese un texto descriptivo para el LUN.

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

Seleccionar...	Si...
Disco dedicado	Sólo un host puede acceder al LUN.
Disco compartido	El LUN es compartido por los hosts en un clúster de conmutación por error de Windows Server. Solo necesita conectar el disco a un host en el clúster de conmutación por error.
Volumen compartido de clúster (CSV)	El LUN es compartido por los hosts en un clúster de conmutación por error de Windows Server que utiliza CSV. Asegúrese de que el host en el que se conecta al disco sea el propietario del grupo de clústeres.

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

Propiedad	Descripción
Asignación automática	Deje que SnapCenter asigne automáticamente un punto de montaje de volumen según la unidad del sistema. Por ejemplo, si la unidad de su sistema es C:, la propiedad de asignación automática crea un punto de montaje de volumen debajo de su unidad C: (C:\scmnpt\). La propiedad de asignación automática no es compatible con discos compartidos.
Asignar letra de unidad	Monte el disco en la unidad que seleccione en la lista desplegable adjunta.
Usar punto de montaje de volumen	Monte el disco en la ruta de unidad que especifique en el campo contiguo. La raíz del punto de montaje del volumen debe ser propiedad del host en el que está creando el disco.
No asigne letra de unidad ni punto de montaje de volumen	Elija esta opción si prefiere montar el disco manualmente en Windows.

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

En este campo...	Haz esto...
Host	Haga doble clic en el nombre del grupo de clústeres para mostrar una lista desplegable que muestra los hosts que pertenecen al clúster; luego seleccione el host para el iniciador. Este campo solo se muestra si el LUN es compartido por hosts en un clúster de conmutación por error de Windows Server.
Elija el iniciador del host	Seleccione Fibre Channel o iSCSI y, a continuación, seleccione el iniciador en el host. Puede seleccionar varios iniciadores FC si está utilizando FC con MPIO.

9. En la página Tipo de grupo, especifique si desea asignar un igroup existente al LUN o crear un nuevo igroup:

Seleccionar...	Si...
Crear un nuevo igroup para los iniciadores seleccionados	Desea crear un nuevo igroup para los iniciadores seleccionados.
Elija 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 nombre del igroup. Escriba las primeras letras del nombre del igroup existente para completar el campo automáticamente.

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

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

Desconectar un disco

Puede desconectar un LUN de un host sin afectar el contenido del LUN, con una excepción: si desconecta un clon antes de que se haya dividido, perderá el contenido del clon.

Antes de empezar

- Asegúrese de que el LUN no esté siendo utilizado por ninguna aplicación.
- Asegúrese de que el LUN no esté siendo monitoreado con software de monitoreo.
- Si el LUN es compartido, asegúrese de eliminar las dependencias de recursos del clúster del LUN y verifique que todos los nodos del clúster estén encendidos, funcionando correctamente y disponibles para SnapCenter.

Acerca de esta tarea

Si desconecta un LUN en un volumen FlexClone que SnapCenter ha creado y no hay otros LUN conectados en el volumen, SnapCenter elimina el volumen. Antes de desconectar el LUN, SnapCenter muestra un mensaje advirtiéndole que el volumen FlexClone podría eliminarse.

Para evitar la eliminación automática del volumen FlexClone, debe cambiar el nombre del volumen antes de desconectar el último LUN. Al cambiar el nombre del volumen, asegúrese de cambiar varios caracteres además del último carácter del nombre.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.
3. Seleccione el host de la lista desplegable **Host**.

Se enumeran los discos.

4. Seleccione el disco que desea desconectar y luego haga clic en **Desconectar**.
5. En el cuadro de diálogo Desconectar disco, haga clic en **Aceptar**.

SnapCenter desconecta el disco.

Eliminar un disco

Puedes eliminar un disco cuando ya no lo necesites. Después de eliminar un disco, no es posible recuperarlo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Discos**.
3. Seleccione el host de la lista desplegable **Host**.

Se enumeran los discos.

4. Seleccione el disco que desea eliminar y luego haga clic en **Eliminar**.
5. En el cuadro de diálogo Eliminar disco, haga clic en **Aceptar**.

SnapCenter elimina el disco.

Crear y administrar recursos compartidos SMB

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

Mejores prácticas: Se recomienda usar los cmdlets porque le permiten aprovechar las plantillas proporcionadas con SnapCenter para automatizar la configuración de recursos compartidos.

Las plantillas encapsulan las mejores prácticas para la configuración de volúmenes y recursos compartidos. Puede encontrar las plantillas en la carpeta Plantillas en la carpeta de instalación del paquete de complementos de SnapCenter para Windows.



Si te sientes cómodo haciéndolo, puedes crear tus propias plantillas siguiendo los modelos proporcionados. Debe revisar los parámetros en la documentación del cmdlet antes de crear una plantilla personalizada.

Crear un recurso compartido SMB

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

No puede utilizar SnapCenter para realizar copias de seguridad de bases de datos en recursos compartidos SMB. El soporte de SMB se limita únicamente al aprovisionamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Compartir**.
3. Seleccione la SVM de la lista desplegable **Máquina virtual de almacenamiento**.
4. Haga clic en **Nuevo**.

Se abre el cuadro de diálogo Nuevo recurso compartido.

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

En este campo...	Haz esto...
Descripción	Introduzca un texto descriptivo para la acción.
Compartir nombre	Introduzca el nombre del recurso compartido, por ejemplo, test_share. El nombre que ingrese para el recurso compartido también se utilizará como nombre del volumen. El nombre de la acción: • Debe ser una cadena UTF-8. • No debe incluir los siguientes caracteres: caracteres de control de 0x00 a 0x1F (ambos incluidos), 0x22 (comillas dobles) y los caracteres especiales \ / [] : (vertical bar) < > + = ; , ?
Compartir ruta	• Haga clic en el campo para ingresar una nueva ruta del sistema de archivos, por ejemplo, /. • Haga doble clic en el campo para seleccionar de una lista de rutas de sistemas de archivos existentes.

6. Cuando esté satisfecho con sus entradas, haga clic en **Aceptar**.

SnapCenter crea el recurso compartido SMB en la SVM.

Eliminar un recurso compartido SMB

Puedes eliminar un recurso compartido SMB cuando ya no lo necesites.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Compartir**.
3. En la página Recursos compartidos, haga clic en el campo **Máquina virtual de almacenamiento** para mostrar un menú desplegable con una lista de máquinas virtuales de almacenamiento (SVM) disponibles, luego seleccione la SVM para el recurso compartido que desea eliminar.
4. De la lista de recursos compartidos en el SVM, seleccione el recurso compartido que desea eliminar y haga clic en **Eliminar**.
5. En el cuadro de diálogo Eliminar recurso compartido, haga clic en **Aceptar**.

SnapCenter elimina el recurso compartido SMB del SVM.

Recuperar espacio en el sistema de almacenamiento

Aunque NTFS rastrea el espacio disponible en un LUN cuando se eliminan o modifican archivos, no informa la nueva información al sistema de almacenamiento. Puede ejecutar el cmdlet de PowerShell de recuperación de espacio en el host del complemento para Windows para garantizar que los bloques recién liberados se marquen como disponibles en el almacenamiento.

Si está ejecutando el cmdlet en un host de complemento remoto, debe haber ejecutado el cmdlet SnapCenterOpen-SMConnection para abrir una conexión al servidor SnapCenter .

Antes de empezar

- Debe asegurarse de que el proceso de recuperación de espacio se haya completado antes de realizar una operación de restauración.
- Si el LUN es compartido por los hosts en un clúster de conmutación por error de Windows Server, debe realizar una recuperación de espacio en el host que posee el grupo de clústeres.
- Para obtener un rendimiento de almacenamiento óptimo, debe realizar la recuperación de espacio con la mayor frecuencia posible.

Debe asegurarse de que se haya escaneado todo el sistema de archivos NTFS.

Acerca de esta tarea

- La recuperación de espacio consume mucho tiempo y consume muchos recursos de la CPU, por lo que generalmente es mejor ejecutar la operación cuando el uso del sistema de almacenamiento y del host de Windows es bajo.
- La recuperación de espacio recupera casi todo el espacio disponible, pero no el 100 por ciento.
- No debe ejecutar la desfragmentación del disco al mismo tiempo que realiza la recuperación de espacio.

Hacerlo puede ralentizar el proceso de recuperación.

Paso

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

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

drive_path es la ruta de la unidad asignada al LUN.

Aprovisionamiento de 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 utilizar cmdlets directamente o agregarlos a scripts.

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

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Si los cmdlets de PowerShell de SnapCenter no funcionan debido a la eliminación de SnapDrive para Windows del servidor, consulte ["Los cmdlets de SnapCenter fallan cuando se desinstala SnapDrive para Windows"](#) .

Aprovisionamiento de almacenamiento en entornos VMware

Puede utilizar el complemento SnapCenter para Microsoft Windows en entornos VMware para crear y administrar LUN y administrar instantáneas.

Plataformas de sistema operativo invitado VMware compatibles

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

Admite hasta un máximo de 16 nodos compatibles con VMware cuando se utiliza el iniciador de software iSCSI de Microsoft, o hasta dos nodos utilizando FC

- LUN de RDM

Compatibilidad con un máximo de 56 LUN RDM con cuatro controladores LSI Logic SCSI para RDMS normal, o 42 LUN RDM con tres controladores LSI Logic SCSI en un complemento VMware VM MSCS box-to-box para configuración de Windows

Admite controlador VMware ParaVirtual SCSI. Se pueden admitir 256 discos en los discos RDM.

Para obtener la información más reciente sobre las versiones compatibles, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Limitaciones relacionadas con el servidor VMware ESXi

- No se admite la instalación del complemento para Windows en un clúster de Microsoft en máquinas virtuales que utilicen credenciales ESXi.

Debe utilizar sus credenciales de vCenter al instalar el complemento para Windows en máquinas virtuales agrupadas.

- Todos los nodos agrupados deben usar el mismo ID de destino (en el adaptador SCSI virtual) para el mismo disco agrupado.
- Cuando crea un LUN RDM fuera del complemento para Windows, debe reiniciar el servicio del complemento para permitirle reconocer el disco recién creado.
- No se pueden utilizar iniciadores iSCSI y FC al mismo tiempo en un sistema operativo invitado VMware.

Privilegios mínimos de vCenter necesarios para las operaciones de SnapCenter RDM

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

- Almacén de datos: eliminar archivo
- Host: Configuración > Configuración de partición de almacenamiento
- Máquina virtual: configuración

Debe asignar estos privilegios a un rol en el nivel de servidor del centro virtual. El rol al que asigna estos

privilegios no se puede asignar a ningún usuario sin privilegios de root.

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

Administrar LUN FC RDM en un clúster de Microsoft

Puede usar el complemento para Windows para administrar un clúster de Microsoft mediante LUN RDM de FC, pero primero debe crear el quórum RDM compartido y el almacenamiento compartido fuera del complemento y luego agregar los discos a las máquinas virtuales en el clúster.

A partir de ESXi 5.5, también puede usar hardware ESX iSCSI y FCoE para administrar un clúster de Microsoft. El complemento para Windows incluye soporte inmediato para clústeres de Microsoft.

Requisitos

El complemento para Windows proporciona soporte para clústeres de Microsoft que utilizan LUN FC RDM en dos máquinas virtuales diferentes que pertenecen a dos servidores ESX o ESXi diferentes, también conocidos como clúster entre cuadros, cuando cumple con 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 principal de VMware.
- Cada host principal debe tener al menos dos adaptadores de red.
- Debe haber al menos un almacén de datos del sistema de archivos de máquina virtual VMware (VMFS) compartido entre los dos servidores ESX o ESXi.
- VMware recomienda que el almacén de datos compartido se cree en una SAN FC.

Si es necesario, el almacén de datos compartido también se puede crear mediante iSCSI.

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

No se pueden utilizar discos virtuales para almacenamiento compartido.

- Se debe configurar un controlador SCSI en cada máquina virtual del clúster en modo de compatibilidad física:

Windows Server 2008 R2 requiere que configure el controlador SCSI SAS LSI Logic en cada máquina virtual. Los LUN compartidos no pueden usar el controlador SAS LSI Logic existente si solo existe uno de su tipo y ya está conectado a la unidad C:.

Los controladores SCSI de tipo paravirtual no son compatibles con los clústeres VMware Microsoft.



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 procesar** (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.
- Debe utilizar credenciales de vCenter y no credenciales de ESX o ESXi cuando instale el complemento para Windows en máquinas virtuales que pertenecen a un clúster de Microsoft.
- El complemento para Windows no puede crear un único igroup con iniciadores de múltiples hosts.

El grupo que contiene los iniciadores de todos los hosts ESXi debe crearse en el controlador de almacenamiento antes de crear los LUN RDM que se utilizarán como discos de clúster compartidos.

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

Cuando se crea un LUN RDM, se crea un grupo iniciador con ALUA.

Limitaciones

El complemento para Windows admite clústeres de Microsoft que utilizan LUN RDM FC/iSCSI en diferentes máquinas virtuales que pertenecen a distintos servidores ESX o ESXi.



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

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

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

- Los iniciadores iSCSI y HBA de ESX no son compatibles con discos compartidos en un clúster de Microsoft.
- El complemento para Windows no admite la migración de máquinas virtuales con vMotion si la máquina virtual es parte de un clúster de Microsoft.
- El complemento para Windows no admite MPIO en máquinas virtuales en un clúster de Microsoft.

Crear un LUN FC RDM compartido

Antes de poder usar LUN FC RDM para compartir almacenamiento entre nodos en un clúster de Microsoft, primero debe crear el disco de quórum compartido y el disco de almacenamiento compartido, y luego agregarlos a ambas máquinas virtuales en el clúster.

El disco compartido no se crea mediante el complemento para Windows. Debe crear y luego agregar el LUN compartido a cada máquina virtual en el clúster. Para obtener más información, consulte ["Agrupar máquinas virtuales en hosts físicos"](#).

Agregar licencias basadas en controlador de SnapCenter Standard

Se requiere una licencia basada en controlador SnapCenter Standard si utiliza controladores de almacenamiento FAS, AFF o ASA.

La licencia basada en controlador tiene las siguientes características:

- El derecho a SnapCenter Standard está incluido con la compra de 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.

- Bloqueado al número de serie del controlador

Para obtener información sobre las licencias necesarias, consulte ["Licencias de 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, seleccione **Sistemas de almacenamiento**.
2. En la página Sistemas de almacenamiento, en el menú desplegable **Tipo**, seleccione si desea ver todas las SVM o clústeres que se agregaron:
 - Para ver todas las SVM que se agregaron, seleccione * ONTAP SVMs*.
 - Para ver todos los clústeres que se agregaron, seleccione * Clústeres ONTAP *.

Quando selecciona el nombre del clúster, todas las SVM que forman parte del clúster se muestran en la sección Máquinas virtuales de almacenamiento.

3. En la lista Conexiones de almacenamiento, busque la columna Licencia del controlador.

La columna Licencia del controlador 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 FAS, AFF o ASA .
- No aplicable indica que una licencia de SnapManager Suite no es aplicable porque el controlador de almacenamiento está en Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select o plataformas de almacenamiento secundarias.

Paso 2: Identificar las licencias instaladas en el controlador

Puede utilizar la línea de comandos ONTAP para ver todas las licencias instaladas en su controlador. Debe ser administrador de clúster en el sistema FAS, AFF o ASA .



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

Pasos

1. Inicie sesión en el controlador de NetApp mediante la línea de comandos ONTAP .

2. Ingrese el comando de visualización de licencia y luego vea el resultado para ver si la licencia de SnapManagerSuite está instalada.

Ejemplo de salida

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

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

Serial Number: 1-81-000000000000000000000000xx
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 de SnapManagerSuite está instalada, por lo tanto, no se requiere ninguna acción de licencia adicional de SnapCenter .

Paso 3: Recupere el número de serie del controlador

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 el controlador utilizando la línea de comando ONTAP .
2. Ingrese el comando `system show -instance` y luego revise la salida para ubicar el número de serie del controlador.

Ejemplo de salida

```
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: xxxxxxxxxx
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: xxxxxxxxxx
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 controlador

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.

- Debes tener el número de serie del controlador.

Pasos

1. Iniciar sesión en el "Sitio de soporte de NetApp" .
2. Vaya a **Sistemas > Licencias de software**.
3. En el área Criterios de selección, asegúrese de que el Número de serie (ubicado en la parte posterior de la unidad) esté seleccionado, ingrese el número de serie del controlador y luego seleccione **¡Ir!**.

Software Licenses

Selection Criteria

Choose a method by which to search

► Serial Number (located on back of unit) ▾ Enter Value:

Enter the Cluster Serial Number value without dashes.

- OR -

► Show Me All: Serial Numbers with Licenses ▾ For Company:

Se muestra una lista de licencias para el controlador especificado.

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

Paso 5: Agregar licencia basada en controlador

Puede usar la línea de comandos de ONTAP para agregar una licencia basada en controlador de SnapCenter cuando usa sistemas FAS, AFF o ASA y tiene una licencia de SnapCenter Standard o SnapManagerSuite.

Antes de empezar

- Debe ser administrador de clúster en el sistema FAS, AFF o ASA .
- Debe tener la licencia SnapCenter Standard o SnapManagerSuite.

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 controlador.

Si desea instalar SnapCenter a modo de prueba, debe comunicarse con su representante de ventas para obtener una licencia de evaluación del paquete Premium para instalar en su controlador.

Pasos

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

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

Este comando está disponible en el nivel de privilegio de administrador.

3. Verifique que la licencia de SnapManagerSuite esté instalada:

```
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 .



Solo es necesario eliminar una licencia de prueba manualmente si está utilizando una licencia basada en controlador SnapCenter Standard.

Pasos

1. En el servidor 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 Set-SmRepositoryPassword para restablecer la contraseña de MySQL.

Para obtener información sobre los cmdlets, consulte ["Guía de referencia de cmdlets del software SnapCenter"](#) .

2. Abra el símbolo del sistema y ejecute `mysql -u root -p` para iniciar sesión en MySQL.

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

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

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

Configurar alta disponibilidad

Configurar servidores SnapCenter para alta disponibilidad

Para admitir alta disponibilidad (HA) en SnapCenter que se ejecuta en Windows o Linux, puede instalar el balanceador de carga F5. F5 permite que SnapCenter Server admita configuraciones activas-pasivas en hasta dos hosts que se encuentren en la misma ubicación. Para utilizar F5 Load Balancer en SnapCenter, debe configurar los servidores de SnapCenter y configurar el balanceador de carga F5.

También puede configurar el equilibrio de carga de red (NLB) para configurar la alta disponibilidad de SnapCenter . Debe configurar NLB manualmente fuera de la instalación de SnapCenter para lograr una alta disponibilidad.

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

Configurar la alta disponibilidad mediante F5

Para obtener instrucciones sobre cómo configurar los servidores SnapCenter para alta disponibilidad mediante el balanceador de carga F5, consulte ["Cómo configurar servidores SnapCenter para alta disponibilidad usando F5 Load Balancer"](#) .

Debe ser miembro del grupo de administradores locales en los servidores SnapCenter (además de estar asignado al rol SnapCenterAdmin) para usar los siguientes cmdlets para agregar y eliminar clústeres F5:

- Agregar SmServerCluster
- Agregar servidor Sm
- Eliminar SmServerCluster

Para más información, consulte ["Guía de referencia de cmdlets del software SnapCenter"](#) .

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 F5.
- Si se produce una conmutación por error entre servidores SnapCenter y también hay una sesión de SnapCenter existente, debe cerrar el navegador e iniciar sesión en SnapCenter nuevamente.
- En la configuración del balanceador de carga (NLB o F5), si agrega un host que está parcialmente resuelto por el host NLB o F5 y si el host de SnapCenter no puede comunicarse con este host, entonces la página del host de SnapCenter cambia frecuentemente entre el estado de host inactivo y el estado de ejecución. Para resolver este problema, debe asegurarse de que ambos hosts de SnapCenter puedan resolver el host en NLB o en el host F5.
- Los comandos de SnapCenter para la configuración de MFA deben ejecutarse en todos los hosts. La configuración de la parte confiada debe realizarse en el servidor de Servicios de federación de Active Directory (AD FS) utilizando los detalles del clúster F5. El acceso a la interfaz de usuario de SnapCenter a nivel de host se bloqueará después de habilitar MFA.
- Durante la conmutación por error, 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 se active.

Configurar la alta disponibilidad mediante el equilibrio de carga de red (NLB)

Puede configurar el equilibrio de carga de red (NLB) para configurar la alta disponibilidad de SnapCenter . Debe configurar NLB manualmente fuera de la instalación de SnapCenter para lograr una alta disponibilidad.

Para obtener información sobre cómo configurar el equilibrio de carga de red (NLB) con SnapCenter , consulte ["Cómo configurar NLB con SnapCenter"](#) .

Configurar alta disponibilidad usando 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) separadas y configurándolos para conmutación por error automática. La arquitectura incluye direcciones IP privadas virtuales, tablas de enrutamiento y sincronización entre bases de datos MySQL activas y en espera.

Pasos

1. Configurar la IP superpuesta privada virtual en AWS. Para obtener más información, consulte ["Configurar la IP superpuesta privada virtual"](#) .

2. Prepare su host de Windows

- a. Forzar que IPv4 tenga prioridad sobre IPv6:
 - Ubicación: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
 - Clave: Componentes deshabilitados
 - Tipo: REG_DWORD
 - Valor: 0x20
- b. Asegúrese de que los nombres de dominio completos se puedan resolver a través de DNS o mediante la configuración del host local a las direcciones IPv4.
- c. Asegúrese de no tener un proxy de sistema configurado.
- d. Asegúrese de que la contraseña de administrador sea la misma en ambos servidores Windows 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 SnapCenter .

- a. Inicie Powershell y conéctese a SnapCenter.
`Open-SmConnection`
- b. Crear el cluster.
`Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
- c. Añade 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 Lambda para ajustar la tabla de enrutamiento en caso de que el punto final de IP privada virtual no esté disponible, monitoreado por AWS CloudWatch. Para obtener más información, consulte ["Crear 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 el punto final no es accesible. 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 un flujo de trabajo utilizando una función de pasos como alternativa al monitoreo 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 fallas y la función de 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 fallas entre dos iteraciones de Step Function. Para obtener más información, consulte ["Comience a usar la tabla DynamoDB"](#) .
 - c. Crear la función de paso. Para obtener más información, consulte ["Documentación de la función de paso"](#) .
 - d. Pruebe un solo paso.
 - e. Pruebe la función completa.

- f. Cree un rol de IAM y ajuste los permisos para poder ejecutar la función Lambda.
- g. Crear un cronograma para activar la función de paso. Para obtener más información, consulte ["Uso de Amazon EventBridge Scheduler para iniciar una función de paso"](#) .

Configurar la alta disponibilidad mediante el equilibrador de carga de Azure

Puede configurar un entorno de SnapCenter de alta disponibilidad mediante el equilibrador de carga de Azure.

Pasos

1. Cree máquinas virtuales en un conjunto de escalado mediante el portal de Azure. El conjunto de escalado de máquinas virtuales de Azure le permite crear y administrar un grupo de máquinas virtuales con equilibrio de carga. La cantidad de instancias de máquinas virtuales puede aumentar o disminuir automáticamente en respuesta a la demanda o a un cronograma definido. Para obtener más información, consulte ["Crear máquinas virtuales en un conjunto de escalado mediante Azure Portal"](#) .
2. Después de configurar las máquinas virtuales, inicie sesión en cada máquina virtual en el conjunto de VM 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. Añade 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, reconstruya el host secundario.

```
Set-SmRepositoryConfig -RebuildSlave -Verbose
```
7. Conmutación por error al segundo host.

```
Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
```

== Cambiar de NLB a F5 para alta disponibilidad

Puede cambiar la configuración de HA de SnapCenter de Equilibrio de carga de red (NLB) para usar F5 Load Balancer.

Pasos

1. Configure los servidores SnapCenter para alta disponibilidad mediante F5. ["Más información"](#) .
2. En el host del servidor SnapCenter , inicie PowerShell.
3. Inicie una sesión utilizando el cmdlet Open-SmConnection y luego ingrese sus credenciales.
4. Actualice el servidor SnapCenter para que apunte a la dirección IP del clúster F5 mediante el cmdlet Update-SmServerCluster.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Alta disponibilidad para el repositorio MySQL de SnapCenter

La replicación de MySQL es una característica de MySQL Server que le permite replicar datos de un servidor de base de datos MySQL (maestro) a otro servidor de base de datos MySQL (esclavo). SnapCenter admite la replicación de MySQL para alta disponibilidad solo en dos nodos habilitados para equilibrio de carga de red (NLB).

SnapCenter realiza operaciones de lectura o escritura en el repositorio maestro y enruta su conexión al repositorio esclavo cuando hay una falla en el repositorio maestro. El repositorio esclavo se convierte entonces en el repositorio maestro. SnapCenter también admite la replicación inversa, que se habilita solo durante la conmutación por error.

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

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

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Debe tener en cuenta las limitaciones relacionadas con la función MySQL HA:

- NLB y MySQL HA no son compatibles más allá de dos nodos.
- No se admite el cambio de una instalación independiente de SnapCenter a una instalación NLB o viceversa ni el cambio de una configuración independiente de MySQL a MySQL HA.
- No se admite la conmutación por error automática si los datos del repositorio esclavo no están sincronizados con los datos del repositorio maestro.

Puede iniciar una conmutación por error forzada mediante el cmdlet *Set-SmRepositoryConfig*.

- Cuando se inicia la conmutación por error, los trabajos que se están ejecutando pueden fallar.

Si se produce una conmutación por error porque MySQL Server o SnapCenter Server no funcionan, es posible que fallen todos los trabajos que se estén ejecutando. Después de conmutar al segundo nodo, todos los trabajos posteriores se ejecutan correctamente.

Para obtener información sobre 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 utilizar los roles existentes de SnapCenter, puede crear sus propios roles y personalizar los permisos.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Roles**.
3. Hacer clic .
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 este rol pueden ver los objetos de otros miembros** para permitir que otros miembros del rol vean recursos como volúmenes y hosts después de actualizar la lista de recursos.

Debe deseleccionar esta opción si no desea que los miembros de este rol vean los objetos a los que están asignados otros miembros.



Cuando esta opción está habilitada, no es necesario asignar a los usuarios acceso a 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 al rol o haga clic en **Seleccionar todo** para otorgar todos los permisos al rol.
7. Haga clic en **Enviar**.

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

Puede utilizar los comandos de inicio de sesión de seguridad para agregar una función RBAC de NetApp ONTAP cuando sus sistemas de almacenamiento ejecutan ONTAP en clúster.

Antes de empezar

- Identifique la tarea (o tareas) que desea realizar y los privilegios necesarios para realizar estas tareas.
- Otorgar privilegios a comandos y/o directorios de comandos.

Hay dos niveles de acceso para cada comando/directorio de comandos: acceso total y solo lectura.

Siempre debes asignar primero los privilegios de acceso total.

- Asignar 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 maneja automáticamente la configuración correcta de los privilegios de ONTAP . Por ejemplo, la herramienta RBAC User Creator para NetApp ONTAP agrega automáticamente los privilegios en el

orden correcto para que los privilegios de acceso total aparezcan primero. Si agrega primero los privilegios de solo lectura y luego agrega los privilegios de acceso total, ONTAP marca los privilegios de acceso total como duplicados y los ignora.



Si posteriormente actualiza SnapCenter o ONTAP, debe volver a ejecutar la herramienta RBAC User Creator para NetApp ONTAP para actualizar los roles de usuario que creó anteriormente. Los roles de usuario creados para una versión anterior de SnapCenter u ONTAP no funcionan correctamente con versiones actualizadas. Cuando vuelva a ejecutar la herramienta, ésta gestionará automáticamente la actualización. No es necesario recrear los roles.

Para obtener más información sobre cómo configurar los roles RBAC de ONTAP, consulte ["Guía de autenticación de administrador y RBAC de ONTAP 9"](#).

Pasos

1. En el sistema de almacenamiento, cree un nuevo rol ingresando el siguiente comando:

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

- `svm_name` es el nombre de la SVM. Si lo deja en blanco, el valor predeterminado será el administrador del clúster.
- `role_name` es el nombre que especifica para el rol.
- El comando es la capacidad de ONTAP.



Debes repetir este comando para cada permiso. Recuerde que los comandos de acceso total deben aparecer antes que los comandos de solo lectura.

Para obtener información sobre la lista de permisos, consulte ["Comandos CLI de ONTAP para crear roles y asignar permisos"](#).

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

```
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 del usuario que estás creando.
- `<password>` es tu contraseña. Si no especifica una contraseña, el sistema le solicitará una.
- `svm_name` es el nombre de la SVM.

3. Asigne el rol al usuario ingresando 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 le permite modificar el usuario para asociarlo con el rol.
- `<svm_name>` es el nombre de la SVM.
- `<role_name>` es el nombre del rol que creó en el Paso 1.
- `<password>` es tu contraseña. Si no especifica una contraseña, el sistema le solicitará una.

4. Verifique que el usuario se haya creado correctamente ingresando el siguiente comando:

```
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.

Crear roles SVM con privilegios mínimos

Hay varios comandos CLI de ONTAP que debe ejecutar cuando crea un rol para un nuevo usuario de SVM en ONTAP. Esta función es necesaria si configura SVM en ONTAP para usar con SnapCenter y no desea utilizar la función vsadmin.

Pasos

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

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



Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

Comandos CLI de ONTAP para crear roles SVM y asignar permisos

Hay varios comandos CLI de ONTAP que debe ejecutar para crear roles 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 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 asígnele todos los permisos.

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



Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

Comandos CLI de ONTAP para crear roles SVM y asignar permisos

Hay varios comandos CLI de ONTAP que debe ejecutar para crear roles 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`

Crear roles de clúster de ONTAP con privilegios mínimos

Debe crear un rol de clúster de ONTAP con privilegios mínimos para no tener que usar el rol de administrador de ONTAP para realizar operaciones en SnapCenter. Puede ejecutar varios comandos CLI de ONTAP para crear la función de clúster de ONTAP y asignar privilegios mínimos.

Pasos

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

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



Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

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

Hay varios comandos CLI de ONTAP que debe ejecutar 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

Crear roles de clúster ONTAP para sistemas ASA r2

Debe crear un rol de clúster de ONTAP con privilegios mínimos para no tener que usar el rol de administrador de ONTAP para realizar operaciones en SnapCenter. Puede ejecutar varios comandos CLI de ONTAP para crear la función de clúster de ONTAP y asignar privilegios mínimos.

Pasos

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

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



Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

```
security login create -user <user_name> -vserver <cluster_name> -application
```

```
http -authmethod password -role <role_name\>
```

3. Desbloquear al usuario.

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

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

Hay varios comandos CLI de ONTAP que debe ejecutar 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

Agregar un usuario o grupo y asignarle roles y activos

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

Antes de empezar

- Debe haber iniciado sesión como rol "SnapCenterAdmin".
- Debe haber creado las cuentas de usuario o grupo en Active Directory en el sistema operativo o la base de datos. No puedes usar SnapCenter para crear estas cuentas.



Puede incluir solo los siguientes caracteres especiales en los nombres de usuario y de grupo: espacio (), guion (-), guión bajo (_) y dos puntos (:).

- SnapCenter incluye varios roles predefinidos.

Puede asignar estos roles al usuario o crear roles nuevos.

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

Esto permite a los usuarios realizar las acciones para las que tienen permiso en los activos que les están asignados.

- Debe 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, complementos y credenciales al usuario mientras crea el usuario o grupo.
- Los activos mínimos que debes asignar a un usuario para realizar determinadas operaciones son los siguientes:

Operación	Cesión de activos
Proteger los recursos	anfitrión, política

Operación	Cesión de activos
Respaldo	host, grupo de recursos, política
Restaurar	anfitrión, grupo de recursos
Clon	host, grupo de recursos, política
Ciclo de vida del clon	anfitrión
Crear un grupo de recursos	anfitrión

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

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

- Si planea replicar instantáneas, debe asignar la conexión de almacenamiento tanto para el volumen de origen como para el de destino al usuario que realiza la operación.

Debe agregar activos antes de asignar acceso a los usuarios.



Si utiliza las funciones del SnapCenter Plug-in for VMware vSphere para proteger máquinas virtuales, VMDK o almacenes de datos, debe usar la GUI de VMware vSphere para agregar un usuario de vCenter a una SnapCenter Plug-in for VMware vSphere. Para obtener información sobre los roles de VMware vSphere, consulte ["Roles predefinidos incluidos en el SnapCenter Plug-in for VMware vSphere"](#).

Pasos

1. En el panel de navegación izquierdo, 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 grupo de trabajo:

Para este campo...	Haz esto...
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 agregar el usuario a un rol. De forma predeterminada, se completa previamente con el nombre de dominio del que se inició sesión.  Debes registrar el dominio no confiable en la página Configuración > Configuración global > Configuración del dominio.
Tipo	Seleccione Usuario o Grupo  SnapCenter solo admite el grupo de seguridad y no el grupo de distribución.
Nombre de usuario	a. Escriba el nombre de usuario parcial y luego haga clic en Agregar.  El nombre de usuario distingue entre mayúsculas y minúsculas. b. Seleccione el nombre de usuario de 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 completo porque no hay una lista de búsqueda para usuarios de dominios cruzados. Repita este paso para agregar usuarios o grupos adicionales al rol seleccionado.
Roles	Seleccione el rol al que desea agregar el usuario.

4. Haga clic en **Asignar** y, a continuación, en la página Asignar activos:

- Seleccione el tipo de activo de la lista desplegable **Activo**.
- En la tabla Activos, seleccione el activo.

Los activos se enumeran solo si el usuario los ha agregado 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.

Configurar los ajustes del registro de auditoría

Se generan registros de auditoría para todas y cada una de las actividades del servidor SnapCenter . De forma predeterminada, los registros de auditoría están protegidos en la ubicación de instalación predeterminada *C:\Program Files\ NetApp\ SnapCenter WebApp\audit*.

Los registros de auditoría se protegen mediante la generación de un resumen firmado digitalmente para cada evento de auditoría para protegerlos de modificaciones no autorizadas. Los resúmenes generados se mantienen en un archivo de suma de verificación de auditoría separado y se someten a controles de integridad periódicos para garantizar la integridad del contenido.

Deberías haber iniciado sesión como rol "SnapCenterAdmin".

Acerca de esta tarea

- Las alertas se envían en los siguientes escenarios:
 - La programación de verificación de integridad del registro de auditoría o el servidor Syslog está habilitado o deshabilitado
 - Comprobación de la integridad del registro de auditoría, registro de auditoría o error del registro del servidor Syslog
 - Poco espacio en disco
- El correo electrónico se envía sólo cuando falla la verificación de integridad.
- Debes modificar las rutas del directorio del registro de auditoría y del directorio del registro de suma de comprobación de auditoría juntas. No puedes modificar sólo uno de ellos.
- Cuando se modifican las rutas del directorio del registro de auditoría y del directorio del registro de suma de comprobación de auditoría, no se puede realizar la verificación de integridad en los registros de auditoría presentes en la ubicación anterior.
- Las rutas del directorio del registro de auditoría y del directorio del registro de suma de comprobación de auditoría deben estar en la unidad local del servidor SnapCenter .

No se admiten unidades compartidas o montadas en red.

- Si se utiliza el protocolo UDP en la configuración del servidor Syslog, los errores debidos 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando Get-Help command_name. Alternativamente, también puede consultar el ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Pasos

1. En la página **Configuración**, navegue a **Configuración > Configuración global > Configuración del registro de auditoría**.
2. En la sección Registro de auditoría, ingrese los detalles.
3. Ingrese al **Directorio de registro de auditoría** y al **Directorio de registro de suma de comprobación de auditoría**
 - a. Introduzca el tamaño máximo del archivo
 - b. Introduzca el máximo de archivos de registro
 - c. Introduzca el porcentaje de uso del espacio en disco para enviar una alerta
4. (Opcional) Habilitar **Registrar hora UTC**.
5. (Opcional) Habilite **Programación de verificación de integridad del registro de auditoría** y haga clic en **Iniciar verificación de integridad** para realizar una verificación de integridad a pedido.

También puede ejecutar el comando **Start-SmAuditIntegrityCheck** para iniciar una verificación de integridad a pedido.

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

Debe importar el certificado del servidor Syslog a la 'Raíz confiable' para el protocolo TLS 1.2.

- a. Ingresar al host del servidor Syslog
 - b. Ingrese el puerto del servidor Syslog
 - c. Introducir el protocolo del servidor Syslog
 - d. Ingresar formato RFC
7. Haga clic en **Guardar**.
 8. Puede ver las comprobaciones de integridad de auditoría y de espacio en disco haciendo clic en **Monitor > Trabajos**.

Configurar conexiones MySQL seguras con SnapCenter Server

Puede generar certificados de capa de sockets seguros (SSL) y archivos de clave si desea proteger la comunicación entre SnapCenter Server y MySQL Server en configuraciones independientes o configuraciones de equilibrio de carga de red (NLB).

Configurar conexiones MySQL seguras para configuraciones independientes de SnapCenter Server

Puede generar certificados de capa de sockets seguros (SSL) y archivos de clave si desea proteger la comunicación entre SnapCenter Server y MySQL Server. Debe configurar los certificados y los archivos de clave en el servidor MySQL y en el servidor SnapCenter .

Se generan los siguientes certificados:

- Certificado CA
- Certificado público del servidor y archivo de clave privada
- Certificado público del cliente y archivo de clave privada

Pasos

1. Configure los certificados SSL y los archivos de clave para servidores y clientes MySQL en Windows mediante el comando openssl.

Para obtener más información, consulte ["MySQL versión 5.7: Creación de certificados y claves SSL mediante openssl"](#)



El valor del nombre común que se utiliza para el certificado del servidor, el certificado del cliente y los archivos de clave debe ser diferente del valor del nombre común que se utiliza para el certificado de CA. Si los valores del nombre común son los mismos, los archivos de certificado y de clave fallan en los servidores compilados mediante OpenSSL.

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

2. Copie los certificados SSL y los archivos de clave a la carpeta MySQL Data.

La ruta de la carpeta de datos MySQL predeterminada es

C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

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

La ruta del archivo de configuración del servidor MySQL predeterminado (my.ini) es

C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini.



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

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

El siguiente ejemplo muestra los certificados y archivos de clave 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"
```

El siguiente ejemplo muestra las rutas actualizadas en la sección [client] del archivo my.ini.

```
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 SnapCenter Server en Internet Information Server (IIS).
5. Reinicie el servicio MySQL.
6. Actualice el valor de la clave MySQLProtocol en el archivo .Web.UI.dll.config de SnapManager.

El siguiente ejemplo muestra el valor de la clave MySQLProtocol actualizada en el archivo .Web.UI.dll.config de SnapManager.

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

7. Actualice el archivo .Web.UI.dll.config de SnapManager con las rutas que se proporcionaron en la sección [client] del archivo my.ini.

El siguiente ejemplo muestra las rutas actualizadas en la sección [client] del archivo my.ini.

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

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

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

8. Inicie la aplicación web SnapCenter Server en IIS.

Configurar conexiones MySQL seguras para configuraciones de alta disponibilidad

Puede generar certificados de capa de sockets seguros (SSL) y archivos de clave para ambos nodos de alta disponibilidad (HA) si desea proteger la comunicación entre SnapCenter Server y los servidores MySQL. Debe configurar los certificados y los archivos de clave en los servidores MySQL y en los nodos HA.

Se generan los siguientes certificados:

- Certificado CA

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

- Archivos de certificado público del servidor y de clave privada del servidor para ambos nodos de alta disponibilidad
- Certificado público del cliente y archivos de clave privada del cliente para ambos nodos de alta disponibilidad

Pasos

1. Para el primer nodo HA, configure los certificados SSL y los archivos de clave para los servidores y clientes MySQL en Windows mediante el comando openssl.

Para obtener más información, consulte ["MySQL versión 5.7: Creación de certificados y claves SSL mediante openssl"](#)



El valor del nombre común que se utiliza para el certificado del servidor, el certificado del cliente y los archivos de clave debe ser diferente del valor del nombre común que se utiliza para el certificado de CA. Si los valores del nombre común son los mismos, los archivos de certificado y de clave fallan en los servidores compilados mediante OpenSSL.

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

2. Copie los certificados SSL y los archivos de clave a la carpeta MySQL Data.

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

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

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



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

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

El siguiente ejemplo muestra los certificados y los archivos de clave 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"
```

El siguiente ejemplo muestra las rutas actualizadas en la sección [client] del archivo my.ini.

```
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 el certificado público del servidor, los archivos de clave privada del servidor, el certificado público del cliente y los archivos de clave privada del cliente. Realice los siguientes pasos:

- a. Copie el certificado CA generado en el primer nodo HA a la carpeta de datos MySQL del segundo nodo NLB.

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



No debe volver a crear un certificado CA. Debe crear únicamente el certificado público del servidor, el certificado público del cliente, el archivo de clave privada del servidor y el archivo de clave privada del cliente.

- b. Para el primer nodo HA, configure los certificados SSL y los archivos de clave para los servidores y clientes MySQL en Windows mediante el comando openssl.

["MySQL versión 5.7: Creación de certificados y claves SSL mediante openssl"](#)



El valor del nombre común que se utiliza para el certificado del servidor, el certificado del cliente y los archivos de clave debe ser diferente del valor del nombre común que se utiliza para el certificado de CA. Si los valores del nombre común son los mismos, los archivos de certificado y de clave fallan en los servidores compilados mediante OpenSSL.

Se recomienda utilizar el FQDN del servidor como nombre común para el certificado del servidor.

- c. Copie los certificados SSL y los archivos de clave a la carpeta MySQL Data.

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



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

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

El siguiente ejemplo muestra los certificados y los archivos de clave 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"
```

El siguiente ejemplo muestra las rutas actualizadas en la sección [client] del archivo my.ini.

```
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 SnapCenter Server en Internet Information Server (IIS) en ambos nodos de alta disponibilidad.
6. Reinicie el servicio MySQL en ambos nodos HA.
7. Actualice el valor de la clave MySQLProtocol en el archivo .Web.UI.dll.config de SnapManager para ambos nodos HA.

El siguiente ejemplo muestra el valor de la clave MySQLProtocol actualizada en el archivo .Web.UI.dll.config de SnapManager.

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

8. Actualice el archivo .Web.UI.dll.config de SnapManager con las rutas que especificó en la sección [client] del archivo my.ini para ambos nodos de HA.

El siguiente ejemplo muestra las rutas actualizadas en la sección [client] de los archivos my.ini.

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

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

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

9. Inicie la aplicación web SnapCenter Server en IIS en ambos nodos de alta disponibilidad.
10. Utilice el cmdlet de PowerShell Set-SmRepositoryConfig -RebuildSlave -Force con la opción -Force en uno de los nodos de alta disponibilidad para establecer una replicación MySQL segura en ambos nodos de alta disponibilidad.

Incluso si el estado de replicación es saludable, la opción -Force le permite reconstruir el repositorio esclavo.

Configurar la autenticación basada en certificados

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

Habilitar la autenticación basada en certificados

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

- Para habilitar la autenticación basada en certificado de cliente:

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

- Para deshabilitar la autenticación basada en certificado de cliente:

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

Exportar certificados de autoridad de certificación (CA) desde SnapCenter Server

Debe exportar los certificados de CA desde el servidor SnapCenter a los hosts del complemento mediante la consola de administración de Microsoft (MMC).

Antes de empezar

Deberías haber configurado el SSL bidireccional.

Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y haga clic en **Archivo > Agregar o quitar complemento**.
2. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
3. En la ventana Complemento de certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
4. Haga clic en **Raíz de consola > Certificados - Equipo local > Personal > Certificados**.
5. Haga clic con el botón derecho en el certificado CA adquirido, que se utiliza para SnapCenter Server y luego seleccione **Todas las tareas > Exportar** para iniciar el asistente de exportación.
6. Realice las siguientes acciones en el asistente.

Para esta opción...	Haz lo siguiente...
Exportar clave privada	Seleccione No, no exportar la clave privada y luego haga clic en Siguiente .
Formato de archivo de exportación	Haga clic en Siguiente .
Nombre del archivo	Haga clic en Explorar y especifique la ruta del archivo para guardar el certificado y haga clic en Siguiente .
Cómo completar el Asistente para exportar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la exportación.



La autenticación basada en certificados no es compatible con las configuraciones de SnapCenter HA ni con el SnapCenter Plug-in for VMware vSphere.

Importar certificado de CA a los hosts del complemento de Windows

Para utilizar el certificado CA de SnapCenter Server exportado, debe importar el certificado relacionado a los hosts del complemento de Windows de SnapCenter mediante la consola de administración de Microsoft (MMC).

Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y haga clic en **Archivo > Agregar o quitar complemento**.
2. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
3. En la ventana Complemento de certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
4. Haga clic en **Raíz de consola > Certificados - Equipo local > Personal > Certificados**.
5. Haga clic derecho en la carpeta "Personal" y luego seleccione **Todas las tareas > Importar** para iniciar el asistente de importación.
6. Realice las siguientes acciones en el asistente.

Para esta opción...	Haz lo siguiente...
Ubicación de la tienda	Haga clic en Siguiente .
Archivo a importar	Seleccione el certificado de SnapCenter Server que termina con la extensión .cer.
Tienda de certificados	Haga clic en Siguiente .
Cómo completar el Asistente para exportar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.

Importar certificado CA a los hosts del complemento UNIX

Debe importar el certificado CA a los hosts del complemento UNIX.

Acerca de esta tarea

- Puede administrar la contraseña para el almacén de claves SPL y el alias del par de claves firmadas por CA en uso.
- La contraseña para el almacén de claves SPL y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves SPL desde el archivo de propiedades SPL. Es el valor correspondiente a la clave `SPL_KEYSTORE_PASS`.
2. Cambiar la contraseña del almacén de claves:

```
$ keytool -storepasswd -keystore keystore.jks
```
3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a 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` en `spl.properties` archivo.
5. Reinicie el servicio después de cambiar la contraseña.

Configurar certificados raíz o intermedios para el almacén de confianza SPL

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves SPL: `/var/opt/snapcenter/spl/etc`.
2. Localizar el archivo `keystore.jks`.
3. Enumere los certificados agregados en el almacén de claves:

```
$ keytool -list -v -keystore keystore.jks
```
4. Agregar un certificado raíz o intermedio:

```
$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks
```
5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza SPL.

Configurar el par de claves firmadas de CA para el almacén de confianza SPL

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del SPL `/var/opt/snapcenter/spl/etc`.
2. Localizar el archivo `keystore.jks``.
3. Enumere los certificados agregados en el almacén de claves:

```
$ keytool -list -v -keystore keystore.jks
```
4. Agregue el certificado CA que tenga clave privada y pública.

```
$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```
5. Enumere los certificados agregados en el almacén de claves.

```
$ keytool -list -v -keystore keystore.jks
```
6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada para el certificado de CA a la contraseña del almacén de claves.

La contraseña del almacén de claves SPL predeterminada es el valor de la clave `SPL_KEYSTORE_PASS` en `spl.properties` archivo.

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

8. Si el nombre de alias en el certificado de CA es largo y contiene espacios o caracteres especiales ("`*`", "`,`", "`,`"), cambie el nombre de alias a un nombre simple:

```
$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
```

- Configure el nombre de alias del almacén de claves ubicado en `spl.properties` archivo. Actualice este valor con la clave `SPL_CERTIFICATE_ALIAS`.
- Reinicie el servicio después de configurar el par de claves firmadas por CA en el almacén de confianza SPL.

Exportar certificados de SnapCenter

Debe exportar los certificados de SnapCenter en formato .pfx.

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Exportar clave privada	Seleccione la opción Sí, exportar la clave privada y luego haga clic en Siguiente .
Formato de archivo de exportación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Archivo para exportar	Especifique un nombre de archivo para el certificado exportado (debe usar .pfx) y luego haga clic en Siguiente .
Cómo completar el Asistente para exportar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la exportación.

Configurar el certificado CA para el host de Windows

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Huella digital**.
 - d. Copia los caracteres hexadecimales del cuadro.
 - e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

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

```
Get-ChildItem -Path Certificado:\LocalMachine\Mi
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
```

. Vincule el certificado recién instalado con los servicios del complemento de host de Windows, ejecutando 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 de SnapCenter

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

Pasos

1. Abra el Administrador de IIS en el servidor Windows donde está instalado SnapCenter .
2. En el panel de navegación izquierdo, haga clic en **Conexiones**.
3. Amplíe 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** y haga clic en **Enlaces**.
6. En la página Enlaces, seleccione **enlace para https**.
7. Haga clic en **Editar**.
8. En la lista desplegable del certificado SSL, seleccione el certificado SSL importado recientemente.
9. Haga clic en **Aceptar**.



El sitio del Programador de SnapCenter (puerto predeterminado: 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 CA. Sin embargo, si su entorno le exige utilizar un certificado CA, repita los pasos 5 a 9 utilizando el sitio del Programador de SnapCenter .



Si el certificado CA implementado recientemente no aparece en el menú desplegable, verifique si el certificado CA está asociado con la clave privada.



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

Habilitar certificados CA para SnapCenter

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

Antes de empezar

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

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Pasos

1. En la página Configuración, navegue a **Configuración > Configuración global > Configuración del certificado CA**.
2. Seleccione **Habilitar validación de certificado**.
3. Haga clic en **Aplicar**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

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



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Configurar el certificado 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 los servicios SnapCenter .

Configurar 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 *ssl_certificate* y *ssl_certificate_key* para que apunten al certificado de CA.
5. Guarde y cierre el archivo.
6. Recargar nginx: `$nginx -s reload`

Configurar el certificado de registro de auditoría

Pasos

1. Abra *INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config* usando 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 la contraseña del certificado CA respectivamente.

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

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

Configurar el certificado de servicios 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*
 - *DIR_DE_INSTALACIÓN/NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
 - *DIR_DE_INSTALACIÓN/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 y la contraseña del certificado CA respectivamente.

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

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

Configurar y habilitar la comunicación SSL bidireccional en el host de Windows

Configurar la comunicación SSL bidireccional en el host de Windows

Debe configurar la comunicación SSL bidireccional para proteger la comunicación mutua entre SnapCenter Server en el host de Windows y los complementos.

Antes de empezar

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

Para más detalles, consulte ["Sección de configuración del certificado CA."](#)

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

No se admite un entorno con algunos hosts o servidores no habilitados para la comunicación SSL bidireccional.

Pasos

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

- a. Elimine el enlace del puerto del 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. Vincule el certificado 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 del certificado de CA, agregue el usuario del servidor web IIS predeterminado de SnapCenter **"IIS AppPool\ SnapCenter"** en la lista de permisos de certificado realizando los siguientes pasos para acceder al certificado de CA recién adquirido.
 - a. Vaya a la consola de administración de Microsoft (MMC) y haga clic en **Archivo > Agregar o quitar complemento**.
 - b. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
 - c. En la ventana del complemento Certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
 - d. Haga clic en **Raíz de consola > Certificados – Equipo local > Personal > Certificados**.
 - e. Seleccione el certificado de SnapCenter .
 - f. Para iniciar el asistente para agregar usuarios y permisos, haga clic con el botón derecho en el certificado de CA y seleccione **Todas las tareas > Administrar claves privadas**.
 - g. Haga clic en **Agregar**, en el asistente Seleccionar usuarios y grupos cambie la ubicación al nombre de la computadora local (la superior en la jerarquía)
 - h. Agregue el usuario IIS AppPool\ SnapCenter y otorgue permisos de control total.
3. Para obtener el permiso IIS del certificado CA, agregue la nueva entrada de claves de registro DWORD en SnapCenter Server desde la siguiente ruta:

En el editor de registro de Windows, navegue hasta la ruta mencionada a continuación,

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProvd  
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
```

Configurar el complemento de Windows de SnapCenter para la comunicación SSL bidireccional

Debe configurar el complemento 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 vincular el puerto, realice las siguientes acciones en el host del complemento de Windows para el puerto SMCore 8145 (predeterminado).
 - a. Elimine el enlace del puerto del 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. Vincula el certificado 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
```

Habilitar la comunicación SSL bidireccional en el host de Windows

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

Antes de empezar

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

Pasos

1. Para habilitar la comunicación SSL bidireccional, ejecute los siguientes comandos en el servidor SnapCenter para los complementos, el servidor y para cada uno de los agentes para los que se requiere 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"}
```

2. Realice la operación de reciclaje del grupo de aplicaciones de IIS SnapCenter mediante el siguiente comando.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Para los complementos de Windows, reinicie el servicio SMCore ejecutando el siguiente comando de PowerShell:

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

Deshabilitar la comunicación SSL bidireccional

Puede deshabilitar la comunicación SSL bidireccional mediante comandos de PowerShell.

Acerca de esta tarea

- Ejecute primero los comandos para todos los complementos y el agente SMCore y luego para el servidor.
- Al deshabilitar la comunicación SSL bidireccional, el certificado CA y su configuración no se eliminan.
- Para agregar un nuevo host a SnapCenter Server, debe deshabilitar el SSL bidireccional para todos los hosts del complemento.
- NLB y F5 no son compatibles.

Pasos

1. Para deshabilitar la comunicación SSL bidireccional, ejecute los siguientes comandos en SnapCenter Server para todos los hosts del complemento 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"}
```

2. Realice la operación de reciclaje del grupo de aplicaciones de IIS SnapCenter mediante el siguiente comando.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Para los complementos de Windows, reinicie el servicio SMCore ejecutando el siguiente comando de PowerShell:

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

Configurar y habilitar la comunicación SSL bidireccional en el host Linux

Configurar la comunicación SSL bidireccional en el host Linux

Debe configurar la comunicación SSL bidireccional para proteger la comunicación mutua entre SnapCenter Server en el host Linux y los complementos.

Antes de empezar

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

Pasos

1. Copie **certificate.pem** a */etc/pki/ca-trust/source/anchors/*.
2. Agregue los certificados en la lista de confianza de su 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. Verifique si los certificados se agregaron 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 SnapCenter .
6. Actualice los valores de las siguientes claves en * SnapManager.Web.UI.dll.config* ubicado en *_/<ruta de instalación>/ NetApp/snapcenter/SnapManagerWeb_* y * SMCoreServiceHost.dll.config* ubicado en */<ruta de instalación>/ NetApp/snapcenter/SMCore*.
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<ruta del certificado.pfx>" />`
 - `<add key="CONTRASEÑA_DEL_CERTIFICADO_DE_SERVICIO" value="<contraseña>" />`
7. Reinicie los siguientes servicios.
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. Verifique que el certificado esté adjunto al puerto web de SnapManager .
`openssl s_client -connect localhost:8146 -brief`
9. Verifique que el certificado esté adjunto al puerto smcore.

```
openssl s_client -connect localhost:8145 -brief
```

10. Administrar la contraseña para el almacén de claves y alias de SPL.

- Recupere la contraseña predeterminada del almacén de claves SPL asignada a la clave **SPL_KEYSTORE_PASS** en el archivo de propiedades SPL.
- Cambiar la contraseña del almacén de claves.
`keytool -storepasswd -keystore keystore.jks`
- Cambiar la contraseña de todos los alias de las entradas de clave privada.
`keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
- Actualice la misma contraseña para la clave **SPL_KEYSTORE_PASS** en *spl.properties*.
- Reiniciar el servicio.

11. En el host Linux del complemento, agregue los certificados raíz e intermedio en el almacén de claves del complemento 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`
 - Compruebe las entradas en keystore.jks.
`keytool -list -v -keystore <path to keystore.jks>`
 - 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 de **certificate.pfx** almacenado en *keystore.jks* y reinicie el servicio SPL: `systemctl restart spl`

13. Verifique que el certificado esté adjunto al puerto smcore.

```
openssl s_client -connect localhost:8145 -brief
```

Habilitar la comunicación SSL en el host Linux

Puede habilitar la comunicación SSL bidireccional para proteger la comunicación mutua entre SnapCenter Server en el host Linux y los complementos mediante comandos de PowerShell.

Paso

- Realice lo siguiente para habilitar la comunicación SSL unidireccional.
 - Inicie sesión en la GUI de SnapCenter .
 - Haga clic en **Configuración** > **Configuración global** y seleccione **Habilitar validación de certificado en SnapCenter Server**.
 - Haga clic en **Hosts** > **Hosts administrados** y seleccione el host de complemento para el que desea habilitar SSL unidireccional.
 - Hacer clic  icono y, a continuación, haga clic en **Habilitar validación de certificado**.

2. Habilite 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"}`

Configurar Active Directory, LDAP y LDAPS

Registrar dominios de Active Directory que no sean de confianza

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

Antes de empezar

Protocolos LDAP y LDAPS

- Puede registrar los dominios de directorio activo que no sean de confianza mediante el protocolo LDAP o LDAPS.
- Debería haber habilitado la comunicación bidireccional entre los hosts del complemento y el servidor SnapCenter .
- La resolución de DNS debe configurarse desde el servidor SnapCenter a los hosts del complemento y viceversa.

Protocolo LDAP

- El nombre de dominio completo (FQDN) debe poder resolverse desde 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 controlador de dominio y esto debería poder resolverse desde el servidor SnapCenter .

Protocolo LDAPS

- Se requieren certificados CA para que LDAPS proporcione cifrado de extremo a extremo durante la comunicación del directorio activo.

["Configurar el certificado de cliente de CA para LDAPS"](#)

- Los nombres de host del controlador de dominio (DCHostName) deben ser accesibles desde SnapCenter Server.

Acerca de esta tarea

- Puede utilizar la interfaz de usuario de SnapCenter , los cmdlets de PowerShell o la API REST para registrar un dominio no confiable.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Configuración global**.
3. En la página Configuración global, haga clic en **Configuración de dominio**.
4. Hacer 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 no confiable para LDAP:

Para este campo...	Haz esto...
Nombre de dominio	Especifique el nombre NetBIOS para el dominio.
FQDN del dominio	Especifique el FQDN y haga clic en Resolver .
Direcciones IP del controlador de dominio	Si el FQDN del dominio no se puede resolver desde el servidor SnapCenter , especifique una o más direcciones IP de controlador de dominio. Para obtener más información, consulte "Agregar la IP del controlador de dominio para un dominio no confiable desde la GUI" .

- b. Si selecciona **LDAPS**, especifique la información necesaria para registrar el dominio no confiable para LDAPS:

Para este campo...	Haz esto...
Nombre de dominio	Especifique el nombre NetBIOS para el dominio.
FQDN del dominio	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 del controlador de dominio no se pueden resolver desde SnapCenter Server, debe rectificar las resoluciones de DNS.

6. Haga clic en **Aceptar**.

Configurar los grupos de aplicaciones de IIS para habilitar los permisos de lectura de Active Directory

Puede configurar Internet Information Services (IIS) en su servidor Windows para crear una cuenta de grupo de aplicaciones personalizada cuando necesite habilitar permisos de lectura de Active Directory para SnapCenter.

Pasos

1. Abra el Administrador de IIS en el servidor Windows donde está instalado SnapCenter .
2. En el panel de navegación izquierdo, haga clic en **Grupos de aplicaciones**.
3. Seleccione SnapCenter en la lista de Grupos de aplicaciones y luego haga clic en **Configuración avanzada** en el panel Acciones.
4. Seleccione Identidad y luego haga clic en ... para editar la identidad del grupo de aplicaciones de SnapCenter .
5. En el campo Cuenta personalizada, ingrese un nombre de cuenta 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 ApplicationPoolIdentity incorporada para el grupo de aplicaciones de SnapCenter .

Configurar el certificado de cliente de CA para LDAPS

Debe configurar el certificado de cliente de CA para LDAPS en el servidor SnapCenter cuando LDAPS de Windows Active Directory esté configurado con los certificados de CA.

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
En la segunda página del asistente	Haga clic en Explorar , seleccione el <i>Certificado raíz</i> y haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.

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

Proteger las bases de datos de Microsoft SQL Server

Complemento de SnapCenter para Microsoft SQL Server

Descripción general del complemento de SnapCenter para Microsoft SQL Server

El complemento SnapCenter para Microsoft SQL Server es un componente del lado del host del software SnapCenter de NetApp que permite la gestión de protección de datos teniendo en cuenta las aplicaciones de las bases de datos de Microsoft SQL Server. El complemento para SQL Server automatiza las operaciones de copia de seguridad, verificación, restauración y clonación de bases de datos de SQL Server en su entorno de SnapCenter .

Cuando se instala el complemento para SQL Server, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen y con la tecnología NetApp SnapVault para realizar replicación de copias de seguridad de disco a disco para fines de cumplimiento de estándares o de archivo.

- Automatiza operaciones de copia de seguridad, restauración y clonación basadas en aplicaciones para bases de datos de Microsoft SQL Server en su entorno de SnapCenter .
- Admite bases de datos de Microsoft SQL Server en VMDK y LUN de asignación de dispositivos sin procesar (RDM) cuando implementa el SnapCenter Plug-in for VMware vSphere y registra el complemento con SnapCenter
- Admite únicamente el aprovisionamiento de recursos compartidos SMB. No se proporciona soporte para realizar copias de seguridad de bases de datos de SQL Server en recursos compartidos SMB.
- Admite la importación de copias de seguridad de SnapManager para Microsoft SQL Server a SnapCenter.

Qué puede hacer con el complemento SnapCenter para Microsoft SQL Server

Cuando el complemento de SnapCenter para Microsoft SQL Server está instalado en su entorno, puede usar SnapCenter para realizar copias de seguridad, restaurar y clonar bases de datos de SQL Server.

Puede realizar las siguientes tareas que admiten operaciones de copia de seguridad, operaciones de restauración y operaciones de clonación de bases de datos y recursos de bases de datos de SQL Server:

- Realizar copias de seguridad de las bases de datos de SQL Server y los registros de transacciones asociados

No se puede crear una copia de seguridad del registro para las bases de datos del sistema master y msdb. Sin embargo, puede crear copias de seguridad de registros para la base de datos del sistema modelo.

- Restaurar recursos de la base de datos
 - Puede restaurar bases de datos del sistema maestro, bases de datos del sistema msdb y bases de datos del sistema modelo.

- No se pueden restaurar varias bases de datos, instancias y grupos de disponibilidad.
- No se puede restaurar la base de datos del sistema a una ruta alternativa.

- Crear clones puntuales de bases de datos de producción

No se pueden realizar operaciones de copia de seguridad, restauración, clonación y ciclo de vida de clonación en las bases de datos del sistema tempdb.

- Verificar las operaciones de respaldo inmediatamente o posponer la verificación hasta más tarde

No se admite la verificación de la base de datos del sistema SQL Server. SnapCenter clona las bases de datos para realizar la 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 respaldo y operaciones de clonación
- Supervisar operaciones de copia de seguridad, operaciones de restauración y operaciones de clonación



El complemento para SQL Server no admite la copia de seguridad ni la recuperación de bases de datos de SQL Server en recursos compartidos SMB.

Funciones del complemento SnapCenter para Microsoft SQL Server

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

El complemento para SQL Server incluye estas características principales:

- **Interfaz gráfica de usuario unificada impulsada por SnapCenter**

La interfaz de SnapCenter le proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite completar procesos de copia de seguridad y restauración consistentes en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y monitorear trabajos en todos los complementos. SnapCenter también ofrece programación centralizada y gestión de políticas para respaldar operaciones de copia de seguridad y clonación.

- **Administración central automatizada**

Puede programar copias de seguridad rutinarias de SQL Server, configurar la retención de copias de seguridad basada en políticas y configurar operaciones de restauración en un punto en el tiempo y actualizadas al minuto. También puede supervisar de forma proactiva su entorno de SQL Server configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología NetApp Snapshot sin interrupciones**

El complemento para SQL Server utiliza la tecnología NetApp Snapshot con el complemento NetApp SnapCenter para Microsoft Windows. Esto le permite realizar copias de seguridad de bases de datos en segundos y restaurarlas rápidamente sin desconectar SQL Server. Las instantáneas consumen un espacio de almacenamiento mínimo.

Además de estas características principales, el complemento para SQL Server ofrece los siguientes beneficios:

- Soporte para flujos de trabajo de copia de seguridad, restauración, clonación y verificación
- Seguridad respaldada por RBAC y delegación de roles centralizada
- Creación de copias puntuales y con uso eficiente del espacio de bases de datos de producción para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

Se requiere una licencia FlexClone en el sistema de almacenamiento que contiene el clon.

- Verificación de copias de seguridad automatizada y sin interrupciones
- Capacidad de ejecutar múltiples copias de seguridad al mismo tiempo en varios servidores
- Cmdlets de PowerShell para la creación de scripts de operaciones de copia de seguridad, verificación, restauración y clonación
- Compatibilidad con grupos de disponibilidad AlwaysOn (AG) en SQL Server para acelerar las operaciones de configuración, copia de seguridad y restauración de AG
- Base de datos en memoria y extensión de grupo de búfer (BPE) como parte de SQL Server 2014
- Soporte para copias de seguridad de LUN y discos de máquinas virtuales (VMDK)
- Soporte para infraestructuras físicas y virtualizadas
- Compatibilidad con iSCSI, Fibre Channel, FCoE, mapeo de dispositivos sin procesar (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 express (NVMe) en Windows Server 2022
 - Flujos de trabajo de copia de seguridad, restauración, clonación y verificación en el diseño VMDK creado en NVMe a través de TCP/IP.
 - Admite la versión de firmware NVMe 1.3 a partir de la actualización 2 de ESX 8.0 y requiere la versión de hardware virtual 21.
 - El clúster de conmutación por error de Windows Server (WSFC) no es compatible con aplicaciones a través de VMDK en NVMe sobre TCP/IP.
- Admite la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios comerciales sigan funcionando incluso en caso de una falla total del sitio, permitiendo que las aplicaciones conmuten por error de manera transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una conmutación por error con la sincronización activa de SnapMirror .

Compatibilidad con la asignación asimétrica de LUN en clústeres de Windows

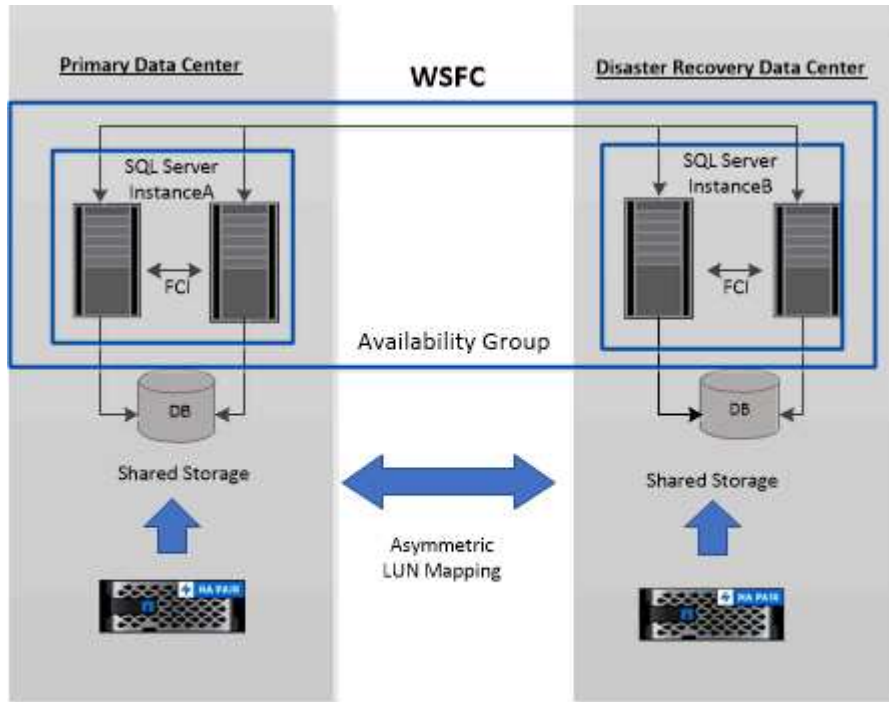
El complemento SnapCenter para Microsoft SQL Server admite la detección en SQL Server 2012 y versiones posteriores, configuraciones de asignación de LUN asimétrica (ALM) para alta disponibilidad y grupos de disponibilidad para recuperación ante desastres. Al descubrir recursos, SnapCenter descubre bases de datos en hosts locales y en hosts remotos en configuraciones de ALM.

Una configuración de ALM es un único clúster de conmutación por error de servidor Windows que contiene uno o más nodos en un centro de datos principal y uno o más nodos en un centro de recuperación ante

desastres.

A continuación se muestra un ejemplo de una configuración de ALM:

- Dos instancias de clúster de conmutación por error (FCI) en un centro de datos de varios sitios
- FCI para alta disponibilidad (HA) local y grupo de disponibilidad (AG) para recuperación ante desastres con una instancia independiente en el sitio 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 en el centro de datos principal no es visible para los nodos del centro de datos de recuperación ante desastres, y viceversa.

La arquitectura ALM combina dos soluciones de almacenamiento compartido utilizadas por FCI, con una solución de almacenamiento dedicada o no compartida utilizada por SQL AG. La solución AG utiliza letras de unidad idénticas para los recursos de disco compartidos en los 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 complemento SnapCenter para Microsoft SQL Server

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas físicas como virtuales. Debe verificar si hay soporte disponible para su tipo de almacenamiento antes de instalar el paquete para su host.

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 [https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"Herramienta de matriz de interoperabilidad de NetApp\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\) .

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Servidor físico	LUN conectados a FC	Interfaz gráfica de usuario (GUI) de SnapCenter o cmdlets de PowerShell	
Servidor físico	LUN conectados a iSCSI	GUI de SnapCenter o cmdlets de PowerShell	
Servidor físico	Recursos compartidos SMB3 (CIFS) que residen en una máquina virtual de almacenamiento (SVM)	GUI de SnapCenter o cmdlets de PowerShell	Soporte únicamente para aprovisionamiento.
Máquina virtual de VMware	LUN RDM conectados mediante un HBA FC o iSCSI	Cmdlets de PowerShell	
Máquina virtual de VMware	LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI	GUI de SnapCenter o cmdlets de PowerShell	
Máquina virtual de VMware	Sistemas de archivos de máquinas virtuales (VMFS) o almacenes de datos NFS	VMware vSphere	
Máquina virtual de VMware	Un sistema invitado conectado a recursos compartidos SMB3 que residen en una SVM	GUI de SnapCenter o cmdlets de PowerShell	Soporte únicamente para aprovisionamiento.
Máquina virtual de VMware	Almacenes de datos vVol tanto en NFS como en SAN	Herramientas ONTAP para VMware vSphere	

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Máquina virtual Hyper-V	LUN de FC virtuales (vFC) conectados mediante un conmutador de canal de fibra virtual	GUI de SnapCenter o cmdlets de PowerShell	Debe utilizar Hyper-V Manager para aprovisionar LUN de FC virtual (vFC) conectados mediante un conmutador de canal de fibra virtual.  No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .
Máquina virtual Hyper-V	LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI	GUI de SnapCenter o cmdlets de PowerShell	 No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Máquina virtual Hyper-V	Un sistema invitado conectado a recursos compartidos SMB3 que residen en una SVM	GUI de SnapCenter o cmdlets de PowerShell	Soporte únicamente para aprovisionamiento.  No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .

Recomendaciones de diseño de almacenamiento para el complemento SnapCenter para Microsoft SQL Server

Un diseño de almacenamiento bien diseñado permite que SnapCenter Server realice copias de seguridad de sus bases de datos para cumplir con sus objetivos de recuperación. Debe tener en cuenta varios factores al definir el diseño de su almacenamiento, incluido el tamaño de la base de datos, la tasa de cambio de la base de datos y la frecuencia con la que realiza copias de seguridad.

Las siguientes secciones definen las recomendaciones y restricciones de diseño de almacenamiento para LUN y discos de máquinas virtuales (VMDK) con el complemento SnapCenter para Microsoft SQL Server instalado en su entorno.

En este caso, los LUN pueden incluir discos VMware RDM y LUN conectados directamente iSCSI que están asignados al invitado.

Requisitos de LUN y VMDK

Opcionalmente, puede utilizar LUN o VMDK dedicados para lograr un rendimiento y una gestión óptimos de las siguientes bases de datos:

- Bases de datos de sistemas maestros y modelos
- Base de datos temporal
- Archivos de base de datos de usuario (.mdf y .ndf)
- Archivos de registro de transacciones de la base de datos de usuario (.ldf)
- Directorio de registro

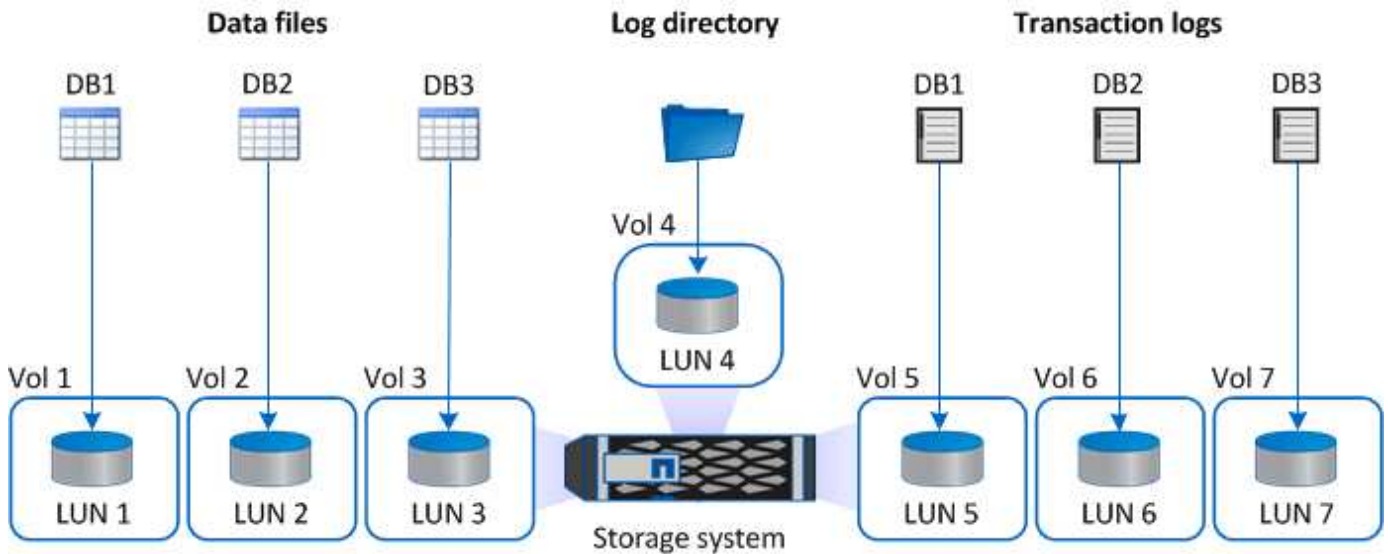
Para restaurar bases de datos grandes, la mejor práctica es utilizar LUN o VMDK dedicados. El tiempo que lleva restaurar un LUN o VMDK completo es menor que el tiempo que lleva restaurar los archivos individuales

almacenados en el LUN o VMDK.

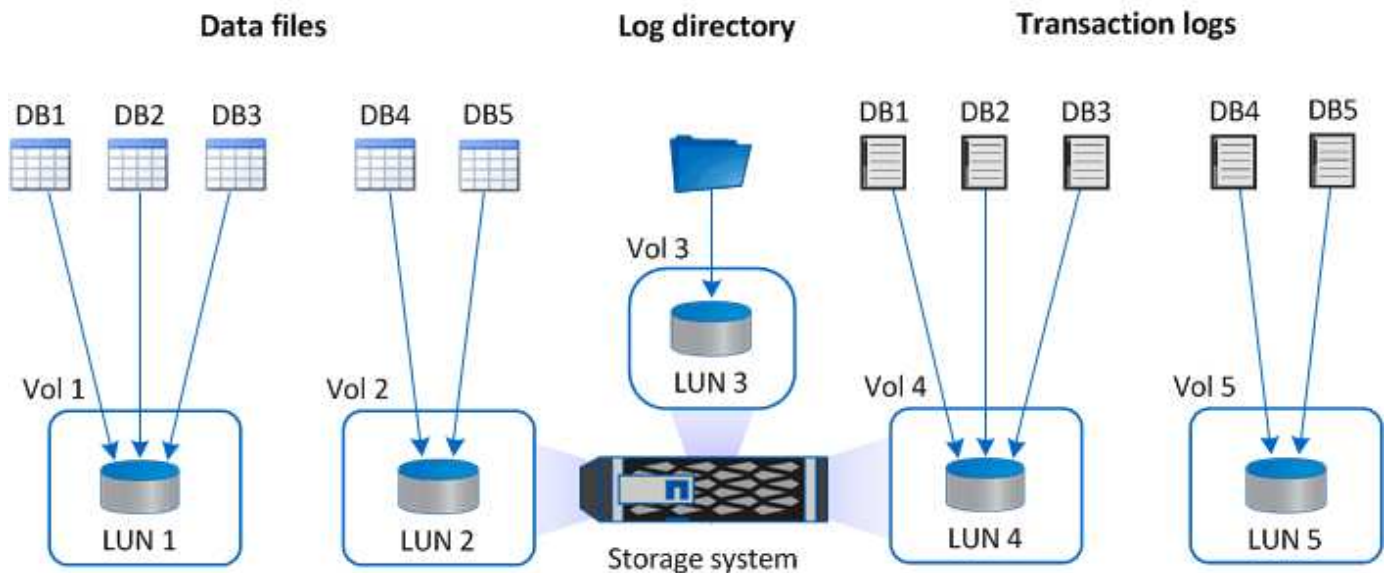
Para el directorio de registro, debe crear un LUN o VMDK separado para que haya suficiente espacio libre en los discos de datos o archivos de registro.

Diseños de muestra de LUN y VMDK

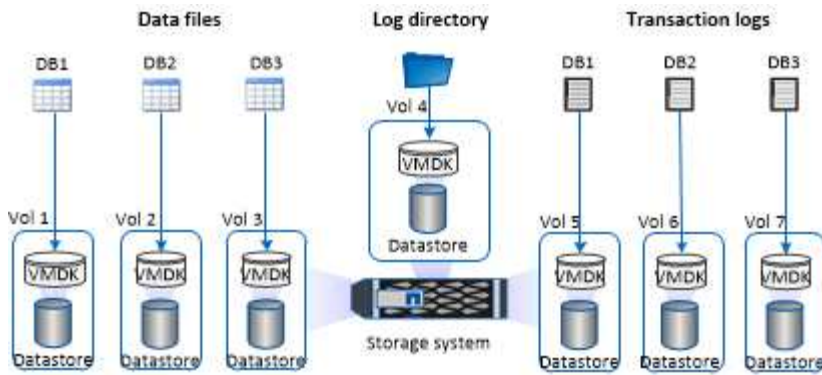
El siguiente gráfico muestra cómo puede configurar el diseño de almacenamiento para bases de datos grandes en LUN:



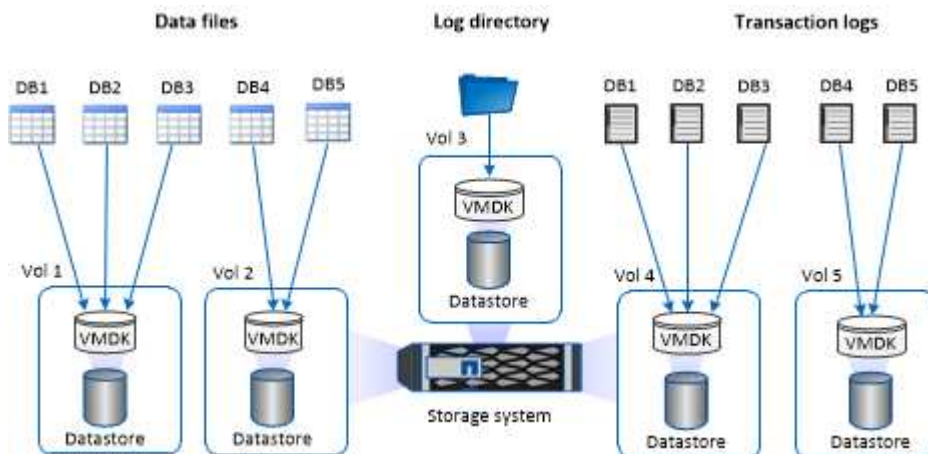
El siguiente gráfico muestra cómo puede configurar el diseño de almacenamiento para bases de datos medianas o pequeñas en LUN:



El siguiente gráfico muestra cómo puede configurar el diseño de almacenamiento para bases de datos grandes en VMDK:



El siguiente gráfico muestra cómo puede configurar el diseño de almacenamiento para bases de datos medianas o pequeñas en VMDK:



Privilegios mínimos de ONTAP necesarios para el complemento SQL

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo
 - lun crear
 - eliminar lun
 - agregar igroup lun
 - crear igroup lun
 - eliminar igroup lun
 - Cambiar nombre de igroup lun
 - Programa de igroup de Lun
 - Asignación de LUN a nodos de informes adicionales
 - creación de mapeo LUN

- eliminar mapeo lun
- Mapeo de LUN: eliminar nodos de informes
- espectáculo de mapeo de lun
- modificar lun
- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen

- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFs de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIF de vserver
- Mostrar copia de sombra de CIF de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi
- Mostrar conexión iscsi de vserver
- espectáculo vserver
- interfaz de red
- Mostrar interfaz de red
- vserver
- espectáculo del metrocluster

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el complemento para SQL Server

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Estrategia de respaldo para recursos de SQL Server

Definir una estrategia de respaldo para los recursos de SQL Server

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a garantizar que tenga los respaldos que necesita para restaurar o clonar con éxito sus bases de datos. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. El RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA, RTO y RPO contribuyen a la estrategia de respaldo.

Tipo de backups admitido

Para realizar copias de seguridad de las bases de datos del sistema y del usuario de SQL Server mediante SnapCenter, es necesario elegir el tipo de recurso, como bases de datos, instancias del servidor SQL y grupos de disponibilidad (AG). Se aprovecha la tecnología de instantáneas para crear copias en línea, de solo lectura, de los volúmenes en los que 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 también esté administrando SQL Server con otras aplicaciones de respaldo. Mantener los registros de transacciones intactos permite que cualquier aplicación de respaldo restaure las bases de datos del sistema. Las copias de seguridad de solo copia son independientes de la secuencia de copias de seguridad programadas y no afectan los procedimientos de copia de seguridad y restauración de la base de datos.

Tipo de copia de seguridad	Descripción	Opción de solo copia con tipo de copia de seguridad
Copia de seguridad completa y copia de seguridad de registros	Realiza una copia de seguridad de la base de datos del sistema y trunca los registros de transacciones. SQL Server trunca los registros de transacciones eliminando las entradas que ya están confirmadas en la base de datos. Una vez completada la copia de seguridad completa, esta opción crea un registro de transacciones que captura la información de las transacciones. Por lo general, deberías elegir esta opción. Sin embargo, si el tiempo de respaldo es corto, puede elegir no ejecutar una copia de seguridad del registro de transacciones con una copia de seguridad completa. No se puede crear una copia de seguridad del registro para las bases de datos del sistema master y msdb. Sin embargo, puede crear copias de seguridad de registros para la base de datos del sistema modelo.	Realiza una copia de seguridad de los archivos de base de datos del sistema y de los registros de transacciones sin truncar los registros. Una copia de seguridad de solo copia no puede servir como base diferencial o copia de seguridad diferencial y no afecta a la base diferencial. Restaurar una copia de seguridad completa de solo copia es lo mismo que restaurar cualquier otra copia de seguridad completa.
Copia de seguridad completa de la base de datos	Realiza una copia de seguridad de los archivos de base de datos del sistema. Puede crear una copia de seguridad completa de la base de datos para las bases de datos del sistema maestro, modelo y msdb.	Realiza una copia de seguridad de los archivos de base de datos del sistema.

Tipo de copia de seguridad	Descripción	Opción de solo copia con tipo de copia de seguridad
Copia de seguridad del registro de transacciones	Realiza una copia de seguridad de los registros de transacciones truncados, copiando solo las transacciones que se confirmaron desde que se realizó la copia de seguridad del registro de transacciones más reciente. Si programa copias de seguridad frecuentes del registro de transacciones junto con copias de seguridad completas de la base de datos, puede elegir puntos de recuperación granulares.	Realiza una copia de seguridad de los registros de transacciones sin truncarlos. Este tipo de backup no afecta la secuencia de los backups de registros regulares. Las copias de seguridad de registros de solo copia son útiles para realizar operaciones de restauración en línea.

Programaciones de copias de seguridad para el complemento para SQL Server

La frecuencia de copia de seguridad (tipo de programación) se especifica en las políticas; una programación de copia de seguridad se especifica en la configuración del grupo de recursos. El factor más crítico a la hora de determinar la frecuencia o el cronograma de una copia de seguridad es la tasa de cambio del recurso y la importancia de los datos. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su Acuerdo de Nivel de Servicio (SLA) y su Objetivo de Punto de Recuperación (RPO).

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso para un recurso muy utilizado, no es necesario ejecutar una copia de seguridad completa más de una o dos veces al día. Por ejemplo, las copias de seguridad periódicas del registro de transacciones podrían ser suficientes para garantizar que tenga las copias de seguridad que necesita. Cuanto más a menudo realice copias de seguridad de sus bases de datos, menos registros de transacciones tendrá que utilizar SnapCenter en el momento de la restauración, lo que puede generar operaciones de restauración más rápidas.

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de respaldo

La frecuencia de las copias de seguridad (con qué frecuencia se deben realizar las copias de seguridad), denominada *tipo de programación* para algunos complementos, es parte de una configuración de políticas. Puede seleccionar la frecuencia de respaldo para la política: horaria, diaria, semanal o mensual. Si no selecciona ninguna de estas frecuencias, la política creada será solo a pedido. Puede acceder a las políticas haciendo clic en **Configuración > Políticas**.

- Programaciones de copias de seguridad

Las programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad) son parte de la configuración de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para realizar copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **Grupos de recursos**.

Número de trabajos de respaldo necesarios para las bases de datos

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño de la base de datos, la cantidad de volúmenes utilizados, la tasa de cambio de la base de datos y su Acuerdo de Nivel de Servicio (SLA).

Para las copias de seguridad de bases de datos, la cantidad de trabajos de copia de seguridad que elija generalmente dependerá de la cantidad de volúmenes en los que colocó sus bases de datos. Por ejemplo, si coloca un grupo de bases de datos pequeñas en un volumen y una base de datos grande en otro volumen, puede crear un trabajo de respaldo para las bases de datos pequeñas y un trabajo de respaldo para la base de datos grande.

Convenciones de nombres de copias de seguridad para el complemento para SQL Server

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

```
resourcegroupname_hostname_timestamp
```

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, `customtext_resourcegroup_policy_hostname` o `resourcegroup_hostname`. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Opciones de retención de copias de seguridad para el complemento para SQL Server

Puede elegir la cantidad de días durante los cuales desea conservar copias de seguridad

o especificar la cantidad de copias de seguridad que desea conservar, hasta un máximo de 255 copias en ONTAP . Por ejemplo, su organización podría exigirle que conserve 10 días de copias de seguridad o 130 copias de seguridad.

Al crear una política, puede especificar las opciones de retención para el tipo de copia de seguridad y el tipo de programación.

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

SnapCenter elimina las copias de seguridad retenidas que tienen etiquetas de retención que coinciden con el tipo de programación. Si se modificó el tipo de programación del recurso o del grupo de recursos, es posible que las copias de seguridad con la etiqueta del tipo de programación anterior aún permanezcan en el sistema.



Para la retención a largo plazo de copias de seguridad, debe utilizar la copia de seguridad SnapVault .

¿Durante cuánto tiempo se deben conservar las copias de seguridad del registro de transacciones en el sistema de almacenamiento de origen?

El complemento SnapCenter para Microsoft SQL Server necesita copias de seguridad del registro de transacciones para realizar operaciones de restauración actualizadas, que restauran su base de datos a un tiempo entre dos copias de seguridad completas.

Por ejemplo, si Plug-in para SQL Server realizó una copia de seguridad completa a las 8:00 a. m. y otra copia de seguridad completa a las 5:00 p. m., podría usar la última copia de seguridad del registro de transacciones para restaurar la base de datos a cualquier momento entre las 8:00 a. m. y las 5:00 p. m. Si los registros de transacciones no están disponibles, Plug-in para SQL Server solo puede realizar operaciones de restauración en un punto en el tiempo, que restauran una base de datos al momento en que Plug-in para SQL Server completó una copia de seguridad completa.

Por lo general, se necesitan operaciones de restauración actualizadas solo por uno o dos días. De forma predeterminada, SnapCenter conserva un mínimo de dos días.

Varias bases de datos en el mismo volumen

Puede colocar todas las bases de datos en el mismo volumen, porque la política de respaldo tiene una opción para establecer el máximo de bases de datos por respaldo (el valor predeterminado es 100).

Por ejemplo, si tiene 200 bases de datos en el mismo volumen, se crean dos instantáneas con 100 bases de datos en cada una de ellas.

Verificación de copia de seguridad mediante el volumen de almacenamiento principal o secundario para el complemento para SQL Server

Puede verificar copias de seguridad en el volumen de almacenamiento principal o en el volumen de almacenamiento secundario SnapMirror o SnapVault . La verificación mediante un volumen de almacenamiento secundario reduce la carga en el volumen de almacenamiento primario.

Cuando se verifica una copia de seguridad que se encuentra en el volumen de almacenamiento primario o secundario, todas las instantáneas primarias y secundarias se marcan como verificadas.

Se requiere la licencia de SnapRestore para verificar copias de respaldo en el volumen de almacenamiento secundario SnapMirror y SnapVault .

Cuándo programar trabajos de verificación

Si bien SnapCenter puede verificar las copias de seguridad inmediatamente después de crearlas, hacerlo puede aumentar significativamente el tiempo necesario para completar el trabajo de copia de seguridad y consume muchos recursos. Por lo tanto, casi siempre es mejor programar la verificación en un trabajo separado para un momento posterior. Por ejemplo, si realiza una copia de seguridad de una base de datos a las 5:00 p. m. todos los días, puede programar que la verificación se realice una hora más tarde, a las 6:00 p. m.

Por la misma razón, normalmente no es necesario ejecutar la verificación de respaldo cada vez que se realiza una copia de seguridad. Realizar una verificación a intervalos regulares pero menos frecuentes suele ser suficiente para garantizar la integridad de la copia de seguridad. 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

Puede restaurar una base de datos de SQL Server desde una copia de seguridad en un almacenamiento primario o secundario. También puede restaurar la base de datos en diferentes destinos además de su ubicación original, lo que le permitirá elegir el destino que admita sus requisitos.

Fuentes para una operación de restauración

Puede restaurar bases de datos desde el almacenamiento primario o secundario.

Destinos para una operación de restauración

Puede restaurar bases de datos en varios destinos:

Destino	Descripción
La ubicación original	De forma predeterminada, SnapCenter restaura la base de datos en la misma ubicación en la misma instancia de SQL Server.
Una ubicación diferente	Puede restaurar la base de datos en una ubicación diferente en cualquier instancia de SQL Server dentro del mismo host.
Ubicación original o diferente utilizando nombres de bases de datos diferentes	Puede restaurar la base de datos con un nombre diferente en cualquier instancia de SQL Server en el mismo host donde se creó la copia de seguridad.



No se admite la restauración en un host alternativo entre servidores ESX para bases de datos SQL en VMDK (almacenes de datos NFS y VMFS).

Modelos de recuperación de SQL Server compatibles con SnapCenter

Se asignan modelos de recuperación específicos a cada tipo de base de datos de forma predeterminada. El administrador de la base de datos de SQL Server puede reasignar cada base de datos a un modelo de recuperación diferente.

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 copias de seguridad de los registros de transacciones.

- Modelo de recuperación completa

Cuando utiliza el modelo de recuperación completa, puede restaurar una base de datos a su estado anterior desde el punto de falla.

- Modelo de recuperación de registros masivos

Cuando utiliza el modelo de recuperación de registro masivo, debe volver a ejecutar manualmente la operación de registro masivo. Debe realizar la operación de registro masivo si no se ha realizado una copia de seguridad del registro de transacciones que contiene el registro de confirmación de la operación antes de la restauración. Si la operación de registro masivo inserta 10 millones de filas en una base de datos, y la base de datos falla antes de que se realice una copia de seguridad del registro de transacciones, la base de datos restaurada no contendrá las filas que se insertaron mediante la operación de registro masivo.

Tipos de operaciones de restauración

Puede utilizar SnapCenter para realizar distintos tipos de operaciones de restauración en recursos de SQL Server.

- Restaurar actualizado al minuto
- Restaurar a un punto anterior en el tiempo

Puede restaurar hasta el minuto o restaurar a un punto anterior en el tiempo en las siguientes situaciones:

- Restaurar desde el almacenamiento secundario de SnapMirror o SnapVault
- Restaurar a ruta alternativa (ubicación)



SnapCenter no admite SnapRestore basado en volumen.

Restaurar al minuto

En una operación de restauración actualizada (seleccionada de manera predeterminada), las bases de datos se recuperan hasta el punto de falla. SnapCenter logra esto realizando la siguiente secuencia:

1. Realiza una copia de seguridad del último registro de transacciones activas antes de restaurar la base de datos.
2. Restaura las bases de datos desde la copia de seguridad completa de la base de datos que seleccione.
3. Aplica todos los registros de transacciones que no se confirmaron en las bases de datos (incluidos los registros de transacciones de las copias de seguridad desde el momento en que se creó la copia de seguridad hasta el momento más actual).

Los registros de transacciones se mueven hacia adelante y se aplican a cualquier base de datos seleccionada.

Una operación de restauración actualizada requiere un conjunto contiguo de registros de transacciones.

Debido a que SnapCenter no puede restaurar registros de transacciones de bases de datos de SQL Server a partir de archivos de respaldo de envío de registros (el envío de registros le permite enviar automáticamente copias de respaldo de registros de transacciones desde una base de datos principal en una instancia de servidor principal a una o más bases de datos secundarias en instancias de servidor secundario independientes), no puede realizar una operación de restauración actualizada a partir de las copias de respaldo de registros de transacciones. Por este motivo, debe utilizar SnapCenter para realizar copias de seguridad de los archivos de registro de transacciones de la base de datos de SQL Server.

Si no necesita conservar la capacidad de restauración actualizada para todas las copias de seguridad, puede configurar la retención de la copia de seguridad del registro de transacciones de su sistema a través de las políticas de copia de seguridad.

Ejemplo de una operación de restauración actualizada

Supongamos que ejecuta la copia de seguridad de SQL Server todos los días al mediodía y el miércoles a las 4:00 p. m. necesita restaurar desde una copia de seguridad. Por alguna razón, la copia de seguridad del miércoles al mediodía no pasó la verificación, por lo que decide restaurar desde la copia de seguridad del martes al mediodía. Después de eso, si se restaura la copia de seguridad, todos los registros de transacciones se mueven hacia adelante y se aplican a las bases de datos restauradas, comenzando con aquellos que no se confirmaron cuando creó la copia de seguridad del martes y continuando con el último registro de transacciones escrito el miércoles a las 4:00 p. m. (si se realizó una copia de seguridad de los registros de transacciones).

Restaurar a un punto anterior en el tiempo

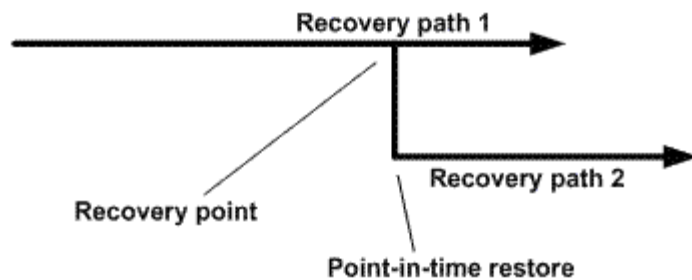
En una operación de restauración a un punto en el tiempo, las bases de datos se restauran únicamente a un momento específico del pasado. Una operación de restauración a un punto en el tiempo ocurre en las siguientes situaciones de restauración:

- La base de datos se restaura a un momento determinado en un registro de transacciones respaldado.
- Se restaura la base de datos y solo se le aplica un subconjunto de los registros de transacciones respaldados.



Restaurar una base de datos a un punto en el tiempo da como resultado una nueva ruta de recuperación.

La siguiente imagen ilustra los problemas que surgen cuando se realiza una operación de restauración en un punto en el tiempo:



En la imagen, la ruta de recuperación 1 consta de una copia de seguridad completa seguida de varias copias de seguridad del registro de transacciones. Restaura la base de datos a un punto en el tiempo. Se crean nuevas copias de seguridad del registro de transacciones después de la operación de restauración en un punto en el tiempo, lo que da como resultado la ruta de recuperación 2. Las nuevas copias de seguridad del registro de transacciones se crean sin crear una nueva copia de seguridad completa. Debido a la corrupción de datos u otros problemas, no es posible restaurar la base de datos actual hasta que se cree una nueva copia de seguridad completa. Además, no es posible aplicar los registros de transacciones creados en la ruta de recuperación 2 a la copia de seguridad completa perteneciente a la ruta de recuperación 1.

Si aplica copias de seguridad del registro de transacciones, también puede especificar una fecha y hora particulares en las que desea detener la aplicación de las transacciones respaldadas. Para hacer esto, especifique una fecha y hora dentro del rango disponible y SnapCenter elimina cualquier transacción que no se haya confirmado antes de ese momento. Puede utilizar este método para restaurar bases de datos a un punto en el tiempo anterior a que ocurriera una corrupción, o para recuperarse de una eliminación accidental de una base de datos o tabla.

Ejemplo de una operación de restauración en un punto en el tiempo

Supongamos que realiza copias de seguridad completas de la base de datos una vez a medianoche y una copia de seguridad del registro de transacciones cada hora. La base de datos falla a las 9:45 a. m., pero aún así se realizan copias de seguridad de los registros de transacciones de la base de datos fallida. Puede elegir entre estos escenarios de restauración en un momento determinado:

- Restaurar la copia de seguridad completa de la base de datos realizada a medianoche y aceptar la pérdida de los cambios en la base de datos realizados posteriormente. (Opción: Ninguna)
- Restaurar la copia de seguridad completa de la base de datos y aplicar todas las copias de seguridad del registro de transacciones hasta las 9:45 a. m. (Opción: Registrar hasta)
- Restaure la copia de seguridad completa de la base de datos y aplique las copias de seguridad del registro de transacciones, especificando la hora en que desea que se restauren las transacciones desde el último conjunto de copias de seguridad del registro de transacciones. (Opción: Por hora específica)

En este caso, es necesario calcular la fecha y hora en que se informó el error. Se eliminan todas las transacciones que no se hayan confirmado antes de la fecha y hora especificadas.

Definir una estrategia de clonación para SQL Server

Definir una estrategia de clonación le permitirá clonar su base de datos con éxito.

1. Revise las limitaciones relacionadas con las operaciones de clonación.

2. Decide el tipo de clon que necesitas.

Limitaciones de las operaciones de clonación

Debe tener en cuenta las limitaciones de las operaciones de clonación antes de clonar las bases de datos.

- Si está utilizando cualquier versión de Oracle desde 11.2.0.4 a 12.1.0.1, la operación de clonación quedará bloqueada cuando ejecute el comando *renamedg*. Puede aplicar el parche de Oracle 19544733 para solucionar este problema.
- No se admite la clonación de bases de datos desde un LUN que está conectado directamente a un host (por ejemplo, mediante el iniciador iSCSI de Microsoft en un host de Windows) a un VMDK o un LUN RDM en el mismo host de Windows u otro host de Windows, o viceversa.
- El directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- Si mueve un LUN que contiene un clon a un nuevo volumen, el clon no se podrá eliminar.

Tipos de operaciones de clonación

Puede utilizar SnapCenter para clonar una copia de seguridad de una base de datos de SQL Server o una base de datos de producción.

- Clonar desde una copia de seguridad de la base de datos

La base de datos clonada puede servir como base para desarrollar nuevas aplicaciones y ayudar a aislar errores de aplicaciones que ocurren en el entorno de producción. La base de datos clonada también se puede utilizar para recuperarse de errores de bases de datos suaves.

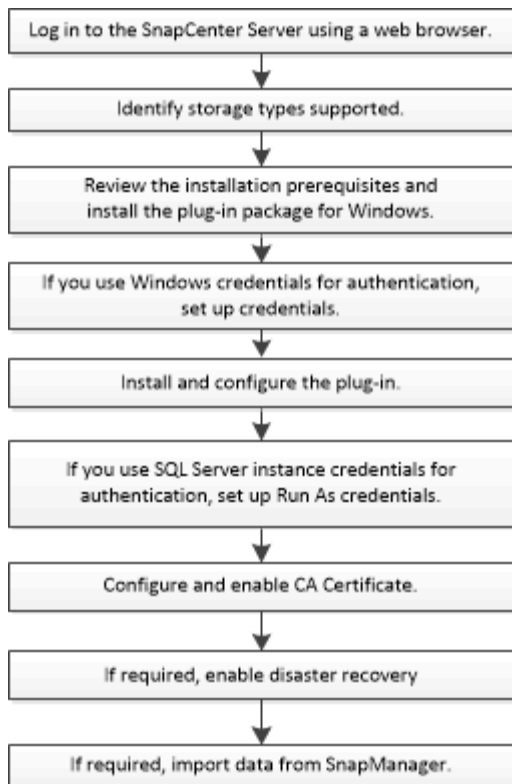
- Ciclo de vida del clon

Puede utilizar SnapCenter para programar trabajos de clonación recurrentes que se realizarán cuando la base de datos de producción no esté ocupada.

Prepárese para instalar el complemento de SnapCenter para Microsoft SQL Server

Flujo de trabajo de instalación del complemento SnapCenter para Microsoft SQL Server

Debe instalar y configurar el complemento SnapCenter para Microsoft SQL Server si desea proteger las bases de datos de SQL Server.



Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para Microsoft SQL Server

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos.

- Si está utilizando iSCSI, el servicio iSCSI debe estar ejecutándose.
- Debe tener un usuario con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Si administra nodos de clúster en SnapCenter, debe tener un usuario con privilegios administrativos para todos los nodos del clúster.
- Debe tener un usuario con permisos de administrador del sistema en SQL Server.

El complemento SnapCenter para Microsoft SQL Server utiliza Microsoft VDI Framework, que requiere acceso de administrador del sistema.

["Artículo de soporte técnico de Microsoft 2926557: Las operaciones de copia de seguridad y restauración de VDI de SQL Server requieren privilegios de administrador del sistema"](#)

- Al instalar un complemento 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 instalado SnapManager para Microsoft SQL Server, debe haber detenido o deshabilitado el servicio y las programaciones.

Si planea importar trabajos de copia de seguridad o clonación en SnapCenter, no desinstale SnapManager para Microsoft SQL Server.

- El host debe poder resolverse al nombre de dominio completo (FQDN) desde el servidor.

Si se modifica el archivo de hosts para que se pueda resolver y si tanto el nombre corto como el FQDN se especifican en el archivo de hosts, cree una entrada en el archivo de hosts de SnapCenter con el siguiente formato: <dirección_ip> <fqdn_de_host> <nombre_de_host>

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.

Artículo	Requisitos
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Configurar credenciales para el paquete de complementos de SnapCenter para Windows

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en bases de datos o sistemas de archivos de Windows.

Antes de empezar

- Debe configurar las credenciales de Windows antes de instalar complementos.
- Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.
- Autenticación SQL en hosts de Windows

Debe configurar las credenciales de SQL después de instalar los complementos.

Si está implementando el complemento de SnapCenter para Microsoft SQL Server, debe configurar las credenciales de SQL después de instalar los complementos. Configurar una credencial para un usuario con permisos de administrador de sistemas de SQL Server.

El método de autenticación SQL se autentica contra una instancia de SQL Server. Esto significa que se debe descubrir una instancia de SQL Server en SnapCenter. Por lo tanto, antes de agregar una credencial SQL, debe agregar un host, instalar paquetes de complementos y actualizar los recursos. Necesita la autenticación de SQL Server para realizar operaciones como programar o descubrir recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, especifique la información necesaria para configurar las credenciales:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para la credencial.
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • Administrador de dominio Especifique el administrador del dominio en el sistema donde va a instalar el complemento 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: UserName No utilice comillas dobles (") ni tildes invertidas (') en las contraseñas. No debe utilizar los símbolos menor que (<) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que<!10, menos que10<!, acento grave`12.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar. Si selecciona el modo de autenticación SQL, también debe especificar la instancia del servidor SQL y el host donde se encuentra la instancia SQL.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Configurar credenciales para un recurso individual de SQL Server

Puede configurar credenciales para realizar trabajos de protección de datos en recursos individuales de SQL Server para cada usuario. Si bien puede configurar las credenciales de forma global, es posible que desee hacerlo solo para un recurso en particular.

Acerca de esta tarea

- Si utiliza credenciales de Windows para la autenticación, debe configurar sus credenciales antes de instalar complementos.

Sin embargo, si está utilizando una instancia de SQL Server para la autenticación, debe agregar la credencial después de instalar los complementos.
- Si ha habilitado la autenticación SQL al configurar las credenciales, la instancia o base de datos detectada se muestra con un ícono de candado de color rojo.

Si aparece el ícono del candado, debe especificar las credenciales de la instancia o base de datos para agregar correctamente la instancia o base de datos a un grupo de recursos.
- Debe asignar la credencial a un usuario de control de acceso basado en roles (RBAC) sin acceso de administrador de sistemas cuando se cumplan las siguientes condiciones:
 - La credencial se asigna a una instancia de SQL.
 - La instancia o host de SQL se asigna a un usuario RBAC.

El usuario debe tener privilegios tanto de grupo de recursos como de respaldo.

Paso 1: Agregar y configurar credenciales

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

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario	Introduzca el nombre de usuario utilizado para la autenticación de SQL Server. - Administrador de dominio o cualquier miembro del grupo de administradores. Especifique el administrador de dominio o cualquier miembro del grupo de administradores en el sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: <i>NetBIOS\Nombre de usuario</i> <i>Dominio FQDN\Nombre de usuario</i> - Administrador local (solo para grupos de trabajo). Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>Nombre de usuario</i>
Password	Introduzca la contraseña utilizada para la autenticación.
Modo de autenticación	Seleccione el modo de autenticación de SQL Server. También puede elegir la autenticación de Windows si el usuario de Windows tiene privilegios de administrador de sistemas en el servidor SQL.
Host	Seleccione el host.
Instancia de SQL Server	Seleccione la instancia de SQL Server.

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

Paso 2: Configurar instancias

- En el panel de navegación izquierdo, seleccione **Recursos**.
- En la página Recursos, seleccione **Instancia** de la lista **Ver**.
 - Seleccione `image:.../media/filter_icon.png`[icono de filtro] y luego seleccione el nombre del host para filtrar las instancias.
 - Seleccione `image:.../media/filter_icon.png`[icono de filtro] para cerrar el panel de filtro.
- En la página Proteger instancia, proteja la instancia y, si es necesario, seleccione **Configurar credenciales**.

Si el usuario que ha iniciado sesión en SnapCenter Server no tiene acceso al complemento SnapCenter para Microsoft SQL Server, entonces el usuario debe configurar las credenciales.



La opción de credenciales no se aplica a bases de datos y 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 administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Añade objetos de computadora 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,...>  
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de  
servicio.
```

4. Configure el gMSA en sus hosts:

- a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
- b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
- c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Instalar el complemento de SnapCenter para Microsoft SQL Server

Agregue hosts e instale el paquete de complementos de SnapCenter para Windows

Debe utilizar la página **Agregar host** de SnapCenter para agregar hosts e instalar el paquete de complementos. Los complementos se instalan automáticamente en los hosts remotos.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
 - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento en un host de Windows, si especifica una credencial que no está incorporada, debe deshabilitar UAC en el host.

- Debe asegurarse de que el servicio de cola de mensajes esté en estado de ejecución.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar la cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para SQL"](#)

Acerca de esta tarea

No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .

Puede agregar un host e instalar los paquetes de complementos para un host individual o para un clúster. Si está instalando los complementos en un clúster o en un clúster de conmutación por error de Windows Server (WSFC), los complementos se instalan en todos los nodos del clúster.

Para obtener información sobre la administración de hosts, consulte ["Administrar hosts"](#) .

Pasos

1. En el panel de navegación izquierdo, seleccione **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página Hosts haga lo siguiente:

Para este campo...	Haz esto...
Tipo de host	Seleccione Windows como tipo de host. El servidor SnapCenter agrega el host y luego instala el complemento para Windows si el complemento aún no está instalado en el host. Si selecciona la opción Microsoft SQL Server en la página Complementos, SnapCenter Server instala el complemento para SQL Server.
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. La dirección IP solo es compatible con hosts de dominios no confiables si se resuelve en el FQDN. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • WSFC Si está agregando un host mediante SnapCenter y el host es parte de un subdominio, debe proporcionar el FQDN.

Para este campo...	Haz esto...
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea instalar.

6. Seleccione **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.
Ruta de instalación	La ruta predeterminada es C:\Archivos de programa\ NetApp\ SnapCenter. Opcionalmente puedes personalizar la ruta.
Agregar todos los hosts en el clúster	Seleccione esta casilla de verificación para agregar todos los nodos del clúster en un WSFC o un grupo de disponibilidad de SQL. Debe agregar todos los nodos del clúster seleccionando la casilla de verificación del clúster correspondiente en la GUI si desea administrar e identificar varios grupos de disponibilidad de SQL disponibles dentro de un clúster.

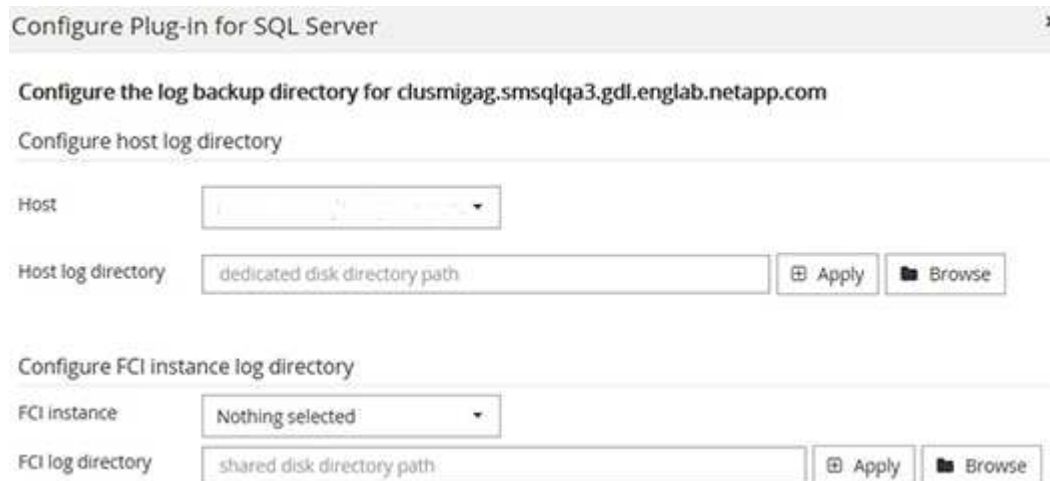
Para este campo...	Haz esto...
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento. Proporcione el nombre gMSA en el siguiente formato: domainName\accountName\$.  Si el host se agrega con gMSA y si el gMSA tiene privilegios de inicio de sesión y de administrador del sistema, se utilizará el gMSA para conectarse a la instancia de SQL.

7. Seleccione **Enviar**.

8. Para el complemento SQL, seleccione el host para configurar el directorio de registro.

- a. Seleccione **Configurar directorio de registro** y en la página Configurar directorio de registro del host, seleccione **Explorar** y complete los siguientes pasos:

Solo se enumeran las LUN (unidades) de NetApp para su selección. SnapCenter realiza una copia de seguridad y replica el directorio de registro del host como parte de la operación de copia de seguridad.



- i. Seleccione la letra de unidad o el punto de montaje en el host donde se almacenará el registro del host.
- ii. Elija un subdirectorio, si es necesario.
- iii. Seleccione **Guardar**.

9. Seleccione **Enviar**.

Si no ha seleccionado la casilla **Omitir comprobaciones previas**, se valida el host para verificar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell, la versión de .NET, la ubicación (para complementos de Windows) y la versión de Java (para complementos de Linux) se validan según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

10. Supervisar el progreso de la instalación.

Instalar el complemento de SnapCenter para Microsoft SQL Server en varios hosts remotos mediante cmdlets

Puede instalar el complemento de SnapCenter para Microsoft SQL Server en varios hosts simultáneamente mediante el cmdlet de PowerShell Install-SmHostPackage.

Antes de empezar

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar el paquete de complemento.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter, establezca una sesión mediante el cmdlet Open-SmConnection y luego ingrese sus credenciales.
3. Instale el complemento de SnapCenter para Microsoft SQL Server en varios hosts remotos mediante el cmdlet Install-SmHostPackage y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Puede utilizar la opción -skipprecheck cuando ya haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.

4. Introduzca sus credenciales para la instalación remota.

Instale el complemento de SnapCenter para Microsoft SQL Server de forma silenciosa desde la línea de comandos

Debe instalar el complemento de SnapCenter para Microsoft SQL Server desde la interfaz de usuario de SnapCenter. Sin embargo, si por algún motivo no puede, puede ejecutar el programa de instalación del complemento para SQL Server sin supervisión en modo silencioso desde la línea de comandos de Windows.

Antes de empezar

- Debe eliminar la versión anterior del complemento SnapCenter para Microsoft SQL Server antes de instalarlo.

Para obtener más información, consulte ["Cómo instalar un complemento de SnapCenter de forma manual y directa desde el host del complemento"](#) .

Pasos

1. Valide si la carpeta C:\temp existe en el host del complemento y si el usuario que inició sesión tiene acceso completo a ella.
2. Descargue el complemento para el software SQL Server desde C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

Se puede acceder a esta ruta desde el host donde está instalado el servidor SnapCenter .

3. Copie el archivo de instalación en el host en el que desea instalar el complemento.
4. Desde un símbolo del sistema de Windows en el host local, navegue hasta el directorio donde guardó los archivos de instalación del complemento.
5. Instalar el complemento para el software 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
```

Reemplace los valores de marcador de posición con 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 complemento (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 del complemento del host.
- domain\administrator es la cuenta de servicio web del complemento SnapCenter para Microsoft Windows.
- contraseña es la contraseña para la cuenta de servicio web del complemento 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 pasados durante la instalación del complemento 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 verificar que los instaladores msix.exe estén instalando el software sin errores.



La instalación del complemento para SQL Server registra el complemento en el host y no en el servidor SnapCenter . Puede registrar el complemento en el servidor SnapCenter agregando el host mediante la GUI de SnapCenter o el cmdlet de PowerShell. Una vez agregado el host, el complemento se descubre automáticamente.

Supervisar el estado de la instalación del complemento para SQL Server

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:

- a. Haga doble clic en el certificado.
- b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
- c. Desplácese por la lista de campos y haga clic en **Huella digital**.
- d. Copia los caracteres hexadecimales del cuadro.
- e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:

- a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado recientemente instalado por el nombre del sujeto.

```
Get-ChildItem -Path Certificado:\LocalMachine\Mi
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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"
```

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Configurar la recuperación ante desastres

Recuperación ante desastres del complemento SnapCenter para SQL Server

Cuando el complemento de SnapCenter para SQL Server no funciona, siga los pasos siguientes para cambiar a un host 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 principal.
- Inserte el complemento SnapCenter para SQL Server en un host alternativo mediante la página **Agregar host** o **Modificar host**. Ver ["Administrar hosts"](#) Para más información.

Pasos

1. Seleccione el host de la página **Hosts** para modificar e instalar el complemento de SnapCenter para SQL Server.
2. (Opcional) Reemplace los archivos de configuración del complemento de SnapCenter para SQL Server de la copia de seguridad de recuperación ante desastres (DR) en la nueva máquina.
3. Importe programaciones de Windows y SQL desde la carpeta del complemento SnapCenter para SQL Server desde la copia de seguridad de recuperación ante desastres.

Información relacionada

Ver el ["API de recuperación ante desastres"](#) video.

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

Puede recuperar el complemento de SnapCenter para el almacenamiento de SQL Server habilitando el modo DR para almacenamiento en la página Configuración global.

Antes de empezar

- Asegúrese de que los complementos estén en modo de mantenimiento.
- Romper la relación SnapMirror/ SnapVault . ["Romper las relaciones de SnapMirror"](#)
- Conecte el LUN desde la unidad secundaria a la máquina 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 del servidor MSSQL.
- Asegúrese de que los recursos de SQL vuelvan a estar en línea.

Acerca de esta tarea

La recuperación ante desastres (DR) no es compatible con configuraciones VMDK y RDM.

Pasos

1. En la página de Configuración, navegue a **Configuración > Configuración global > Recuperación ante desastres**.
2. Seleccione **Habilitar recuperación ante desastres**.
3. Haga clic en **Aplicar**.

4. Verifique si el trabajo de DR está habilitado o no haciendo clic en **Monitor > Trabajos**.

Después de terminar

- Si se crean nuevas bases de datos después de la conmutación por error, las bases de datos estarán en modo no DR.

Las nuevas bases de datos continuarán funcionando como lo hacían antes de la conmutación por error.

- Las nuevas copias de seguridad que se crearon en modo DR aparecerán en SnapMirror o SnapVault (secundario) en la página Topología.

Se muestra un ícono "i" junto a las nuevas copias de seguridad para indicar que estas copias de seguridad se crearon durante el modo DR.

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

Para obtener más información, consulte la ["Guía de referencia de cmdlets del software SnapCenter"](#).

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

Conmutación por recuperación desde el complemento SnapCenter para el almacenamiento secundario de SQL Server al almacenamiento principal

Una vez que el complemento SnapCenter para el almacenamiento principal de SQL Server vuelva a estar en línea, deberá realizar una conmutación por recuperación al almacenamiento principal.

Antes de empezar

- Coloque el complemento de SnapCenter para SQL Server en modo **Mantenimiento** desde la página Hosts administrados.
- Desconecte el almacenamiento secundario del host y conéctese desde el almacenamiento primario.
- Para volver al almacenamiento principal, asegúrese de que la dirección de la relación siga 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 la operación de resincronización inversa una vez más.

Para más información véase ["Relaciones de espejo de resincronización inversa"](#)

- Reinicie el servicio del servidor MSSQL.
- Asegúrese de que los recursos de SQL vuelvan a estar en línea.



Durante la conmutación por error o la recuperación del complemento, el estado general del complemento no se actualiza inmediatamente. El estado general del host y del complemento se actualiza durante la siguiente operación de actualización del host.

Pasos

1. En la página de Configuración, navegue a **Configuración > Configuración global > Recuperación ante desastres**.
2. Desmarque **Habilitar recuperación ante desastres**.
3. Haga clic en **Aplicar**.
4. Verifique si el trabajo de DR está habilitado o no haciendo clic en **Monitor > Trabajos**.

Después de terminar

Puede eliminar las copias de seguridad del complemento SnapCenter para SQL Server que se crearon durante la conmutación por error mediante la interfaz de usuario o el siguiente cmdlet: `Remove-SmDRFailoverBackups`

Instalar el SnapCenter Plug-in for VMware vSphere

Si su base de datos o sistema de archivos está almacenado en máquinas virtuales (VM), o si desea proteger las VM y los almacenes de datos, debe implementar el SnapCenter Plug-in for VMware vSphere .

Para obtener información sobre la implementación, consulte ["Descripción general de la implementación"](#) .

Implementar certificado de CA

Para configurar el certificado CA con el SnapCenter Plug-in for VMware vSphere, consulte ["Crear o importar certificado SSL"](#) .

Configurar el archivo CRL

El SnapCenter Plug-in for VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL para el SnapCenter Plug-in for VMware vSphere es `/opt/netapp/config/crl`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Prepárese para la protección de datos

Requisitos previos para utilizar el complemento de SnapCenter para Microsoft SQL Server

Antes de comenzar a utilizar el complemento para SQL Server, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter.
- Configure el entorno de SnapCenter agregando o asignando conexiones del sistema de almacenamiento y creando credenciales.



SnapCenter no admite varias SVM con el mismo nombre en diferentes clústeres. Cada SVM compatible con SnapCenter debe tener un nombre único.

- Agregue hosts, instale los complementos, descubra (actualice) los recursos y configure los complementos.
- Mueva una base de datos existente de Microsoft SQL Server desde un disco local a un LUN de NetApp o viceversa ejecutando Invoke-SmConfigureResources.

Para obtener información sobre cómo ejecutar el cmdlet, consulte la ["Guía de referencia de cmdlets del software SnapCenter"](#)

- Si utiliza SnapCenter Server para proteger bases de datos SQL que residen en LUN o VMDK de VMware RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter. La documentación del SnapCenter Plug-in for VMware vSphere tiene más información.

["Documentación del SnapCenter Plug-in for VMware vSphere"](#)

- Realice el aprovisionamiento de almacenamiento del lado del host mediante el complemento SnapCenter para Microsoft Windows.
- Configure las relaciones de SnapMirror y SnapVault, si desea una replicación del backup.

Para obtener más detalles, consulte la información de instalación de SnapCenter .

Para los usuarios de SnapCenter 4.1.1, la documentación del SnapCenter Plug-in for VMware vSphere 4.1.1 tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, NetApp Data Broker 1.0 y 1.0.1, la documentación tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados mediante el SnapCenter Plug-in for VMware vSphere que proporciona el dispositivo virtual NetApp Data Broker basado en Linux (formato Open Virtual Appliance). Para los usuarios de SnapCenter 4.3.x, la documentación del SnapCenter Plug-in for VMware vSphere 4.3 tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual basado en Linux del SnapCenter Plug-in for VMware vSphere (formato Open Virtual Appliance).

["Documentación del SnapCenter Plug-in for VMware vSphere"](#)

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger SQL Server

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de copia de seguridad, clonación y restauración que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser bases de datos, instancias de bases de datos o grupos de disponibilidad de Microsoft SQL Server que usted respalda o clona con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host o clúster.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

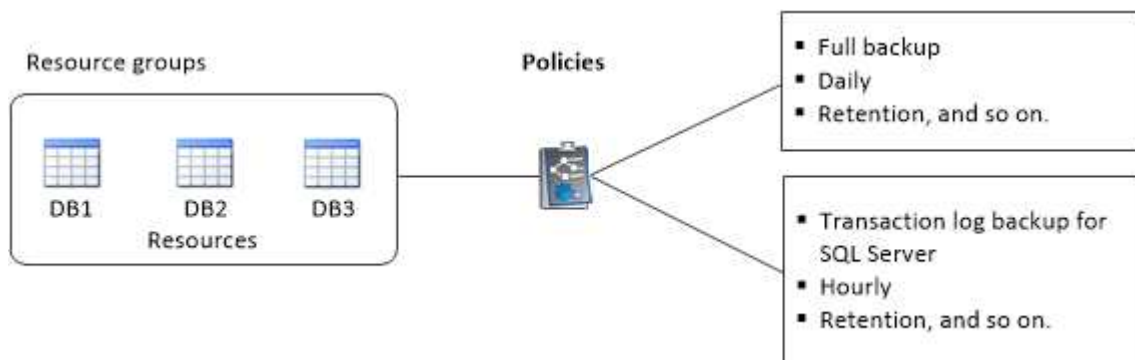
- Las políticas especifican la frecuencia de las copias de seguridad, la retención de copias, la replicación,

los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede seleccionar una política cuando realiza una copia de seguridad a pedido para un solo recurso.

Piense en un grupo de recursos como si definiera *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera *cómo* desea protegerla. Si está realizando una copia de seguridad de todas las bases de datos o de todos los sistemas de archivos de un host, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Al crear el grupo de recursos y adjuntar las políticas, puede configurar el grupo de recursos para realizar una copia de seguridad completa diariamente y otra programación que realice copias de seguridad de registros cada hora.

La siguiente imagen ilustra la relación entre recursos, grupos de recursos y políticas para bases de datos:



Realizar una copia de seguridad de la base de datos, instancia o grupo de disponibilidad de SQL Server

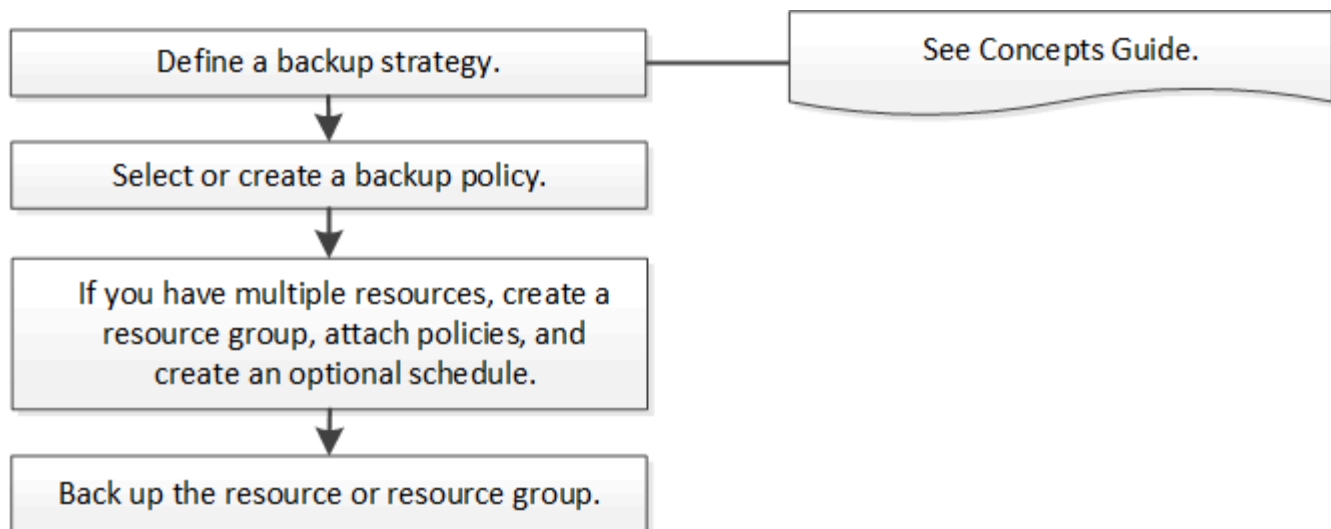
Flujo de trabajo de respaldo

Cuando instala el complemento de SnapCenter para Microsoft SQL Server en su entorno, puede usar SnapCenter para realizar copias de seguridad de los recursos de SQL Server.

Puede programar varias copias de seguridad para que se ejecuten en todos los servidores simultáneamente.

Las operaciones de copia de seguridad y restauración no se pueden realizar simultáneamente en el mismo recurso.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar las operaciones de copia de seguridad:



Las opciones Realizar copia de seguridad ahora, Restaurar, Administrar copias de seguridad y Clonar en la página Recursos se deshabilitan si selecciona un LUN que no sea de NetApp, una base de datos que esté dañada o una base de datos que se esté restaurando.

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 ["Guía de referencia de cmdlets del software SnapCenter"](#)

Cómo SnapCenter realiza copias de seguridad de las bases de datos

SnapCenter utiliza la tecnología Snapshot para realizar copias de seguridad de las bases de datos de SQL Server que residen en LUN o VMDK. SnapCenter crea la copia de seguridad creando instantáneas de las bases de datos.

Cuando selecciona una base de datos para una copia de seguridad completa desde la página Recursos, SnapCenter selecciona automáticamente todas las demás bases de datos que residen en el mismo volumen de almacenamiento. Si el LUN o VMDK almacena solo una única base de datos, puede borrar o volver a seleccionar la base de datos individualmente. Si el LUN o VMDK alberga varias bases de datos, debe borrar o volver a seleccionar las bases de datos como un grupo.

Todas las bases de datos que residen en un solo volumen se respaldan simultáneamente mediante instantáneas. Si la cantidad máxima de bases de datos de respaldo simultáneas es 35, y si más de 35 bases de datos residen en un volumen de almacenamiento, entonces la cantidad total de instantáneas que se crean es igual a la cantidad de bases de datos dividida por 35.



Puede configurar la cantidad máxima de bases de datos para cada instantánea en la política de respaldo.

Cuando SnapCenter crea una instantánea, todo el volumen del sistema de almacenamiento se captura en la instantánea. Sin embargo, la copia de seguridad sólo es válida para el servidor host SQL para el que se creó la copia de seguridad.

Si los datos de otros servidores host SQL residen en el mismo volumen, estos datos no se pueden restaurar desde la instantánea.

Encuentre más información

Determinar si hay recursos disponibles para realizar copias de seguridad

Los recursos son las bases de datos, las instancias de aplicación, los grupos de disponibilidad y componentes similares que mantienen los complementos que ha instalado. Puede agregar esos recursos a grupos de recursos para poder realizar trabajos de protección de datos, pero primero debe identificar qué recursos tiene disponibles. La determinación de los recursos disponibles también verifica que la instalación del complemento se haya completado correctamente.

Antes de empezar

- Debe haber completado ya tareas como instalar SnapCenter Server, agregar hosts, crear conexiones del sistema de almacenamiento y agregar credenciales.
- Para descubrir las bases de datos de Microsoft SQL, se debe cumplir una de las siguientes condiciones.
 - El usuario que se utilizó para agregar el host del complemento a SnapCenter Server debe tener los permisos necesarios (sysadmin) en Microsoft SQL Server.
 - Si no se cumple la condición anterior, en SnapCenter Server debe configurar el usuario que tenga los permisos necesarios (sysadmin) en Microsoft SQL Server. El usuario debe configurarse en el nivel de instancia de Microsoft SQL Server y puede ser un usuario de SQL o de Windows.
- Para descubrir 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 RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter.

Para obtener más información, consulte ["Implementar el SnapCenter Plug-in for VMware vSphere"](#)

- Si el host se agrega con gMSA y si el gMSA tiene privilegios de inicio de sesión y de administrador del sistema, se utilizará el gMSA para conectarse a la instancia de SQL.

Acerca de esta tarea

No se pueden realizar copias de seguridad de bases de datos cuando la opción **Estado general** en la página Detalles está configurada en No disponible para copia de seguridad. La opción **Estado general** se establece como No disponible para copia de seguridad cuando se cumple alguna de las siguientes condiciones:

- Las bases de datos no están 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 fuera de línea, en restauración, con recuperación pendiente, sospechosas, etc.

- Las bases de datos no tienen privilegios suficientes.

Por ejemplo, si un usuario sólo tiene acceso de visualización a la base de datos, no se podrán identificar los archivos ni las propiedades de la base de datos y, por lo tanto, no se podrán realizar copias de seguridad.



SnapCenter solo puede realizar copias de seguridad de la base de datos principal si tiene una configuración de grupo de disponibilidad en SQL Server Standard Edition.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos**, o **Instancia**, o **Grupo de disponibilidad**, de la lista desplegable **Ver**.

Hacer clic  y seleccione el nombre del host y la instancia de SQL Server para filtrar los recursos. Luego puedes hacer clic  para cerrar el panel de filtro.

3. Haga clic en **Actualizar recursos**.

Los recursos recientemente agregados, renombrados o eliminados se actualizan en el inventario de SnapCenter Server.



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

Los recursos se muestran junto con información como el tipo de recurso, el nombre del host o clúster, los grupos de recursos asociados, el tipo de copia de seguridad, las políticas y el estado general.

- Si la base de datos está en un almacenamiento que no es NetApp , `Not available for backup` se muestra en la columna **Estado general**.

No se pueden realizar operaciones de protección de datos en una base de datos que se encuentre en un almacenamiento que no sea NetApp .

- Si la base de datos está en un almacenamiento NetApp y no está protegida, `Not protected` se muestra en la columna **Estado general**.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, la interfaz de usuario muestra `Backup not run` mensaje en la columna **Estado general**.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida y si se activa la copia de seguridad para la base de datos, la interfaz de usuario muestra `Backup succeeded` mensaje en la columna **Estado general**.



Si habilitó una autenticación SQL al configurar las credenciales, la instancia o base de datos detectada se muestra con un ícono de candado rojo. Si aparece el ícono del candado, debe especificar las credenciales de la instancia o base de datos para agregar correctamente la instancia o base de datos a un grupo de recursos.

1. Después de que el administrador de SnapCenter asigna los recursos a un usuario RBAC, el usuario RBAC debe iniciar sesión y hacer clic en **Actualizar recursos** para ver el **Estado general** más reciente de los recursos.

Migrar recursos al sistema de almacenamiento NetApp

Una vez que haya provisionado su sistema de almacenamiento NetApp mediante el complemento SnapCenter para Microsoft Windows, puede migrar sus recursos al sistema de almacenamiento NetApp o de un LUN NetApp a otro LUN NetApp mediante la interfaz gráfica de usuario (GUI) de SnapCenter o mediante los cmdlets de PowerShell.

Antes de empezar

- Debe haber agregado sistemas de almacenamiento a SnapCenter Server.
- Debes haber actualizado (descubierto) los recursos de SQL Server.

La mayoría de los campos de estas páginas del asistente se explican por sí solos. La siguiente información describe algunos de los campos para los que podría necesitar orientación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** o **Instancia** de la lista desplegable **Ver**.
3. Seleccione la base de datos o la instancia de la lista y haga clic en **Migrar**.
4. En la página Recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre de la base de datos (opcional)	Si ha seleccionado una instancia para migrar, debe seleccionar las bases de datos de esa instancia en la lista desplegable Bases de datos .
Elegir destinos	Seleccione la ubicación de destino para los archivos de datos y registro. Los archivos de datos y de registro se mueven a las carpetas Datos y Registro respectivamente en la unidad NetApp seleccionada. Si alguna carpeta en la estructura de carpetas no está presente, se crea una carpeta y se migra el recurso.
Mostrar detalles del archivo de base de datos (opcional)	Seleccione esta opción cuando desee migrar varios archivos de una sola base de datos.  Esta opción no se muestra cuando selecciona el recurso Instancia.
Opciones	Seleccione Eliminar copia de la base de datos migrada en la ubicación original para eliminar la copia de la base de datos de la fuente. Opcional: EJECUTAR ACTUALIZAR ESTADÍSTICAS en las tablas antes de separar la base de datos.

5. En la página Verificar, realice las siguientes acciones:

Para este campo...	Haz esto...
Opciones de comprobación de consistencia de la base de datos	Seleccione Ejecutar antes para comprobar la integridad de la base de datos antes de la migración. Seleccione Ejecutar después para comprobar la integridad de la base de datos después de la migración.
Opciones DBCC CHECKDB	• Seleccione la opción PHYSICAL_ONLY para limitar la verificación de integridad a la estructura física de la base de datos y para detectar páginas rotas, fallas de suma de comprobación y fallas de hardware comunes que afectan la base de datos. • Seleccione la opción NO_INFOMSGS para suprimir todos los mensajes informativos. • Seleccione la opción ALL_ERRORMSGs para mostrar todos los errores informados por objeto. • Seleccione la opción NOINDEX si no desea comprobar índices no agrupados. La base de datos de SQL Server utiliza el Comprobador de consistencia de base de datos de Microsoft SQL Server (DBCC) para comprobar la integridad lógica y física de los objetos de la base de datos.  Es posible que desees 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 de base de datos interna.

6. Revise el resumen y luego haga clic en **Finalizar**.

Crear políticas de respaldo para bases de datos de SQL Server

Puede crear una política de respaldo para el recurso o el grupo de recursos antes de usar SnapCenter para realizar un respaldo de los recursos de SQL Server, o puede crear una política de respaldo en el momento en que crea un grupo de recursos o realiza un respaldo de un solo recurso.

Antes de empezar

- Debes haber definido tu estrategia de protección de datos.
- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, identificar recursos y crear conexiones del sistema de almacenamiento.

- Debe haber configurado el directorio de registro del host para realizar copias de seguridad del registro.
- Debes haber actualizado (descubierto) los recursos de SQL Server.
- Si está replicando instantáneas a un espejo o bóveda, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) tanto para los volúmenes de origen como para los volúmenes 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 prescripts y postscripts, debe establecer el valor del parámetro usePowershellProcessforScripts en verdadero en el archivo web.config.

El valor predeterminado es falso.

- Revise los requisitos previos y las limitaciones específicos de la sincronización activa de SnapMirror . Para obtener información, consulte ["Límites de objetos para la sincronización activa de SnapMirror"](#) .

Acerca de esta tarea

- Una política de respaldo es un conjunto de reglas que rigen cómo administrar y conservar los respaldos, y con qué frecuencia se realizan respaldos del recurso o grupo de recursos. Además, puede especificar la configuración de replicación y script. Especificar opciones en una política ahorra tiempo cuando desea reutilizar la política para otro grupo de recursos.

SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCOREServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.

Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas que la cantidad especificada 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 .

Paso 1: Crear un nombre de política

1. En el panel de navegación izquierdo, seleccione **Configuración**.
2. En la página de Configuración, seleccione **Políticas**.

3. Seleccione **Nuevo**.
4. En la página **Nombre**, ingrese el nombre y los detalles de la política.

Paso 2: Configurar las opciones de política

1. En la página Tipo de política, realice los siguientes pasos:
 - a. Seleccione su tipo de almacenamiento.
 - b. Seleccione el alcance de su política.

Copia de seguridad completa y copia de seguridad de registros

Realice una copia de seguridad de los archivos de base de datos y de los registros de transacciones y trunque 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 deben respaldarse para cada instantánea.



Debe aumentar este valor si desea ejecutar varias operaciones de copia de seguridad simultáneamente.

Copia de seguridad completa

Realice una copia de seguridad de los archivos de la base de datos.

- i. Seleccione **Copia de seguridad completa**.
- ii. Introduzca el número máximo de bases de datos que deben respaldarse para cada instantánea. El valor predeterminado es 100



Debe aumentar este valor si desea ejecutar varias operaciones de copia de seguridad simultáneamente.

Copia de seguridad del registro

- i. Realice una copia de seguridad de los registros de transacciones.
- ii. Seleccione **Copia de seguridad del registro**.

Copia de seguridad de solo copia

- i. Si está realizando una copia de seguridad de sus recursos mediante otra aplicación de copia de seguridad, seleccione **Copiar solo copia de seguridad**.

Mantener los registros de transacciones intactos permite que cualquier aplicación de respaldo restaure las bases de datos. Por lo general, no debería utilizar la opción de solo copiar en ninguna otra circunstancia.



Microsoft SQL no admite la opción **Copiar solo copia de seguridad** junto con la opción **Copia de seguridad completa y copia de seguridad del registro** para el almacenamiento secundario.

Paso 3: Configurar los ajustes del grupo de disponibilidad

1. En la sección Configuración del grupo de disponibilidad, realice las siguientes acciones:

- a. Realizar copia de seguridad únicamente en la réplica de copia de seguridad preferida.

Seleccione esta opción para realizar copias de seguridad solo en la réplica de copia de seguridad preferida. La réplica de respaldo preferida se decide según las preferencias de respaldo configuradas para el AG en SQL Server.

- b. Seleccionar réplicas para realizar copias de seguridad.

Elija la réplica AG principal o la réplica AG secundaria para la copia de seguridad.

- c. Seleccionar prioridad de copia de seguridad (prioridad de copia de seguridad mínima y máxima)

Especifique un número de prioridad de respaldo mínimo y un número de prioridad de respaldo máximo que deciden la réplica de AG para la copia de seguridad. Por ejemplo, puede tener una prioridad mínima de 10 y una prioridad máxima de 50. En este caso, se consideran para la copia de seguridad todas las réplicas de AG con una prioridad mayor a 10 y menor a 50.

De forma predeterminada, la prioridad mínima es 1 y la prioridad máxima es 100.



En las configuraciones de clúster, las copias de seguridad se conservan en cada nodo del clúster según la configuración de retención establecida en la política. Si el nodo propietario del AG cambia, las copias de seguridad se realizan de acuerdo con la configuración de retención y se conservarán las copias de seguridad del nodo propietario anterior. La retención de AG se aplica únicamente a nivel de nodo.

Paso 4: Configurar los ajustes de instantánea y replicación

1. En la página Instantánea y replicación, realice los siguientes pasos:

- a. Especifique el tipo de programación seleccionando **A pedido**, **Por hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.

Solo puede seleccionar un tipo de programación para una política.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

Paso 5: Configure los ajustes de retención actualizados

1. En la sección Configuración de retención actualizada, según el tipo de copia de seguridad seleccionado en la página de tipo de copia de seguridad, realice una o más de las siguientes acciones:

Número específico de copias

Conservar sólo un número específico de instantáneas.

1. Seleccione la opción **Conservar copias de seguridad de registros aplicables a los últimos <número> días** y especifique la cantidad de días que se conservarán. Si está cerca de este límite, es posible que desee eliminar las copias más antiguas.

Número específico de días

Conservar las copias de seguridad durante un número específico de días.

1. Seleccione la opción **Mantener copias de seguridad de registros aplicables a los últimos <número> días de copias de seguridad completas** y especifique la cantidad de días que desea conservar las copias de seguridad de registros.

Paso 6: Configurar los ajustes de la instantánea

1. Para configurar la retención de copia de seguridad completa, realice las siguientes acciones:

- a. Especifique el número total de instantáneas a conservar
 - i. Para especificar la cantidad de instantáneas que desea conservar, seleccione **Copias para conservar**.
 - ii. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.



De forma predeterminada, el valor del recuento de retención se establece en 2. Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva 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 subyacente de NetApp ONTAP .

2. Tiempo de conservación de las instantáneas
 - a. Si desea especificar la cantidad de días durante los cuales desea conservar las instantáneas antes de eliminarlas, seleccione **Conservar copias durante**.
3. Seleccione **Período de bloqueo de copia de instantánea** y especifique la duración en días, meses o años.

El período de retención del 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: Configurar las opciones de replicación secundaria

1. En la sección Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Actualizar SnapMirror

Actualice SnapMirror después de crear una copia de instantánea local.

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

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

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

Ver ["Ver copias de seguridad y clones de SQL Server en la página Topología"](#) .

Actualizar SnapVault

Actualice SnapVault después de crear una copia de instantánea.

1. Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco.

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

Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón **Actualizar** en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP.

Para obtener más información sobre SnapLock Vault, consulte ["Confirmar copias de instantáneas en WORM en un destino de bóveda"](#)

Ver ["Ver copias de seguridad y clones de SQL Server en la página Topología"](#) .

Recuento de reintentos de errores

1. Introduzca el número de intentos de replicación que deben ocurrir antes de que el proceso se detenga.

Paso 8: Configurar los ajustes del script

1. En la página Script, ingrese la ruta y los argumentos del prescript o postscript que se debe ejecutar antes o después de la operación de respaldo, respectivamente.

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



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.



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

Paso 9: Configurar los ajustes de verificación

En la página de Verificación, realice los siguientes pasos:

1. En la sección Ejecutar verificación para las siguientes programaciones de copias de seguridad, seleccione la frecuencia de la programación.
2. En la sección Opciones de verificación de consistencia de la base de datos, 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 verificación de integridad a la estructura física de la base de datos y detectar páginas rotas, fallas de suma de comprobación y fallas de hardware comunes que afectan la base de datos.
 - b. Suprimir todos los mensajes de información (NO_INFOMSGS)
 - i. Seleccione **Suprimir todos los mensajes de información (NO_INFOMSGS)** para suprimir todos los mensajes informativos. Seleccionado por defecto.
 - c. Mostrar todos los mensajes de error informados por objeto (ALL_ERRORMSGs)
 - i. Seleccione **Mostrar todos los mensajes de error informados por objeto (ALL_ERRORMSGs)** para mostrar todos los errores informados por objeto.
 - d. No comprobar índices no agrupados (NOINDEX)
 - i. Seleccione **No comprobar índices no agrupados (NOINDEX)** si no desea comprobar índices no agrupados. La base de datos de SQL Server utiliza el Comprobador de consistencia de base de datos de Microsoft SQL Server (DBCC) para comprobar la integridad lógica y física de los objetos de la base de datos.
 - e. Limite las comprobaciones y obtenga los bloqueos en lugar de utilizar una instantánea de base de datos interna (TABLOCK)
 - i. Seleccione **Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una copia de instantánea de base de datos interna (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una copia de instantánea de base de datos interna.
3. En la sección **Copia de seguridad del registro**, seleccione **Verificar copia de seguridad del registro al finalizar** para verificar la copia de seguridad del registro al finalizar.
4. En la sección **Configuración del script de verificación**, ingrese la ruta y los argumentos del prescript o postscript que deben ejecutarse antes o después de la operación de verificación, respectivamente.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

Paso 10: Revisar el resumen

1. Revise el resumen y luego seleccione **Finalizar**.

Crear grupos de recursos y adjuntar políticas para SQL Server

Un grupo de recursos es un contenedor al que se agregan recursos que desea respaldar y proteger juntos. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados con una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

Puede proteger recursos individualmente sin crear un nuevo grupo de recursos. Puede realizar copias de seguridad del recurso protegido.

Acerca de esta tarea

- 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 .
- No se admite agregar nuevas bases de datos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror .
- No se admite agregar nuevas bases de datos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror . Puede agregar recursos al grupo de recursos solo en estado normal o de conmutación por recuperación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista **Ver**.



Si ha agregado recientemente un recurso a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recién agregado.

3. Haga clic en **Nuevo grupo de recursos**.
4. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca el nombre del grupo de recursos. El nombre del grupo de recursos no debe exceder los 250 caracteres.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

Para este campo...	Haz esto...
Utilice un formato de nombre personalizado para la copia de instantáneas	Opcional: Ingrese un nombre y formato de instantánea personalizados. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Recursos, realice los siguientes pasos:

- Seleccione el nombre de host, el tipo de recurso y la instancia de SQL Server de las listas desplegables para filtrar la lista de recursos.



Si ha agregado recursos recientemente, aparecerán en la lista de Recursos disponibles solo después de actualizar su lista de recursos.

- Para mover recursos de la sección **Recursos disponibles** a la sección Recursos seleccionados, realice uno de los siguientes pasos:

- Seleccione **Seleccionar automáticamente todos los recursos en el mismo volumen de almacenamiento** para mover todos los recursos del mismo volumen a la sección Recursos seleccionados.
- Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.

6. En la página Políticas, realice los siguientes pasos:

- Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- En la sección Configurar programaciones para políticas seleccionadas, haga clic en *  * en la columna Configurar programaciones de la política para la que desea configurar la programación.
- En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación especificando la fecha de inicio, la fecha de vencimiento y la frecuencia, y luego haga clic en **Aceptar**.

Debe hacer esto para cada frecuencia indicada en la póliza. Los horarios configurados se enumeran en la columna Horarios aplicados en la sección **Configurar horarios para políticas seleccionadas**.

- Seleccione el programador de Microsoft SQL Server.

También debe seleccionar una instancia de programador para asociarla con la política de programación.

Si no selecciona el programador de Microsoft SQL Server, el valor predeterminado será el programador de Microsoft Windows.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter . No debe modificar las programaciones ni cambiar el nombre del trabajo de respaldo creado en el programador de Windows o en el agente de SQL Server.

7. En la página de Verificación, 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 host 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 **Cargar localizadores** para cargar los volúmenes SnapMirror y SnapVault para realizar la verificación en el almacenamiento secundario.
- b. Seleccione la política para la que desea configurar su programa de verificación y luego haga clic en  .
- c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada .

- d. Haga clic en **Aceptar**.

Los horarios configurados se enumeran en la columna Horarios aplicados. Puedes revisar y luego

editar haciendo clic en  * o eliminar haciendo clic en  *.

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

9. Revise el resumen y luego haga clic en **Finalizar**.

Información relacionada

["Crear políticas de respaldo para bases de datos de SQL Server"](#)

Cree grupos de recursos y habilite la protección secundaria para los recursos de Microsoft SQL Server en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:
 - a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:
 - a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
 - b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.

- c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Requisitos para realizar copias de seguridad de recursos SQL

Antes de realizar una copia de seguridad de un recurso SQL, debe asegurarse de que se cumplan varios requisitos.

- Debe haber migrado un recurso de un sistema de almacenamiento que no sea NetApp a un sistema de almacenamiento NetApp .
- Debes haber creado una política de respaldo.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.
- La operación de copia de seguridad iniciada por un usuario de directorio activo (AD) falla si la credencial de la instancia de SQL no está asignada al usuario o grupo de AD. Debe asignar la credencial de instancia de SQL al usuario o grupo de AD desde la página **Configuración > Acceso de usuario**.
- Debe haber creado un grupo de recursos con una política adjunta.
- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, la operación de respaldo en algunos hosts podría activarse tarde debido a problemas de red. Debe configurar el valor de FMaxRetryForUninitializedHosts en web.config utilizando el cmdlet PS Set-SmConfigSettings.

Cree una conexión al 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

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de administración única.

Pasos

1. Inicie una sesión de conexión de PowerShell Core mediante el cmdlet `Open-SmConnection`.

Este ejemplo abre una sesión de PowerShell:

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

2. Cree una nueva conexión al sistema de almacenamiento mediante el cmdlet `Add-SmStorageConnection`.

Este ejemplo crea una nueva conexión al sistema de almacenamiento:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una nueva credencial mediante el cmdlet `Add-SmCredential`.

Este ejemplo crea una nueva credencial llamada `FinanceAdmin` con credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede

obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Realizar copias de seguridad de los recursos de SQL

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Acerca de esta tarea

- Para optimizar la operación de copia de seguridad, debe crear un registro de búsqueda inversa de nombres de clúster y direcciones IP de Windows en el servidor DNS.
- Para la autenticación de credenciales de Windows, debe configurar sus credenciales antes de instalar los complementos.
- Para la autenticación de la instancia de SQL Server, debe agregar la credencial después de instalar los complementos.
- Para la autenticación gMSA, debe configurar gMSA mientras registra el host con SnapCenter en la página **Agregar host** o **Modificar host** para habilitar y usar gMSA.
- Si el host se agrega con gMSA y si gMSA tiene privilegios de inicio de sesión y de administrador del sistema, entonces gMSA puede conectarse a la instancia de SQL.
 - SnapCenter verificará si la autenticación para instancias de SQL está configurada. Si la autenticación está configurada, se accederá a la instancia de SQL utilizando esta credencial.
 - Si la autenticación no está configurada, utilice gMSA para ver si el complemento SQL está funcionando actualmente. Si el complemento está en funcionamiento, se utilizará para establecer una conexión a la instancia de SQL.
 - Se accederá a la instancia de SQL a través de la autenticación de credenciales de Windows cuando la autenticación para las instancias de SQL no esté configurada y el complemento no esté operativo.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos**, **Instancia** o **Grupo de disponibilidad** en la lista desplegable **Ver**.

- a. Seleccione la base de datos, instancia o grupo de disponibilidad que desea respaldar.

Cuando realiza una copia de seguridad de una instancia, la información sobre el estado de la última copia de seguridad o la marca de tiempo de esa instancia no estará disponible en la página de recursos.

En la vista de topología, no se puede diferenciar si el estado de la copia de seguridad, la marca de tiempo o la copia de seguridad son para una instancia o una base de datos.

3. En la página Recursos, seleccione la casilla de verificación **formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.

Por ejemplo, customtext_policy_hostname o resource_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

4. En la página Políticas, realice las siguientes tareas:

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

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

En la sección **Configurar programaciones para políticas seleccionadas**, se enumeran las políticas seleccionadas.

- b. Seleccionar *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En **Agregar horarios para la política** policy_name Cuadro de diálogo, configure la programación y luego seleccione **Aceptar**.

Aquí policy_name es el nombre de la política que has seleccionado.

Los horarios configurados se enumeran en la columna **Horarios aplicados**.

- a. Seleccione **Usar programador de Microsoft SQL Server** y, a continuación, seleccione la instancia del programador de la lista desplegable **Instancia del programador** que esté asociada con la política de programación.

5. En la página de Verificación, 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 host 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 el secundario** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- b. Seleccione la política para la que desea configurar su programa de verificación y luego seleccione *  *.
- c. En el cuadro de diálogo Agregar programaciones de verificación *policy_name*, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	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 falla con el error: No se pudo montar el disco.

- d. Seleccione **Aceptar**.

Los horarios configurados se enumeran en la columna Horarios aplicados.

6. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

7. Revise el resumen y luego seleccione **Finalizar**.

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

8. Seleccione **Hacer copia de seguridad ahora**.
9. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

- b. Seleccione **Verificar después de la copia de seguridad** para verificar su copia de seguridad.

c. Seleccione **Copia de seguridad**.



No debe cambiar el nombre del trabajo de copia de seguridad creado en el programador de Windows o en el agente de SQL Server.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

Se crea un grupo de recursos implícito. Puede ver esto seleccionando el usuario o grupo respectivo en la página de 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 configuraciones de MetroCluster , es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar. Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese guión, el `do_start method` El comando inicia el servicio del complemento VMware de SnapCenter . Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

Información relacionada

["Crear políticas de respaldo para bases de datos de SQL Server"](#)

["Las operaciones de respaldo fallan con un error de conexión MySQL debido al retraso en TCP_TIMEOUT"](#)

["La copia de seguridad falla con el error del programador de Windows"](#)

["Las operaciones de inactividad o agrupación de recursos fallan"](#)

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

Se muestra la solicitud de nombre de usuario y contraseña.

2. Cree una política de respaldo mediante el cmdlet `Add-SmPolicy`.

Este ejemplo crea una nueva política de respaldo con un tipo de respaldo SQL de FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Este ejemplo crea una nueva política de respaldo con un tipo de respaldo del sistema de archivos de Windows de CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra los recursos del host mediante el cmdlet Get-SmResources.

Este ejemplo descubre los recursos para el complemento de Microsoft SQL en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

Este ejemplo descubre los recursos de los sistemas de archivos de Windows en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

Este ejemplo crea un nuevo grupo de recursos de respaldo de base de datos 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"
```

Este ejemplo crea un nuevo grupo de recursos de respaldo del sistema de archivos de 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. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Vea el estado del trabajo de respaldo mediante el cmdlet Get-SmBackupReport.

Este ejemplo muestra un informe de resumen de trabajos de todos los trabajos que se ejecutaron en la fecha especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de grupos de recursos de SQL Server

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o seleccionando , y luego seleccionando la etiqueta. Luego puedes seleccionar  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si ha asociado varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

- b. Después de realizar la copia de seguridad, seleccione **Verificar** para verificar la copia de seguridad a pedido.

La opción **Verificar** de la política se aplica únicamente a trabajos programados.

c. Seleccione **Copia de seguridad**.

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

Información relacionada

["Crear políticas de respaldo para bases de datos de SQL Server"](#)

["Crear grupos de recursos y adjuntar políticas para SQL Server"](#)

["Las operaciones de respaldo fallan con un error de conexión MySQL debido al retraso en TCP_TIMEOUT"](#)

["La copia de seguridad falla con el error del programador de Windows"](#)

Supervisar las operaciones de copia de seguridad de recursos de SQL en la página Trabajos de SnapCenter

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desee verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en los recursos SQL en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 del complemento SnapCenter para Microsoft SQL Server

Puede cancelar operaciones de copia de seguridad que estén en ejecución, en cola o que no respondan. Cuando se cancela una operación de copia de seguridad, el servidor SnapCenter detiene la operación y elimina todas las instantáneas del almacenamiento si la copia de seguridad creada no está registrada en el servidor SnapCenter . Si la copia de seguridad ya está registrada en SnapCenter Server, no revertirá la instantánea ya creada incluso después de que se active la cancelación.

Antes de empezar

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.
- Puede cancelar únicamente las operaciones de registro o de copia de seguridad completa que estén en cola o en ejecución.
- No es posible cancelar la operación una vez iniciada la verificación.

Si cancela la operación antes de la verificación, la operación se cancelará y no se realizará la operación de verificación.

- Puede cancelar una operación de copia de seguridad desde la página Monitor o desde el panel Actividad.
- Además de utilizar la GUI de SnapCenter , puede utilizar cmdlets de PowerShell para cancelar operaciones.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, seleccione Monitor > Trabajos. 2. Seleccione el trabajo y seleccione Cancelar trabajo.
Panel de actividades	1. Después de iniciar el trabajo de respaldo, seleccione  en el panel Actividad para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, seleccione Cancelar trabajo.

Resultado

La operación se cancela y el recurso vuelve al estado anterior. Si la operación que canceló no responde en el estado de cancelación o ejecución, debe ejecutar la `Cancel-SmJob -JobID <int> -Force cmdlet` para detener forzosamente la operación de copia de seguridad.

Ver copias de seguridad y clones de SQL Server en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario.

Acerca de esta tarea

En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Puede revisar los siguientes íconos en la vista **Administrar copias** para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .
 - La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del

almacenamiento secundario.

Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), puede ver los siguientes íconos adicionales:



El sitio de réplica está activo.



El sitio de réplica está inactivo.



No se ha restablecido la relación de espejo secundario o bóveda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso seleccionado es una base de datos clonada, proteja la base de datos clonada; la fuente del clon se muestra en la página Topología. Haga clic en **Detalles** para ver la copia de seguridad utilizada para clonar.

Si el recurso está protegido, se muestra la página Topología del recurso seleccionado.

4. Revise la tarjeta Resumen para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración 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 respaldo de SnapCenter consultando a ONTAP los sitios principales y de réplica. Una programación

semanal también realiza esta actividad para 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 Async Mirror o Async MirrorVault con el nuevo destino principal se deben configurar manualmente después de la conmutación por error. Desde ONTAP 9.15.1 en adelante, Async Mirror o Async MirrorVault se configura automáticamente en el nuevo destino principal.
- Después de la conmutación por error, se debe crear una copia de seguridad para que SnapCenter esté al tanto de la conmutación por error. Puede hacer clic en **Actualizar** sólo después de haber creado una copia de seguridad.

5. En la vista **Administrar copias**, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación, cambio de nombre y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

7. Seleccione un clon de la tabla y haga clic en **Clonar división**.
8. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en .

Limpiar el recuento de copias de seguridad secundarias mediante cmdlets de PowerShell

Puede utilizar el cmdlet Remove-SmBackup para limpiar el recuento de copias de seguridad de las copias de seguridad secundarias que no tienen instantánea. Es posible que desee utilizar este cmdlet cuando la cantidad total de instantáneas que se muestran en la topología Administrar copias no coincidan con la configuración de retención de instantáneas de almacenamiento secundario.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Limpie el recuento de copias de seguridad secundarias utilizando el parámetro -CleanupSecondaryBackups.

Este ejemplo limpia el recuento de copias de seguridad para copias de seguridad secundarias sin instantáneas:

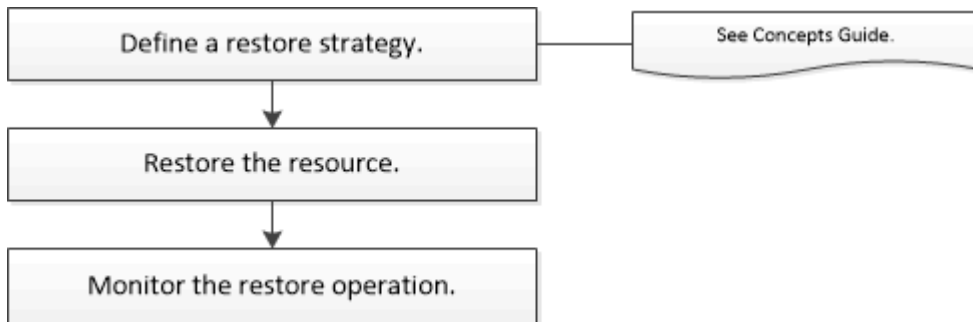
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s) .
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

Restaurar recursos de SQL Server

Restaurar flujo de trabajo

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server restaurando los datos de una o más copias de seguridad en su sistema de archivos activo y luego recuperando la base de datos. También puede restaurar bases de datos que estén en grupos de disponibilidad y luego agregar las bases de datos restauradas al grupo de disponibilidad. 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 la base de datos:



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 ["Guía de referencia de cmdlets del software SnapCenter"](#)

Encuentre más información

["Restaurar una base de datos de SQL Server desde un almacenamiento secundario"](#)

["Restaurar y recuperar recursos mediante cmdlets de PowerShell"](#)

["La operación de restauración podría fallar en Windows 2008 R2"](#)

Requisitos para restaurar una base de datos

Antes de restaurar una base de datos de SQL Server desde una copia de seguridad del complemento de SnapCenter para Microsoft SQL Server, debe asegurarse de que se cumplan varios requisitos.

- La instancia de SQL Server de destino debe estar en línea y en ejecución antes de poder restaurar una base de datos.

Esto se aplica tanto a las operaciones de restauración de la base de datos del usuario como a las operaciones de restauración de la base de datos del sistema.

- Las operaciones de SnapCenter que están programadas para ejecutarse en los datos de SQL Server que está restaurando deben estar deshabilitadas, incluidos todos los trabajos programados en servidores de administración remota o de verificación remota.
- Si las bases de datos del sistema no funcionan, primero debe reconstruirlas utilizando una utilidad de SQL Server.
- Si está instalando el complemento, asegúrese de otorgar permisos para que otras funciones puedan restaurar las copias de seguridad del grupo de disponibilidad (AG).

La restauración de AG falla cuando se cumple una de las siguientes condiciones:

- Si el complemento lo instala el usuario RBAC y un administrador intenta restaurar una copia de seguridad de AG
- Si un administrador instala el complemento y un usuario RBAC intenta restaurar una copia de seguridad de AG
- Si está restaurando copias de seguridad del directorio de registro personalizado en un host alternativo, el servidor SnapCenter y el host del complemento deben tener la misma versión de SnapCenter instalada.
- Debe tener instalado el hotfix de Microsoft, KB2887595. El sitio de soporte de Microsoft contiene más información sobre KB2887595.

["Artículo de soporte técnico de Microsoft 2887595: Paquete acumulativo de actualizaciones de Windows RT 8.1, Windows 8.1 y Windows Server 2012 R2: noviembre de 2013"](#)

- Debes haber realizado una copia de seguridad de los grupos de recursos o de la base de datos.
- Si está replicando instantáneas a un espejo o bóveda, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) tanto para los volúmenes de origen como para los volúmenes 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 copia de seguridad y clonación deben detenerse antes de restaurar la base de datos.
- La operación de restauración puede expirar si el tamaño de la base de datos está en terabytes (TB).

Debe aumentar el valor del parámetro RESTTimeout de SnapCenter Server a 20000000 ms ejecutando el siguiente comando: `Set-SmConfigSettings -Agent -configSettings @"{"RESTTimeout" = "20000000"}.` Según el tamaño de la base de datos, el valor de tiempo de espera se puede cambiar y el valor máximo que se puede establecer es 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 Restaurar.

Restaurar copias de seguridad de bases de datos de SQL Server

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server respaldadas. La

restauración de la base de datos es un proceso de varias fases que copia todos los datos y las páginas de registro de una copia de seguridad de SQL Server especificada a una base de datos especificada.

Acerca de esta tarea

- Puede restaurar las bases de datos de SQL Server respaldadas en una instancia de SQL Server diferente en el mismo host donde se creó la copia de seguridad.

Puede utilizar SnapCenter para restaurar las bases de datos de SQL Server respaldadas en una ruta alternativa para no reemplazar una versión de producción.

- SnapCenter puede restaurar bases de datos en un clúster de Windows sin desconectar el grupo de clústeres de SQL Server.
- Si se produce una falla del clúster (una operación de movimiento de grupo de clústeres) durante una operación de restauración (por ejemplo, si el nodo que posee los recursos deja de funcionar), debe volver a conectarse a la instancia de SQL Server y luego reiniciar la operación de restauración.
- No se puede restaurar la base de datos cuando los usuarios o los trabajos del Agente SQL Server acceden a la base de datos.
- No se pueden restaurar las bases de datos del sistema a una ruta alternativa.
- `SCRIPTS_PATH` se define utilizando la clave `PredefinedWindowsScriptsDirectory` ubicada en el archivo `SMCoreServiceHost.exe.Config` del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio `SMcore`. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: `API /4.7/configsettings`

Puede utilizar la API `GET` para mostrar el valor de la clave. La API `SET` no es compatible.

- La mayoría de los campos de las páginas del Asistente de restauración se explican por sí solos. La siguiente información describe campos para los cuales podría necesitar orientación.
- Para la operación de restauración de sincronización activa de SnapMirror , debe seleccionar la copia de seguridad de la ubicación principal.
- Para las políticas habilitadas para SnapLock , para ONTAP 9.12.1 y versiones anteriores, si especifica un período de bloqueo de instantáneas, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de vencimiento de SnapLock . El administrador de almacenamiento debe limpiar manualmente los clones después del tiempo de vencimiento de SnapLock .

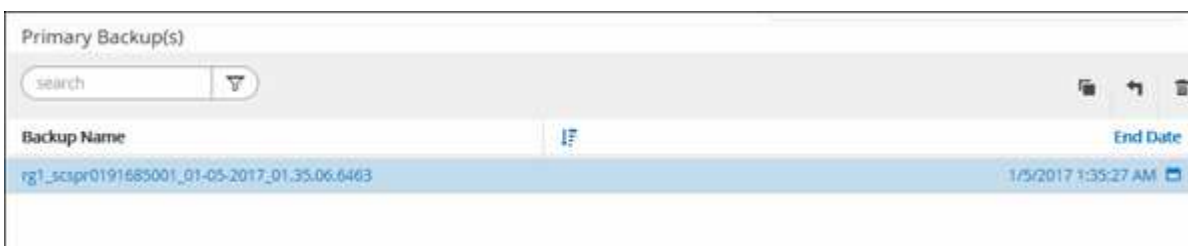
Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de la lista.

Se muestra la página de topología.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento.
5. Seleccione la copia de seguridad de la tabla y luego haga clic en el botón  icono.



6. En la página Restaurar ámbito, seleccione una de las siguientes opciones:

Opción	Descripción
Restaurar la base de datos en el mismo host donde se creó la copia de seguridad	Seleccione esta opción si desea restaurar la base de datos en el mismo servidor SQL donde se realizan las copias de seguridad.
Restaurar la base de datos a 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 en uno diferente donde se realizan las copias de seguridad. 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 extensión del archivo de base de datos original. Si la opción Restaurar la base de datos en un host alternativo no se muestra en la página Restaurar ámbito, borre la memoria caché del navegador.

Opción	Descripción
Restaurar la base de datos utilizando archivos de base de datos existentes	Seleccione esta opción si desea que la base de datos se restaure en un servidor SQL alternativo en el mismo host o en uno diferente donde se realizan las copias de seguridad. Los archivos de base de datos ya deben estar presentes en las rutas de archivos existentes indicadas. 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 **Ámbito de recuperación**, seleccione una de las siguientes opciones:

Opción	Descripción
Ninguno	Seleccione Ninguno cuando necesite restaurar solo la copia de seguridad completa sin ningún registro.
Todas las copias de seguridad de registros	Seleccione la operación de restauración de copia de seguridad actualizada Todas las copias de seguridad de registros para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa.
Mediante copias de seguridad de registros hasta	Seleccione Por copias de seguridad de registros para realizar una operación de restauración en un punto en el tiempo, que restaura la base de datos basándose en los registros de copia de seguridad hasta el registro de copia de seguridad con la fecha seleccionada.
Por fecha específica hasta	Seleccione Por fecha específica hasta para especificar la fecha y la hora después de las cuales los registros de transacciones no se aplicarán a la base de datos restaurada. Esta operación de restauración en un punto determinado del tiempo detiene la restauración de las entradas del registro de transacciones que se registraron después de la fecha y hora especificadas.

Opción	Descripción
Utilice un directorio de registro personalizado	Si ha seleccionado Todas las copias de seguridad de registros, Por copias de seguridad de registros o Por fecha específica hasta y los registros se encuentran en una ubicación personalizada, seleccione Usar directorio de registros 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 en un host alternativo o Restaurar la base de datos utilizando archivos de base de datos existentes. También puede utilizar la ruta compartida, pero asegúrese de que el usuario SQL pueda acceder a ella.  El directorio de registro personalizado no es compatible con la base de datos del grupo de disponibilidad.

8. En la página de Operaciones previas, realice los siguientes pasos:

a. En la página Opciones de restauración previa, 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 **Conservar configuración de replicación de base de datos SQL** para restaurar la base de datos y conservar 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 **Salir de restauración si falla la copia de seguridad del registro de transacciones antes de la restauración** para cancelar la operación de restauración si falla la copia de seguridad del registro de transacciones.

b. Especifique scripts opcionales para ejecutar antes de realizar un trabajo de restauración.

Por ejemplo, puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

9. En la página Post Ops, realice los siguientes pasos:

a. En la sección Elegir estado de la base de datos después de completar la restauración, seleccione una de las siguientes opciones:

- Seleccione **Operacional, pero no disponible para restaurar registros de transacciones adicionales** si está restaurando todas las copias de seguridad necesarias ahora.

Este es el comportamiento predeterminado, que deja la base de datos lista para su uso revirtiendo las transacciones no confirmadas. No puede restaurar registros de transacciones adicionales hasta que cree una copia de seguridad.

- Seleccione **No operativo, pero disponible para restaurar registros transaccionales adicionales** para dejar la base de datos no operativa sin revertir las transacciones no confirmadas.

Se pueden restaurar registros de transacciones adicionales. No puedes utilizar la base de datos hasta que se recupere.

- Seleccione **Modo de solo lectura, disponible para restaurar registros transaccionales adicionales** para dejar la base de datos en modo de solo lectura.

Esta opción deshace las transacciones no confirmadas, pero guarda las acciones deshechas en un archivo en espera para que se puedan revertir los efectos de recuperación.

Si la opción **Deshacer directorio** está habilitada, se restauran más registros de transacciones. Si la operación de restauración del registro de transacciones no es exitosa, los cambios se pueden revertir. La documentación de SQL Server contiene más información.

- b. Especifique scripts opcionales para ejecutar después de realizar un trabajo de restauración.

Por ejemplo, puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a `SCRIPTS_PATH`.

10. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

11. Revise el resumen y luego haga clic en **Finalizar**.
12. Supervise el proceso de restauración utilizando la página **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId  
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269  
-Confirm:$false  
output:  
Name : Restore  
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar una base de datos de SQL Server desde un almacenamiento secundario

Puede restaurar las bases de datos de SQL Server respaldadas desde los LUN físicos (RDM, iSCSI o FCP) en un sistema de almacenamiento secundario. La función Restaurar es un proceso multifase que copia todos los datos y las páginas de registro de una copia de seguridad de SQL Server especificada que reside en el sistema de almacenamiento secundario a una base de datos especificada.

Antes de empezar

- Debes haber replicado las instantáneas del sistema de almacenamiento primario al secundario.

- Debe asegurarse de que el servidor SnapCenter y el host del complemento puedan conectarse al sistema de almacenamiento secundario.
- La mayoría de los campos de las páginas del asistente de restauración se explican en el proceso de restauración básico. La siguiente información describe algunos de los campos para los que podría necesitar orientación.

Acerca de esta tarea

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **Complemento de SnapCenter para SQL Server** de la lista.
2. En la página Recursos, seleccione **Base de datos** o **Grupo de recursos** en la lista desplegable **Ver**.
3. Seleccione la base de datos o el grupo de recursos.

Se muestra la página de topología de la base de datos o del grupo de recursos.

4. En la sección Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento secundario (duplicado o bóveda).
5. Seleccione la copia de seguridad de la lista y luego haga clic en  .
6. En la página Ubicación, elija el volumen de destino para restaurar el recurso seleccionado.
7. Complete el asistente de restauración, revise el resumen y luego haga clic en **Finalizar**.

Si restauró una base de datos en una ruta diferente que comparten otras bases de datos, debe realizar una copia de seguridad completa y una verificación de copia de seguridad para confirmar que la base de datos restaurada esté libre de corrupción a nivel físico.

Restaurar recursos mediante cmdlets de PowerShell

Restaurar una copia de seguridad de un recurso incluye iniciar una sesión de conexión con el servidor SnapCenter , enumerar las copias de seguridad y recuperar información de las copias de seguridad, y restaurar una copia de seguridad.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```

PS C:\> Get-SmBackupReport -FromDate "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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Resembrar bases de datos del grupo de disponibilidad

Reseed es una opción para restaurar bases de datos del grupo de disponibilidad (AG). Si una base de datos secundaria se desincroniza con la base de datos principal en un AG, puede volver a generar la base de datos secundaria.

Antes de empezar

- Debe haber creado una copia de seguridad de la base de datos AG secundaria que desea restaurar.
- El servidor SnapCenter y el host del complemento deben tener la misma versión de SnapCenter instalada.

Acerca de esta tarea

- No se puede realizar la operación de resiembra en bases de datos primarias.

- No se puede realizar una operación de resiembra si la base de datos de réplica se elimina del grupo de disponibilidad. Cuando se elimina la réplica, la operación de resiembra falla.
- Mientras se ejecuta la operación de resiembra en la base de datos del grupo de disponibilidad de SQL, no debe activar copias de seguridad de registros en las bases de datos de réplica de la base de datos de ese grupo de disponibilidad. Si activa copias de seguridad de registros durante la operación de resiembra, la operación de resiembra falla con el mensaje de error La base de datos reflejada, "database_name" no tiene suficientes datos del registro de transacciones para preservar la cadena de copia de seguridad de registros de la base de datos principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **Complemento de SnapCenter para SQL Server** de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista **Ver**.
3. Seleccione la base de datos AG secundaria de la lista.
4. Haga clic en **Resembrar**.
5. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Supervisar las operaciones de restauración de recursos SQL

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Cancelar operaciones de restauración de recursos SQL

Puede cancelar trabajos de restauración que estén en cola.

Debe iniciar 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.
- Puede utilizar la GUI de SnapCenter, los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones de restauración que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de restauración en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 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 Actividad para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

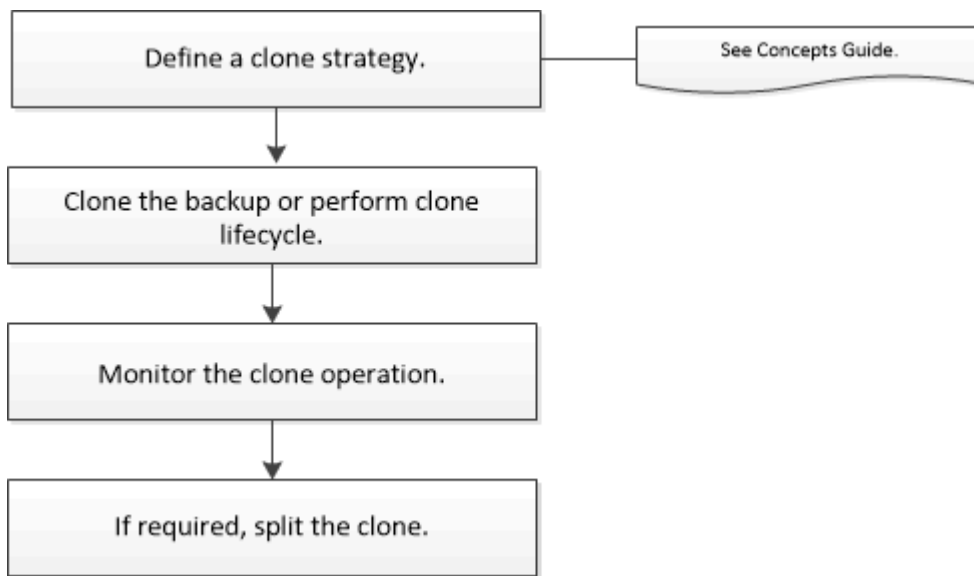
Clonar recursos de base de datos de SQL Server

Flujo de trabajo de clonación

Debe realizar varias tareas utilizando SnapCenter Server antes de clonar recursos de base de datos desde una copia de seguridad. La clonación de bases de datos es el proceso de crear una copia en un punto determinado del tiempo de una base de datos de producción o de su conjunto de copias de seguridad. Puede clonar bases de datos para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de la base de datos actual durante los ciclos de desarrollo de aplicaciones, para utilizar las herramientas de extracción y manipulación de datos al completar almacenes de datos, o para recuperar datos que se eliminaron o modificaron por error.

Una operación de clonación de base de datos genera informes basados en los ID de trabajo.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar las operaciones de clonación:



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 ["Guía de referencia de cmdlets del software SnapCenter"](#)

Encuentre más información

["Clonar desde una copia de seguridad de la base de datos de SQL Server"](#)

["Realizar ciclo de vida de clonación"](#)

["La operación de clonación puede fallar o tardar más tiempo en completarse con el valor TCP_TIMEOUT predeterminado"](#)

Clonar desde una copia de seguridad de la base de datos de SQL Server

Puede utilizar SnapCenter para clonar una copia de seguridad de una base de datos de SQL Server. Si desea acceder o restaurar una versión anterior de los datos, puede clonar copias de seguridad de la base de datos a pedido.

Antes de empezar

- Debe haberse preparado para la protección de datos completando tareas como agregar hosts, identificar recursos y crear conexiones al sistema de almacenamiento.
- Deberías haber realizado copias de seguridad de las bases de datos o de los grupos de recursos.
- El tipo de protección, como espejo, bóveda o espejo-bóveda para LUN de datos y LUN de registro, debe ser el mismo para descubrir localizadores secundarios durante la clonación a un host alternativo mediante copias de seguridad de registros.
- Si no se puede encontrar la unidad clonada montada durante una operación de clonación de SnapCenter , debe cambiar el parámetro CloneRetryTimeout de SnapCenter Server a 300.
- Debe asegurarse de que los agregados que alojan los volúmenes estén en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

- Al clonar una instancia de base de datos independiente, asegúrese de que la ruta del punto de montaje exista y que sea un disco dedicado.
- Al clonar en una instancia de clúster de conmutación por error (FCI), asegúrese de que existan los puntos de montaje, que sea un disco compartido y que la ruta y la FCI pertenezcan al mismo grupo de recursos SQL.
- Asegúrese de que solo haya 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 está en un volumen compartido de clúster (csv), entonces la base de datos clonada estará en el csv.
- SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.



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

- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione **Complemento de SnapCenter para SQL Server** de la lista.
2. En la página Recursos, seleccione **Base de datos** o **Grupo de recursos** en la lista **Ver**.



No se admite la clonación del backup de una instancia.

3. Seleccione la base de datos o el grupo de recursos.
4. Desde la página de vista **Administrar copias**, seleccione la copia de seguridad del sistema de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. Seleccione la copia de seguridad y luego seleccione *  *.
6. En la página **Opciones de clonación**, realice las siguientes acciones:

Para este campo...	Haz esto...
Servidor clonado	Seleccione un host en el que se debe crear el clon.
Instancia de clonación	Seleccione una instancia de clonación en la que desea clonar la copia de seguridad de la base de datos. Esta instancia de SQL debe estar ubicada en el servidor clon especificado.
Sufijo de clonación	Introduzca un sufijo que se agregará al nombre del archivo clonado para identificar que la base de datos es un clon. Por ejemplo, <i>db1_clone</i>. Si está clonando en la misma ubicación que la base de datos original, debe proporcionar un sufijo para diferenciar la base de datos clonada de la base de datos original. De lo contrario la operación falla.

Para este campo...	Haz esto...
Asignar automáticamente el punto de montaje o Asignar automáticamente el punto de montaje del volumen en la ruta	Elija si desea asignar automáticamente un punto de montaje o un punto de montaje de volumen bajo una ruta. Asignar automáticamente el punto de montaje del volumen bajo la ruta: el punto de montaje bajo una ruta le permite proporcionar un directorio específico. Los puntos de montaje se crearán dentro de ese directorio. Antes de elegir esta opción, debe asegurarse de que el directorio esté vacío. Si hay una base de datos en el directorio, la base de datos estará en un estado no válido después de la operación de montaje.

7. En la página Registros, seleccione una de las siguientes opciones:

Para este campo...	Haz esto...
Ninguno	Elija esta opción cuando desee clonar solo la copia de seguridad completa sin ningún registro.
Todas las copias de seguridad de registros	Elija esta opción para clonar todas las copias de seguridad de registros disponibles con fecha posterior a la copia de seguridad completa.
Mediante copias de seguridad de registros hasta	Elija esta opción para clonar la base de datos en función de los registros de respaldo que se crearon hasta el registro de respaldo con la fecha seleccionada.
Por fecha específica hasta	Especifique la fecha y la hora después de las cuales los registros de transacciones no se aplicarán a la base de datos clonada. Este clon de punto en el tiempo detiene la clonación de las entradas del registro de transacciones que se registraron después de la fecha y hora especificadas.

8. En la página **Script**, ingrese el tiempo de espera del script, la ruta y los argumentos del prescript o postscript que se deben ejecutar antes o después de la operación de clonación, respectivamente.

Por ejemplo, puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

El tiempo de espera predeterminado del script es de 60 segundos.

9. En la página **Notificación**, de la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de clonación realizada, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

Para EMS, puede consultar ["Gestionar la recopilación de datos de EMS"](#)

10. Revise el resumen y luego seleccione **Finalizar**.
11. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

Después de terminar

Una vez creado el clon, nunca debes cambiarle el nombre.

Información relacionada

["La operación de clonación puede fallar o tardar más tiempo en completarse con el valor TCP_TIMEOUT predeterminado"](#)

["La clonación de la base de datos de la instancia del clúster de conmutación por error falla"](#)

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Enumere las copias de seguridad que se pueden clonar mediante el cmdlet Get-SmBackup o Get-SmResourceGroup.

Este ejemplo muestra información sobre todas las copias de seguridad 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	

Este ejemplo muestra información sobre un grupo de recursos específico, sus recursos y 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}  
HostResourceMapping : {}  
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 clonación desde una copia de seguridad existente utilizando el cmdlet New-SmClone.

Este ejemplo crea un clon a partir de una copia de seguridad especificada 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
```

Este ejemplo crea un clon de una instancia específica 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. Vea el estado del trabajo de clonación mediante el cmdlet Get-SmCloneReport.

Este ejemplo muestra un informe clonado para el ID de trabajo especificado:

```
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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar ciclo de vida de clonación

Con SnapCenter, puede crear clones desde un grupo de recursos o una base de datos. Puede realizar una clonación a pedido o programar operaciones de clonación recurrentes de un grupo de recursos o una base de datos. Si clona una copia de seguridad periódicamente, puede usar el clon para desarrollar aplicaciones, completar datos o recuperar datos.

SnapCenter le permite programar múltiples operaciones de clonación para que se ejecuten simultáneamente en múltiples servidores.

Antes de empezar

- Al clonar una instancia de base de datos independiente, asegúrese de que la ruta del punto de montaje exista y que sea un disco dedicado.
- Al clonar en una instancia de clúster de conmutación por error (FCI), asegúrese de que existan los puntos de montaje, que sea un disco compartido y que la ruta y la FCI pertenezcan al mismo grupo de recursos SQL.
- Si la base de datos de origen o la instancia de destino está en un volumen compartido de clúster (csv), entonces la base de datos clonada estará en el csv.



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

Acerca de esta tarea

- SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.

- La mayoría de los campos de las páginas del Asistente para el ciclo de vida de clones se explican por sí solos. La siguiente información describe campos para los cuales podría necesitar orientación.
- Para ONTAP 9.12.1 y versiones anteriores, si especifica un período de bloqueo de instantáneas, los clones creados a partir de las instantáneas a prueba de manipulaciones heredarán el tiempo de vencimiento de SnapLock . El administrador de almacenamiento debe limpiar manualmente los clones después del tiempo de vencimiento de SnapLock .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione el grupo de recursos o la base de datos y luego haga clic en **Clonar ciclo de vida**.
4. En la página Opciones, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre del trabajo de clonación	Especifique el nombre del trabajo del ciclo de vida del clon que ayuda a supervisar y modificar el trabajo del ciclo de vida del clon.
Servidor clonado	Seleccione el host en el que se colocará el clon.
Instancia de clonación	Seleccione la instancia de clonación en la que desea clonar la base de datos. Esta instancia de SQL debe estar ubicada en el servidor clon especificado.

Para este campo...	Haz esto...
Sufijo de clonación	Introduzca un sufijo que se agregará a la base de datos de clones para identificar que es un clon. Cada instancia de SQL que se utiliza para crear un grupo de recursos clonados debe tener un nombre de base de datos único. Por ejemplo, si el grupo de recursos clonados contiene una base de datos de origen "db1" de una instancia SQL "inst1", y si "db1" se clona en "inst1", entonces el nombre de la base de datos clonada debe ser "db1clone". "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 SQL "inst2", entonces el nombre de la base de datos clonada puede seguir siendo "db1" (el sufijo es opcional) porque la base de datos se clona en una instancia diferente.
Asignar automáticamente el punto de montaje o Asignar automáticamente el punto de montaje del volumen en la ruta	Elija si desea asignar automáticamente un punto de montaje o un punto de montaje de volumen bajo una ruta. Al elegir asignar automáticamente un punto de montaje de volumen en una ruta, podrá proporcionar un directorio específico. Los puntos de montaje se crearán dentro de ese directorio. Antes de elegir esta opción, debe asegurarse de que el directorio esté vacío. Si hay una base de datos en el directorio, la base de datos estará en un estado no válido después de la operación de montaje.

- En la página Ubicación, seleccione una ubicación de almacenamiento para crear un clon.
- En la página Script, ingrese la ruta y los argumentos del prescript o postscript que deben ejecutarse antes o después de la operación de clonación, respectivamente.

Por ejemplo, puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

El tiempo de espera predeterminado del script es de 60 segundos.

- En la página Programación, realice una de las siguientes acciones:
 - Seleccione **Ejecutar ahora** si desea ejecutar el trabajo de clonación inmediatamente.
 - Seleccione **Configurar programación** cuando desee determinar con qué frecuencia debe ocurrir la operación de clonación, cuándo debe comenzar la programación de clonación, en qué día debe ocurrir la operación de clonación, cuándo debe expirar la programación y si los clones deben eliminarse después de que expire la programación.
- En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto

del correo electrónico. Si desea adjuntar el informe de la operación de clonación realizada, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

Para EMS, puede consultar "[Gestionar la recopilación de datos de EMS](#)"

9. Revise el resumen y luego haga clic en **Finalizar**.

Debes supervisar el proceso de clonación utilizando la página **Monitor > Trabajos**.

Supervisar operaciones de clonación de bases de datos SQL

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Cancelar operaciones de clonación de recursos SQL

Puede cancelar operaciones de clonación que estén en cola.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones de clonación.

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 clonación en ejecución.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de clonación en cola.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de clonación en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 2. Seleccione la operación y haga clic en Cancelar trabajo.
Panel de actividades	1. Después de iniciar la operación de clonación, haga clic en  en el panel Actividad para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte ["Dividir un volumen FlexClone de su volumen principal"](#) .

- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Proteger las bases de datos de SAP HANA

Complemento de SnapCenter para bases de datos SAP HANA

Descripción general del complemento de SnapCenter para la base de datos SAP HANA

El complemento SnapCenter para la base de datos SAP HANA es un componente del lado del host del SnapCenter software de NetApp que permite la gestión de protección de datos consciente de la aplicación de las bases de datos SAP HANA. El complemento para la base de datos SAP HANA automatiza la copia de seguridad, la restauración y la clonación de bases de datos SAP HANA en su entorno SnapCenter .

SnapCenter admite contenedores de bases de datos de contenedores únicos y multiinquilino (MDC). Puede utilizar el complemento para la base de datos SAP HANA en entornos Windows y Linux. El complemento que no está instalado en el host de la base de datos HANA se conoce como complemento de host centralizado. Este complemento puede administrar varias bases de datos HANA en diferentes hosts.

Cuando se instala el complemento para la base de datos SAP HANA, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen. También puede utilizar el complemento con la tecnología NetApp SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de los estándares.

El complemento para la base de datos SAP HANA admite la sincronización activa de SnapMirror (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]) que permite que los servicios comerciales sigan funcionando incluso ante una falla total del sitio, lo que permite que las aplicaciones conmuten por error de manera transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una conmutación por error con la sincronización activa de SnapMirror .

Qué puede hacer utilizando el complemento SnapCenter para la base de datos SAP HANA

Cuando instala el complemento para la base de datos SAP HANA en su entorno, puede usar SnapCenter para realizar copias de seguridad, restaurar y clonar bases de datos SAP HANA y sus recursos. También puede realizar tareas que respalden dichas operaciones.

- Agregar bases de datos.
- Crear copias de seguridad.
- Restaurar desde copias de seguridad.
- Copias de seguridad clonadas.
- Programar operaciones de respaldo.
- Supervisar operaciones de copia de seguridad, restauración y clonación.
- Ver informes de operaciones de copia de seguridad, restauración y clonación.

Funciones del complemento SnapCenter para la base de datos SAP HANA

SnapCenter se integra con la aplicación complementaria y con las tecnologías NetApp en el sistema de almacenamiento. Para trabajar con el complemento para la base de datos SAP HANA, utilice la interfaz gráfica de usuario de SnapCenter .

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite realizar operaciones consistentes de copia de seguridad, restauración y clonación en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y supervisar trabajos en todos los complementos.

- **Administración central automatizada**

Puede programar operaciones de respaldo, configurar la retención de respaldo basada en políticas y realizar operaciones de restauración. También puede supervisar su entorno de forma proactiva configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología de copia Snapshot de NetApp sin interrupciones**

SnapCenter utiliza la tecnología NetApp Snapshot con el complemento para la base de datos SAP HANA para realizar copias de seguridad de los recursos.

El uso del complemento para la base de datos SAP HANA también ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de copia de seguridad, restauración y clonación
- Seguridad respaldada por RBAC y delegación de roles centralizada

También puede configurar las credenciales para que los usuarios autorizados de SnapCenter tengan permisos a nivel de aplicación.

- Creación de copias puntuales y con uso eficiente del espacio de recursos para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

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

- Compatibilidad con la función de instantánea del grupo de consistencia (CG) de ONTAP como parte de la creación de copias de seguridad.
- Capacidad de ejecutar múltiples copias de seguridad simultáneamente en múltiples hosts de recursos

En una sola operación, las instantáneas se consolidan cuando los recursos de un solo host comparten el mismo volumen.

- Capacidad de crear instantáneas mediante comandos externos.
- Soporte para copias de seguridad basadas en archivos.
- Soporte para Linux LVM en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el complemento de SnapCenter para la base de datos SAP HANA

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas

físicas como en máquinas virtuales (VM). Debe verificar la compatibilidad con su tipo de almacenamiento antes de instalar el complemento de SnapCenter para la base de datos SAP HANA.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • Volúmenes conectados a NFS
VMware ESXi	• El escaneo de los adaptadores de bus de host (HBA) puede demorar mucho tiempo en completarse porque SnapCenter escanea todos los adaptadores de bus de host presentes en el host. Puede editar el archivo LinuxConfig.pm ubicado en <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> para establecer el valor del parámetro SCSI_HOSTS_OPTIMIZED_RESCAN en 1 para volver a escanear solo los HBA que figuran en HBA_DRIVER_NAMES. • LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creados • Volúmenes NFS conectados directamente al sistema invitado • Almacenes de datos vVol tanto en NFS como en SAN El almacén de datos vVol solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP necesarios para el complemento SAP HANA

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo

- lun crear
- lun crear
- lun crear
- eliminar lun
- agregar igroup lun
- crear igroup lun
- eliminar igroup lun
- Cambiar nombre de igroup lun
- Cambiar nombre de igroup lun
- Programa de igroup de Lun
- Asignación de LUN a nodos de informes adicionales
- creación de mapeo LUN
- eliminar mapeo lun
- Mapeo de LUN: eliminar nodos de informes
- espectáculo de mapeo de lun
- modificar lun
- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- lun reserva persistente clara
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen

- clonación de volumen división parada
- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- tiempo de caducidad de modificación de instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFs de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIF de vserver
- Mostrar copia de sombra de CIF de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi
- Mostrar conexión iscsi de vserver

- espectáculo vserver
- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red
 - Mostrar interfaz de red
 - vserver

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para bases de datos SAP HANA

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#) .

Estrategia de respaldo para bases de datos de SAP HANA

Definir una estrategia de respaldo para bases de datos de SAP HANA

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a tener los respaldos que necesita para restaurar o clonar sus recursos con éxito. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Acerca de esta tarea

Un SLA define el nivel de servicio que se espera y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. RPO define la estrategia para la edad de los

archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA, RTO y RPO contribuyen a la estrategia de protección de datos.

Pasos

1. Determina cuándo debes realizar copias de seguridad de tus recursos.
2. Decide cuántos trabajos de respaldo necesitas.
3. Decide cómo nombrar tus copias de seguridad.
4. Decida si desea crear una política basada en copias de instantáneas para realizar copias de seguridad de instantáneas consistentes con la aplicación de la base de datos.
5. Decide si quieres verificar la integridad de la base de datos.
6. Decida si desea utilizar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
7. Determine el período de retención de las instantáneas en el sistema de almacenamiento de origen y el destino SnapMirror .
8. Determine si desea ejecutar algún comando antes o después de la operación de copia de seguridad y proporcione un script previo o posterior.

Descubrimiento automático de recursos en el host Linux

Los recursos son bases de datos de SAP HANA y volúmenes que no son de datos en el host Linux que administra SnapCenter. Después de instalar el complemento de SnapCenter para la base de datos SAP HANA, las bases de datos SAP HANA en ese host Linux se detectan automáticamente y se muestran en la página Recursos.

El descubrimiento automático es compatible con los siguientes recursos de SAP HANA:

- Contenedores individuales

Después de instalar o actualizar el complemento, los recursos de contenedor único ubicados en un complemento de host centralizado continuarán como recursos agregados manualmente.

Después de instalar o actualizar el complemento, las bases de datos de SAP HANA se descubren automáticamente solo en los hosts SAP HANA Linux que están registrados directamente en SnapCenter.

- Contenedor de base de datos multiinquilino (MDC)

Después de instalar o actualizar el complemento, los recursos de MDC ubicados en un complemento de host centralizado continuarán como recursos agregados manualmente.

Debe continuar agregando manualmente los recursos de MDC en el complemento de host centralizado después de actualizar a SnapCenter 4.3.

Para los hosts SAP HANA Linux registrados directamente en SnapCenter, la instalación o actualización del complemento activará un descubrimiento automático de recursos en el host. Después de actualizar el complemento, por cada recurso MDC que estaba ubicado en el host del complemento, se descubrirá automáticamente otro recurso MDC con un formato GUID diferente y se registrará en SnapCenter. El nuevo recurso estará en estado bloqueado.

Por ejemplo, en SnapCenter 4.2, si el recurso E90 MDC estaba ubicado en el host del complemento y se registró manualmente, después de actualizar a SnapCenter 4.3, se descubrirá y registrará otro recurso E90 MDC con un GUID diferente en SnapCenter.

El descubrimiento automático no es compatible con las siguientes configuraciones:

- Diseños RDM y VMDK



En caso de que se descubran los recursos mencionados anteriormente, las operaciones de protección de datos no se respaldarán en estos recursos.

- Configuración de múltiples hosts de HANA
- Varias instancias en el mismo host
- Replicación del sistema HANA de escalamiento horizontal de múltiples niveles
- Entorno de replicación en cascada en modo de replicación del sistema

Tipo de backups admitido

El tipo de copia de seguridad especifica el tipo de copia de seguridad que desea crear. SnapCenter admite los tipos de copia de seguridad basada en archivos y copias de seguridad basadas en instantáneas para bases de datos de SAP HANA.

Copia de seguridad basada en archivos

Las copias de seguridad basadas en archivos verifican la integridad de la base de datos. Puede programar la operación de copia de seguridad basada en archivos para que se realice en intervalos específicos. Sólo se realizan copias de seguridad de los inquilinos activos. No es posible restaurar ni clonar copias de seguridad basadas en archivos desde SnapCenter.

Copia de seguridad basada en instantáneas

Las copias de seguridad basadas en instantáneas aprovechan la tecnología Snapshot de NetApp para crear copias en línea, de solo lectura, de los volúmenes en los que residen las bases de datos de SAP HANA.

Cómo el complemento SnapCenter para la base de datos SAP HANA utiliza instantáneas del grupo de consistencia

Puede utilizar el complemento para crear instantáneas de grupos de consistencia para grupos de recursos. Un grupo de consistencia es un contenedor que puede albergar múltiples volúmenes para que puedas administrarlos como una sola entidad. Un grupo de consistencia son instantáneas simultáneas de múltiples volúmenes, que proporcionan copias consistentes de un grupo de volúmenes.

También puede especificar el tiempo de espera para que el controlador de almacenamiento agrupe las instantáneas de manera consistente. Las opciones de tiempo de espera disponibles son **Urgente**, **Medio** y **Relajado**. También puede habilitar o deshabilitar la sincronización del diseño de archivo Write Anywhere (WAFL) durante la operación de instantánea de grupo consistente. La sincronización de WAFL mejora el rendimiento de una instantánea de grupo de consistencia.

Cómo gestiona SnapCenter el mantenimiento de las copias de seguridad de registros y datos

SnapCenter administra el mantenimiento de las copias de seguridad de registros y datos en los niveles del sistema de almacenamiento y del sistema de archivos, y dentro del catálogo de copias de seguridad de SAP HANA.

Las instantáneas del almacenamiento primario o secundario y sus entradas correspondientes en el catálogo de SAP HANA se eliminan según la configuración de retención. Las entradas del catálogo de SAP HANA también se eliminan durante la copia de seguridad y la eliminación del grupo de recursos.

Consideraciones para determinar los cronogramas de copias de seguridad para la base de datos de SAP HANA

El factor más crítico para determinar un cronograma de respaldo es la tasa de cambio del recurso. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su acuerdo de nivel de servicio (SLA) y su objetivo de punto de recuperación (RPO).

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de copia de seguridad (con qué frecuencia se deben realizar las copias de seguridad)

La frecuencia de copia de seguridad, también llamada tipo de programación para algunos complementos, es parte de una configuración de política. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual.

- Programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad)

Las programaciones de copias de seguridad son parte de la configuración de un recurso o de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m.

Número de trabajos de respaldo necesarios para las bases de datos de SAP HANA

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño del recurso, la cantidad de volúmenes utilizados, la tasa de cambio del recurso y su Acuerdo de Nivel de Servicio (SLA).

Convenciones de nomenclatura de copias de seguridad para bases de datos del complemento SAP HANA

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

`resourcegroupname_hostname_timestamp`

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dtst1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, `customtext_resourcegroup_policy_hostname` o `resourcegroup_hostname`. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Estrategia de restauración y recuperación para bases de datos de SAP HANA

Definir una estrategia de restauración y recuperación para los recursos de SAP HANA

Debe definir una estrategia antes de restaurar y recuperar su base de datos para poder realizar operaciones de restauración y recuperación con éxito.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos de SAP HANA agregados manualmente
2. Determinar las estrategias de restauración compatibles con las bases de datos SAP HANA detectadas automáticamente
3. Decide el tipo de operaciones de recuperación que deseas realizar.

Tipos de estrategias de restauración compatibles con recursos de SAP HANA agregados manualmente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter. Hay dos tipos de estrategias de restauración para recursos de SAP HANA agregados manualmente. No es posible recuperar recursos de SAP HANA agregados manualmente.



No es posible recuperar recursos de SAP HANA agregados manualmente.

Restauración completa de recursos

- Restaura todos los volúmenes, qtrees y LUN de un recurso



Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Restauración a nivel de archivo

- Restaura archivos de volúmenes, qtrees o directorios
- Restaura solo los LUN seleccionados

Tipos de estrategias de restauración compatibles con bases de datos SAP HANA detectadas automáticamente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter. Hay dos tipos de estrategias de restauración para las bases de datos de SAP HANA detectadas automáticamente.

Restauración completa de recursos

- Restaura todos los volúmenes, qtrees y LUN de un recurso
 - Se debe seleccionar la opción **Volume Revert** para restaurar el volumen completo.



Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Base de datos de inquilinos

- Restaura la base de datos de inquilinos

Si se selecciona la opción **Base de datos de inquilinos**, se deben usar HANA Studio o scripts de recuperación de HANA externos a SnapCenter para realizar la operación de recuperación.

Tipos de operaciones de restauración para bases de datos SAP HANA detectadas automáticamente

SnapCenter admite SnapRestore basado en volumen (VBSR), SnapRestore de archivo único y tipos de restauración de conexión y copia para bases de datos SAP HANA detectadas automáticamente.

SnapRestore basado en volumen (VBSR) se realiza en entornos NFS para los siguientes escenarios:

- Cuando la copia de seguridad seleccionada para restaurar se realiza en versiones anteriores a SnapCenter 4.3, y solo si está seleccionada la opción **Recurso completo**
- Cuando la copia de seguridad seleccionada para restaurar se toma en SnapCenter 4.3 y si la opción **Volume Revert** está seleccionada

SnapRestore de archivo único se realiza en entornos NFS para los siguientes escenarios:

- Cuando la copia de seguridad seleccionada para restaurar se toma en SnapCenter 4.3 y solo se selecciona la opción **Recurso completo**
- Para contenedores de bases de datos multiinquilino (MDC), cuando la copia de seguridad seleccionada para restaurar se toma en SnapCenter 4.3 y se selecciona la opción **Base de datos de inquilino**
- Cuando la copia de seguridad seleccionada es de una ubicación secundaria de SnapMirror o SnapVault y está seleccionada la opción **Recurso completo**

SnapRestore de archivo único se realiza en entornos SAN para los siguientes escenarios:

- Cuando se realizan copias de seguridad en versiones anteriores a SnapCenter 4.3, y solo si está seleccionada la opción **Recurso completo**

- Cuando se realizan copias de seguridad en SnapCenter 4.3, y solo si está seleccionada la opción **Recurso completo**
- Cuando se selecciona la copia de seguridad desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Recurso completo**

La restauración basada en conectar y copiar se realiza en entornos SAN para el siguiente escenario:

- Para MDC, cuando la copia de seguridad seleccionada para restaurar se toma en SnapCenter 4.3 y se selecciona la opción **Base de datos de inquilinos**



Las opciones **Recurso completo**, **Reversión de volumen** y **Base de datos de inquilinos** están disponibles en la página Restaurar alcance.

Tipos de operaciones de recuperación compatibles con las bases de datos de SAP HANA

SnapCenter le permite realizar diferentes tipos de operaciones de recuperación para bases de datos de SAP HANA.

- Recuperar la base de datos hasta el estado más reciente
- Recuperar la base de datos hasta un punto específico en el tiempo

Debe especificar la fecha y hora para la recuperación.

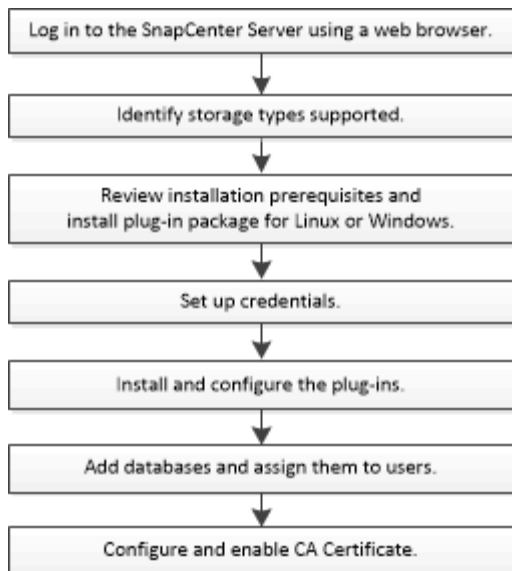
- Recuperar la base de datos hasta una copia de seguridad de datos específica

SnapCenter también ofrece la opción Sin recuperación para las bases de datos de SAP HANA.

Prepárese para instalar el complemento de SnapCenter para la base de datos SAP HANA

Flujo de trabajo de instalación del complemento de SnapCenter para la base de datos SAP HANA

Debe instalar y configurar el complemento de SnapCenter para la base de datos SAP HANA si desea proteger las bases de datos SAP HANA.



Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para la base de datos SAP HANA

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos. El complemento de SnapCenter para la base de datos SAP HANA está disponible en entornos Windows y Linux.

- Debes tener instalado Java 11 en tu host.



IBM Java no es compatible con hosts Windows y Linux.

- Debe tener instalado el terminal interactivo de base de datos SAP HANA (cliente HDBSQL) en el host.
- Para Windows, el servicio de creación de complementos debe ejecutarse utilizando el usuario de Windows “LocalSystem”, que es el comportamiento predeterminado cuando el complemento para la base de datos SAP HANA se instala como administrador de dominio.
- Para Windows, las claves del almacén de usuarios deben crearse como usuario del SISTEMA.
- Al instalar un complemento 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 complemento de SnapCenter para Microsoft Windows se implementará de forma predeterminada con el complemento SAP HANA en los hosts de Windows.
- En el caso del host Linux, se accede a las claves de HDB Secure User Store como usuario del sistema operativo HDBSQL.
- El servidor SnapCenter debe tener acceso al puerto 8145 o personalizado del complemento para el host de base de datos SAP HANA.

Hosts de Windows

- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Al instalar el complemento para la base de datos SAP HANA en un host Windows, el complemento de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.

- Debes tener instalado Java 11 en tu host Windows.

["Descargar JAVA para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Hosts Linux

- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Linux.

["Descargar JAVA para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Para las bases de datos SAP HANA que se ejecutan en un host Linux, al instalar el complemento para la base de datos SAP HANA, el complemento de SnapCenter para UNIX se instala automáticamente.
- Debe tener **bash** como el shell predeterminado para la instalación del complemento.

Comandos suplementarios

Para ejecutar un comando complementario en el complemento 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 complementarios en el host del complemento, abra el archivo *allowed_commands.config* en un editor. Ingrese cada comando en una línea separada y los comandos no distinguen entre mayúsculas y minúsculas. Asegúrese de especificar la ruta de acceso completa y de encerrarla entre comillas (") si contiene espacios.

Por ejemplo:

comando: montar

comando: desmontar

Comando: "C:\Archivos de programa\ NetApp\ SnapCreator commands\sdcli.exe"

comando: myscript.bat

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.



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

Configurar privilegios de sudo para usuarios no root para el host Linux

SnapCenter 2.0 y versiones posteriores permiten que un usuario no root instale el paquete de complementos de SnapCenter para Linux e inicie el proceso de complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el permiso 555. De lo contrario, la instalación del complemento podría fallar.
- Para el usuario no root, asegúrese de que el nombre del usuario no root y el grupo del usuario sean los mismos.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- `/inicio/USUARIO_LINUX/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl`

Pasos

1. Inicie sesión en el host Linux en el que desea instalar el paquete de complementos de SnapCenter para Linux.

2. Agregue las siguientes líneas al archivo `/etc/sudoers` utilizando la utilidad `visudo` para 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/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMDEXECUTOR, 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 RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux. .



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux

Antes de instalar el paquete de complementos de SnapCenter para Linux, debe familiarizarse con algunos requisitos básicos de tamaño y espacio del sistema host.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Servidor empresarial SUSE Linux (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .
RAM mínima para el complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 Oracle Java y OpenJDK Si ha actualizado JAVA a la última versión, 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 correcta. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Configurar credenciales para el complemento de SnapCenter para la base de datos SAP HANA

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en bases de datos o sistemas de archivos de Windows.

Acerca de esta tarea

- Hosts Linux

Debe configurar credenciales para instalar complementos en hosts Linux.

Debe configurar las credenciales para el usuario root o para un usuario no root que tenga privilegios de sudo para instalar e iniciar el proceso del complemento.

Mejor práctica: Si bien se le permite crear credenciales para Linux después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

- Hosts de Windows

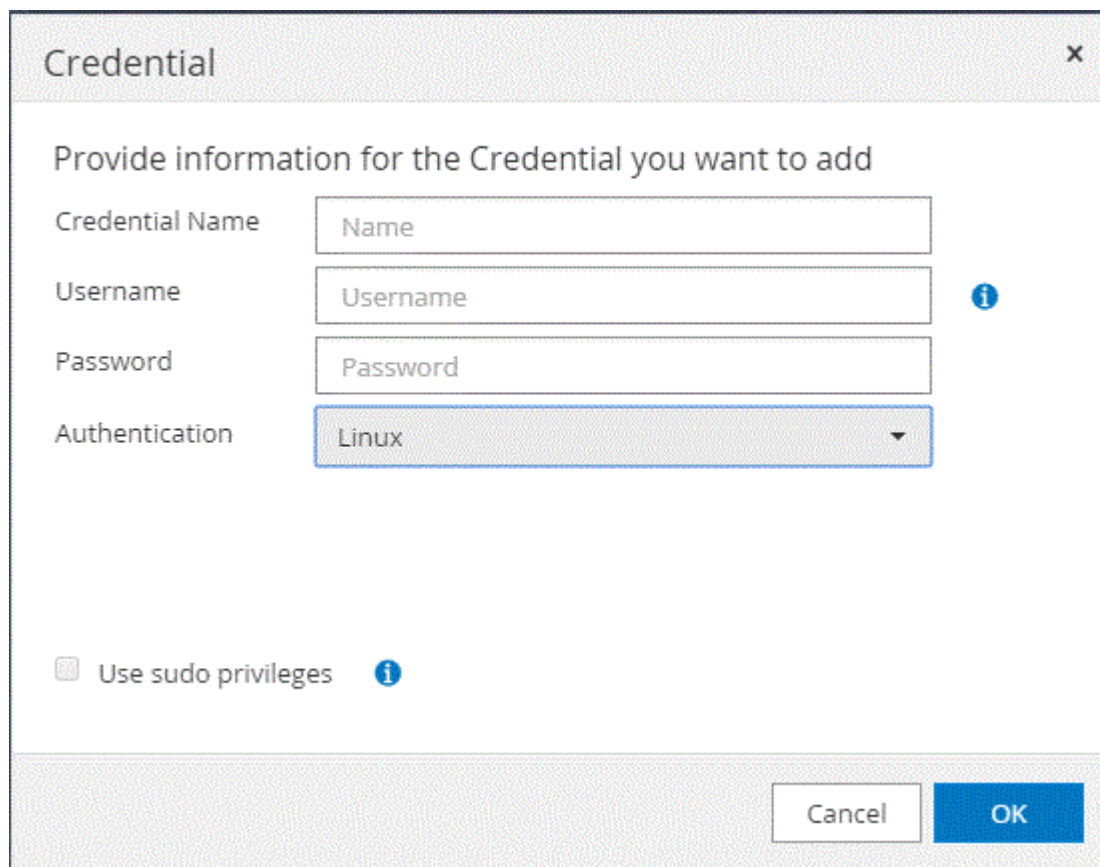
Debe configurar las credenciales de Windows antes de instalar complementos.

Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.

Si configura 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 de respaldo al nombre de usuario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.



Credential

Provide information for the Credential you want to add

Credential Name

Username 

Password

Authentication

☐ Use sudo privileges 

Cancel OK

4. En la página Credencial, especifique la información necesaria para configurar las credenciales:

Para este campo...	Haz esto...
Nombre de la 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 del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: <i>NetBIOS\Nombre de usuario</i> <i>Dominio FQDN\Nombre de usuario</i> - 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>NombreDeUsuario</i> No utilice comillas dobles (") ni tildes invertidas (') en las contraseñas. No debe utilizar los símbolos menor que (<) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que<!10, menos que10<!, acento grave`12.
Password	Introduzca la contraseña utilizada para la autenticación.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar.

Para este campo...	Haz esto...
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no sea root.  Aplicable únicamente a usuarios de Linux.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Configurar gMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$
.. Añade objetos de computadora 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,...>
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de servicio.
```

4. Configure el gMSA en sus hosts:

- a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
 - b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
 - c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Instalar el complemento de SnapCenter para bases de datos SAP HANA

Agregar hosts e instalar paquetes de complementos en hosts remotos

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar los paquetes de complementos. Los complementos se instalan automáticamente en los hosts remotos. Puede agregar un host e instalar paquetes de complementos 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 complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior

- Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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 esté ejecutándose.
- La documentación de administración contiene información sobre la gestión de hosts.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar la cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para SAP HANA"](#)

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .
- Para que la replicación del sistema SAP HANA descubra recursos en los sistemas primario y secundario, se recomienda agregar ambos sistemas mediante el usuario root o sudo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host: • Ventanas • Linux  El complemento para SAP HANA se instala en el host del cliente HDBSQL, y este host puede estar en un sistema Windows o en un sistema Linux.
Host name	Introduzca el nombre del host de comunicación. Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN. Debe configurar el cliente HDBSQL y HDBUserStore en este host.

Para este campo...	Haz esto...
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que proporcionó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección Seleccionar complementos para instalar, seleccione los complementos que desea instalar.
6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.
Ruta de instalación	El complemento para SAP HANA se instala en el host del cliente HDBSQL, y este host puede estar en un sistema Windows o en un sistema Linux. • Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\ NetApp\ SnapCenter. Opcionalmente, puedes personalizar la ruta. • Para el paquete de complementos de SnapCenter para Linux, la ruta predeterminada es /opt/ NetApp/snapcenter. Opcionalmente, puedes personalizar la ruta.

Para este campo...	Haz esto...
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Para el host de Windows, seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento.  Proporcione el nombre gMSA en el siguiente formato: domainName\accountName\$.  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla "Omitir comprobaciones previas", se valida el host para verificar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell, la versión de .NET, la ubicación (para complementos de Windows) y la versión de Java (para complementos de Linux) se validan según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Si el tipo de host es Linux, verifique la huella digital y luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

Los archivos de registro específicos de la instalación se encuentran en /custom_location/snapcenter/logs.

Instalar paquetes de complementos de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de complementos de SnapCenter para Linux o Windows en varios hosts simultáneamente mediante el cmdlet de PowerShell Install-SmHostPackage.

Antes de empezar

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar el paquete de complemento.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet Open-SmConnection y luego ingrese sus credenciales.
3. Instale el complemento en varios hosts utilizando el cmdlet Install-SmHostPackage y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la "[Guía de referencia de cmdlets del software SnapCenter](#)".

Puede utilizar la opción -skipprecheck cuando haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.

4. Introduzca sus credenciales para la instalación remota.

Instale el complemento de SnapCenter para la base de datos SAP HANA en hosts Linux mediante la interfaz de línea de comandos

Debe instalar el complemento de SnapCenter para la base de datos SAP HANA mediante la interfaz de usuario (UI) de SnapCenter . Si su entorno no permite la instalación remota del complemento desde la interfaz de usuario de SnapCenter , puede instalar el complemento para la base de datos SAP HANA en modo de consola o en modo silencioso mediante la interfaz de línea de comandos (CLI).

Antes de empezar

- Debe instalar el complemento para la base de datos SAP HANA en cada uno de los hosts Linux donde reside el cliente HDBSQL.
- El host Linux en el que está instalando el complemento de SnapCenter para la base de datos SAP HANA debe cumplir con los requisitos de software, base de datos y sistema operativo dependientes.

La herramienta Matriz de Interoperabilidad (IMT) contiene la información más reciente sobre las configuraciones admitidas.

<https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT>

- El complemento de SnapCenter para la base de datos SAP HANA es parte del paquete de complementos de SnapCenter para Linux. Antes de instalar el paquete de complementos de SnapCenter para Linux, ya debe haber instalado SnapCenter en un host Windows.

Pasos

1. Copie el archivo de instalación del paquete de complementos de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\ SnapCenter\Package Repository al host donde desea instalar el complemento para la base de datos SAP HANA.

Puede acceder a esta ruta desde el host donde está instalado SnapCenter Server.

2. Desde el símbolo del sistema, navegue hasta el directorio donde copió el archivo de instalación.

3. Instalar el complemento:

```
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 especifica el puerto de comunicación HTTPS de SMCore.
- -DSERVER_IP especifica la dirección IP del servidor SnapCenter .
- -DSERVER_HTTPS_PORT especifica el puerto HTTPS del servidor SnapCenter .
- -DUSER_INSTALL_DIR especifica el directorio donde desea instalar el paquete de complementos de SnapCenter para Linux.
- DINSTALL_LOG_NAME especifica 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 /<directorio de instalación>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y luego agregue el parámetro PLUGINS_ENABLED = hana:3.0.
5. Agregue el host al servidor SnapCenter mediante el cmdlet Add-Smhost y los parámetros necesarios.

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 cmdlets del software SnapCenter"](#) .

Supervisar el estado de instalación del complemento para SAP HANA

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-



Completado con advertencias o no se pudo iniciar debido a advertencias

- En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Huella digital**.
 - d. Copia los caracteres hexadecimales del cuadro.
 - e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:

- a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado recientemente instalado por el nombre del sujeto.

```
Get-ChildItem -Path Certificado:\LocalMachine\My
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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 para el servicio de complementos 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 por 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. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave
privada en el almacén de claves a la misma contraseña utilizada para el
almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar 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 agregar 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 /opt/NetApp/snapcenter/scc/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 de alias en el certificado de CA es largo y contiene
espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a
un nombre simple:
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configure el nombre de 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 en el archivo agent.properties contra la clave CRL_PATH.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Configurar el certificado de CA para el servicio de complementos SAP HANA de SnapCenter 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 por 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 correspondiente a la clave *KEYSTORE_PASS*.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool con su ruta completa.

```
C:\Archivos de programa\Java\<versión_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves:

```
keytool -keypasswd -alias "nombre_alias_en_certificado" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe agregar 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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo *keystore.jks*.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 "nombre_de_alias_en_certificado_de_CA" -keystore keystore.jks
```

8. Configure el nombre de 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 para el certificado CA relacionado, consulte ["Cómo actualizar el archivo de lista de revocación de certificados en SnapCenter CA Certificate"](#).
- 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 en el archivo *agent.properties* contra la clave CRL_PATH.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede

obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Instalar el SnapCenter Plug-in for VMware vSphere

Si su base de datos o sistema de archivos está almacenado en máquinas virtuales (VM), o si desea proteger las VM y los almacenes de datos, debe implementar el SnapCenter Plug-in for VMware vSphere .

Para obtener información sobre la implementación, consulte ["Descripción general de la implementación"](#) .

Implementar certificado de CA

Para configurar el certificado CA con el SnapCenter Plug-in for VMware vSphere, consulte ["Crear o importar certificado SSL"](#) .

Configurar el archivo CRL

El SnapCenter Plug-in for VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL para el SnapCenter Plug-in for VMware vSphere es */opt/netapp/config/crl*.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Prepárese para la protección de datos

Requisitos previos para utilizar el complemento de SnapCenter para la base de datos SAP HANA

Antes de utilizar el complemento de SnapCenter para la base de datos SAP HANA, el administrador de SnapCenter debe instalar y configurar el servidor de SnapCenter y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter Server.
- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento y creando credenciales, si corresponde.
- Instale Java 11 en su host Linux o Windows.

Debe configurar la ruta de Java en la variable de ruta ambiental de la máquina host.

- Configure SnapMirror y SnapVault si desea replicación de respaldo.
- Instale el cliente HDBSQL en el host donde instalará el complemento para la base de datos SAP HANA.

Configure las claves de almacenamiento de usuarios para los nodos de SAP HANA que administrará a través de este host.

- Para la base de datos SAP HANA 2.0SPS05, si utiliza una cuenta de usuario de base de datos SAP HANA, asegúrese de tener los siguientes permisos para realizar operaciones de copia de seguridad, restauración y clonación en SnapCenter Server:
 - Administrador de respaldo
 - Catálogo leído
 - Administrador de copias de seguridad de bases de datos
 - Operador de recuperación de base de datos

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger las bases de datos de SAP HANA

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de copia de seguridad, clonación y restauración que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser bases de datos de SAP HANA que usted respalda o clona con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

- Las políticas especifican la frecuencia de las copias de seguridad, la replicación, los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede

seleccionar una política cuando realiza una copia de seguridad a pedido para un solo recurso.

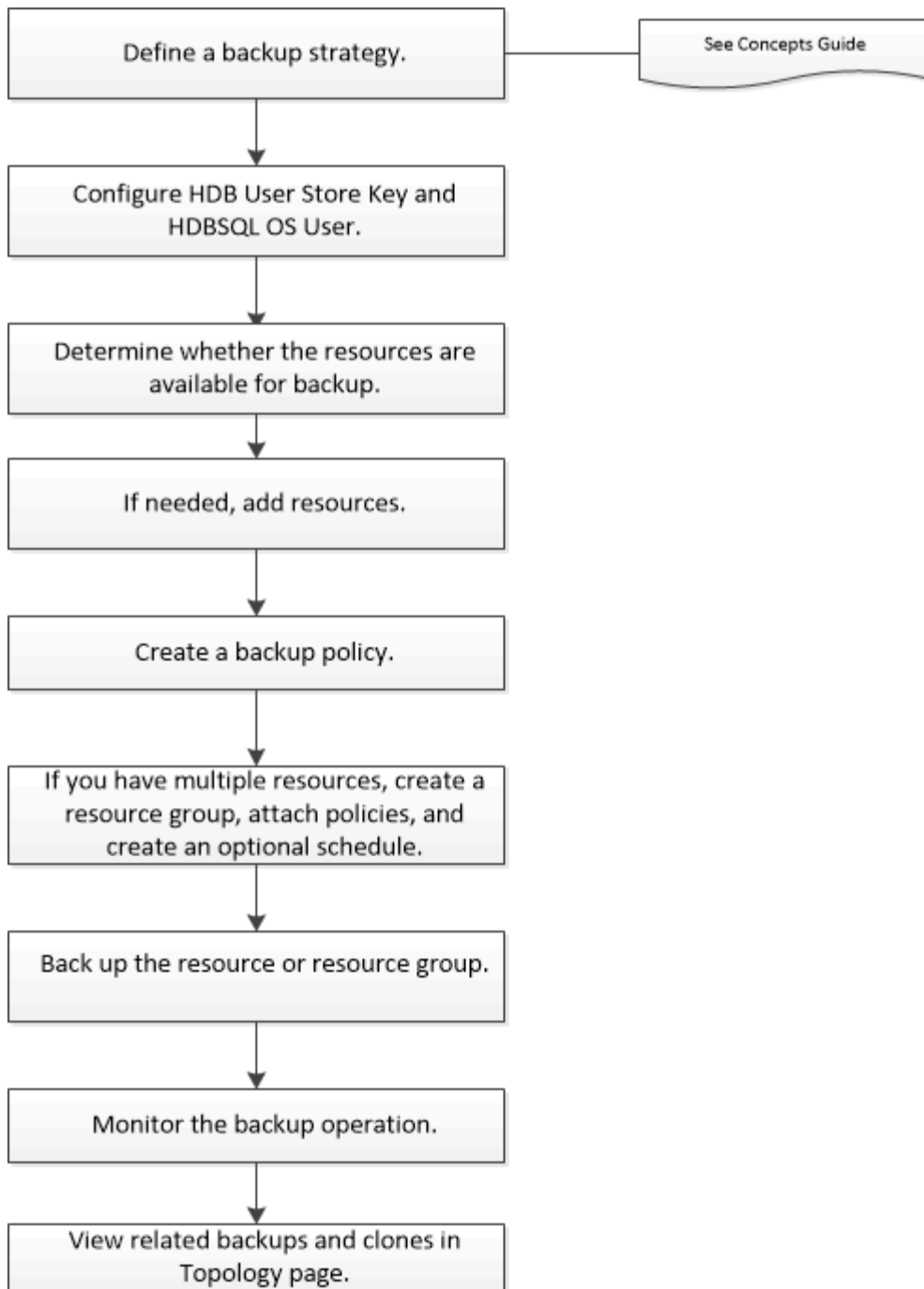
Piense en un grupo de recursos como si definiera lo que desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera cómo desea protegerla. Si está realizando una copia de seguridad de todas las bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos del host. Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Al crear el grupo de recursos y adjuntar las políticas, puede configurar el grupo de recursos para que realice una copia de seguridad completa diariamente.

Realizar copias de seguridad de los recursos de SAP HANA

Realizar copias de seguridad de los recursos de SAP HANA

Puede crear una copia de seguridad de un recurso (base de datos) o de un grupo de recursos. El flujo de trabajo de respaldo incluye la planificación, la identificación de las bases de datos para el respaldo, la administración de políticas de respaldo, la creación de grupos de recursos y la asociación de políticas, la creación de respaldos y el monitoreo de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen más información sobre los cmdlets de PowerShell. ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Configurar la clave de almacenamiento de usuarios de HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA

Debe configurar la clave de almacén de usuarios HDB y el usuario del sistema operativo HDBSQL para realizar operaciones de protección de datos en las bases de datos de SAP HANA.

Antes de empezar

- Si la base de datos SAP HANA no tiene configuradas la clave de almacenamiento de usuario seguro HDB y el usuario del sistema operativo SQL HDB, aparece un ícono de candado rojo solo para los recursos descubiertos automáticamente. Si durante una operación de descubrimiento posterior, se descubre que la clave de almacenamiento de usuario seguro de HDB configurada es incorrecta o no proporciona acceso a la base de datos en sí, entonces volverá a aparecer el ícono del candado rojo.
- Debe configurar la clave de almacén de usuario seguro de HDB y el usuario del sistema operativo SQL de HDB para poder proteger la base de datos o agregarla a un grupo de recursos para realizar operaciones de protección de datos.
- Debe configurar el usuario del sistema operativo HDB SQL para acceder a la base de datos del sistema. Si el usuario del sistema operativo SQL de HDB está configurado para acceder solo a la base de datos del inquilino, la operación de descubrimiento fallará.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione Complemento de SnapCenter para base de datos SAP HANA de la lista.
2. En la página Recursos, seleccione el tipo de recurso de la lista **Ver**.
3. (Opcional) Haga clic en  y seleccione el nombre del host.

Luego puedes hacer clic  para cerrar el panel de filtro.

4. Seleccione la base de datos y luego haga clic en **Configurar base de datos**.
5. En la sección Configurar ajustes de la base de datos, ingrese la clave de almacenamiento de usuario seguro de HDB.



Se muestra el nombre de host del complemento y el usuario del sistema operativo HDB SQL se completa automáticamente como <sid>adm.

6. Haga clic en **Aceptar**.

Puede modificar la configuración de la base de datos desde la página Topología.

Descubra recursos y prepare contenedores de bases de datos multiinquilino para la protección de datos

Descubra las bases de datos automáticamente

Los recursos son bases de datos de SAP HANA y volúmenes que no son de datos en el host Linux que administra SnapCenter. Puede agregar estos recursos a grupos de recursos para realizar operaciones de protección de datos después de descubrir las bases de datos de SAP HANA que están disponibles.

Antes de empezar

- Ya debe haber completado tareas como instalar el servidor SnapCenter , agregar la clave de almacenamiento de usuario HDB, agregar hosts y configurar las conexiones del sistema de almacenamiento.
- Debe haber configurado la clave de almacenamiento de usuario seguro de HDB y el usuario del sistema operativo SQL de HDB en el host Linux.
 - Debe configurar la clave de almacenamiento de usuarios 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 complemento de SnapCenter para la base de datos SAP HANA no admite el descubrimiento automático de los recursos que residen en entornos virtuales RDM/VMDK. Debe proporcionar la información de almacenamiento para los entornos virtuales al agregar las bases de datos manualmente.

Acerca de esta tarea

Después de instalar el complemento, todos los recursos de ese host Linux se descubren automáticamente y se muestran en la página Recursos.

Los recursos descubiertos automáticamente no se pueden modificar ni eliminar.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento para la base de datos SAP HANA de la lista.
2. En la página Recursos, seleccione el tipo de recurso de la lista Ver.
3. (Opcional) Haga clic en  * y luego seleccione el nombre del host.

Luego puedes hacer clic en  * para cerrar el panel de filtro.

4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

Los recursos se muestran junto con información como el tipo de recurso, el nombre del host, los grupos de recursos asociados, el tipo de copia de seguridad, las políticas y el estado general.

- Si la base de datos está en un almacenamiento NetApp y no está protegida, se muestra No protegido en la columna Estado general.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, y no se realiza ninguna operación de respaldo, se muestra Copia de seguridad no ejecutada en la columna Estado general. De lo contrario, el estado cambiará a Copia de seguridad fallida o Copia de seguridad exitosa según el último estado de la copia de seguridad.



Si la base de datos SAP HANA no tiene una clave de almacenamiento de usuario seguro HDB configurada, aparece un ícono de candado rojo junto al recurso. Si durante una operación de descubrimiento posterior, se descubre que la clave de almacenamiento de usuario seguro de HDB configurada es incorrecta o no proporciona acceso a la base de datos en sí, entonces volverá a aparecer el ícono del candado rojo.



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

Después de terminar

Debe configurar la clave de almacenamiento de usuario seguro de HDB y el usuario del sistema operativo HDBSQL para poder proteger la base de datos o agregarla al grupo de recursos para realizar operaciones de protección de datos.

["Configurar la clave de almacenamiento de usuarios de HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA"](#)

Preparar contenedores de bases de datos multiinquilino para la protección de datos

Para los hosts de SAP HANA registrados directamente en SnapCenter, la instalación o

actualización del complemento de SnapCenter para la base de datos de SAP HANA activará un descubrimiento automático de recursos en el host. Después de instalar o actualizar el complemento, por cada recurso de contenedor de base de datos multiinquilino (MDC) que estaba ubicado en el host del complemento, se descubrirá automáticamente otro recurso MDC con un formato GUID diferente y se registrará en SnapCenter. El nuevo recurso estará en estado "bloqueado".

Acerca de esta tarea

Por ejemplo, en SnapCenter 4.2, si el recurso E90 MDC estaba ubicado en el host del complemento y se registró manualmente, después de actualizar a SnapCenter 4.3, se descubrirá y registrará otro recurso E90 MDC con un GUID diferente en SnapCenter.



Las copias de seguridad asociadas con el recurso de SnapCenter 4.2 y versiones anteriores deben conservarse hasta que expire el período de retención. Una vez que expire el período de retención, puede eliminar el antiguo recurso MDC y continuar administrando el nuevo recurso MDC descubierto automáticamente.

El recurso "Old MDC resource" es el recurso MDC para un host de complemento que se agregó manualmente en SnapCenter 4.2 o versiones anteriores.

Realice los siguientes pasos para comenzar a utilizar el nuevo recurso descubierto en SnapCenter 4.3 para operaciones de protección de datos:

Pasos

1. En la página Recursos, seleccione el antiguo recurso MDC con copias de seguridad agregadas a la versión anterior de SnapCenter y colóquelo en "modo de mantenimiento" desde la página Topología.

Si el recurso es parte de un grupo de recursos, coloque el grupo de recursos en "modo de mantenimiento".

2. Configure el nuevo recurso MDC descubierto después de actualizar a SnapCenter 4.3 seleccionando el nuevo recurso en la página Recursos.

"Nuevo recurso MDC" es el recurso MDC recientemente descubierto una vez que el servidor SnapCenter y el host del complemento se actualizaron a 4.3. El nuevo recurso MDC se puede identificar como un recurso con el mismo SID que el recurso MDC antiguo, para un host determinado, y con un ícono de candado rojo junto a él en la página Recursos.

3. Proteja el nuevo recurso MDC descubierto después de actualizar a SnapCenter 4.3 seleccionando políticas de protección, programaciones y configuraciones de notificación.
4. Elimine las copias de seguridad realizadas en SnapCenter 4.2 o versiones anteriores según la configuración de retención.
5. Eliminar el grupo de recursos de la página Topología.
6. Eliminar el antiguo recurso MDC de la página Recursos.

Por ejemplo, si el período de retención de instantáneas principales es de 7 días y el de las instantáneas secundarias es de 45 días, una vez transcurridos 45 días y una vez eliminadas todas las copias de seguridad, deberá eliminar el grupo de recursos y el antiguo recurso MDC.

Información relacionada

["Configurar la clave de almacenamiento de usuarios de HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA"](#)

Agregar recursos manualmente al host del complemento

El descubrimiento automático no es compatible con ciertas instancias de HANA. Debes agregar estos recursos manualmente.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts, configurar conexiones del sistema de almacenamiento y agregar la clave de almacenamiento de usuario de HDB.
- Para la replicación del sistema SAP HANA, se recomienda agregar todos los recursos de ese sistema HANA en un grupo de recursos y realizar una copia de seguridad del grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación y toma de control.

["Crear grupos de recursos y adjuntar políticas"](#) .

Acerca de esta tarea

El descubrimiento automático no es compatible con las siguientes configuraciones:

- Diseños RDM y VMDK



En caso de que se descubran los recursos mencionados anteriormente, las operaciones de protección de datos no se respaldarán en estos recursos.

- Configuración de múltiples hosts de HANA
- Varias instancias en el mismo host
- Replicación del sistema HANA de escalamiento horizontal de múltiples niveles
- Entorno de replicación en cascada en modo de replicación del sistema

Pasos

1. En el panel de navegación izquierdo, seleccione el complemento SnapCenter para la base de datos SAP HANA de la lista desplegable y luego haga clic en **Recursos**.
2. En la página Recursos, haga clic en **Agregar base de datos SAP HANA**.
3. En la página Proporcionar detalles de recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de recurso	Introduzca el tipo de recurso. Los tipos de recursos son contenedor único, contenedor de base de datos multiinquilino (MDC) y volumen sin datos.
Nombre del sistema HANA	Introduzca el nombre descriptivo del sistema SAP HANA. Esta opción solo está disponible si seleccionó los tipos de recursos Contenedor único o MDC.

Para este campo...	Haz esto...
SID	Introduzca el ID del sistema (SID). El sistema SAP HANA instalado se identifica mediante un único SID.
Host de complementos	Seleccione el host del complemento.
Claves de almacenamiento seguro de usuarios de 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 del sistema SAP HANA, la clave de usuario secundaria no está validada. Esto se utilizará durante la adquisición.
Usuario del sistema operativo HDBSQL	Introduzca el nombre de usuario para el cual está configurada la clave de almacenamiento de usuario seguro de HDB. Para Windows, es obligatorio que el usuario del sistema operativo HDBSQL sea el usuario del SISTEMA. Por lo tanto, debe configurar la clave de almacenamiento de usuario seguro HDB para el usuario del SISTEMA.

4. En la página Proporcionar espacio de almacenamiento, seleccione un sistema de almacenamiento y elija uno o más volúmenes, LUN y qtrees, y luego haga clic en **Guardar**.

Opcional: Puede hacer clic en el *  * Icono para agregar más volúmenes, LUN y qtrees de otros sistemas de almacenamiento.

5. Revise el resumen y luego haga clic en **Finalizar**.

Las bases de datos se muestran junto con información como el SID, el host del complemento, los grupos de recursos y políticas asociados, y el estado general.

Si desea proporcionar a los usuarios acceso a los recursos, debe asignar los recursos a los usuarios. Esto permite a los usuarios realizar las acciones para las que tienen permiso en los activos que les están asignados.

"Agregar un usuario o grupo y asignarle roles y activos"

Después de agregar las bases de datos, puede modificar los detalles de la base de datos de SAP HANA.

No puede modificar lo siguiente si hay copias de seguridad asociadas con el recurso SAP HANA:

- Contenedores de bases de datos multiinquilino (MDC): SID o cliente HDBSQL (complemento) Host
- Contenedor único: SID o host de cliente HDBSQL (complemento)
- Volumen sin datos: nombre del recurso, SID asociado o host del complemento

Crear políticas de respaldo para bases de datos de SAP HANA

Antes de usar SnapCenter para realizar copias de seguridad de los recursos de base de datos de SAP HANA, debe crear una política de copia de seguridad para el recurso o grupo de recursos que desea respaldar. Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad.

Antes de empezar

- Debes haber definido tu estrategia de backup.

Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para bases de datos de SAP HANA.

- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, configurar conexiones del sistema de almacenamiento y agregar recursos.
- El administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino si está replicando instantáneas a un espejo o bóveda.

Además, puede especificar configuraciones de replicación, scripts y aplicaciones en la política. Estas opciones ahorran tiempo cuando desea reutilizar la política para otro grupo de recursos.

- Revise los requisitos previos y las limitaciones específicos de la sincronización activa de SnapMirror . Para obtener información, consulte ["Límites de objetos para la sincronización activa de SnapMirror"](#) .

Acerca de esta tarea

- Replicación del sistema SAP HANA
 - Puede proteger el sistema principal SAP HANA y se pueden realizar todas las operaciones de protección de datos.
 - Puede proteger el sistema SAP HANA secundario, pero no se pueden crear copias de seguridad.

Después de la conmutación por error, se puede realizar toda la operación de protección de datos ya que el sistema SAP HANA secundario se convierte en el sistema SAP HANA principal.

No es posible crear una copia de seguridad del volumen de datos de SAP HANA, pero SnapCenter continúa protegiendo los volúmenes que no son de datos (NDV).

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.
 - Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas que la cantidad especificada 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.
5. En la página Tipo de política, realice los siguientes pasos:
 - Elija el tipo de almacenamiento
 - Elija el tipo de copia de seguridad:

Si quieres...	Haz esto...
Crear una copia de seguridad utilizando la tecnología Snapshot	Seleccione Basado en instantánea .
Realizar una comprobación de integridad de la base de datos	Seleccione Copia de seguridad basada en archivos . Sólo se realizan copias de seguridad de los inquilinos activos.

6. En la página Instantánea y replicación, realice los siguientes pasos:
 - Especifique el tipo de programación seleccionando **A pedido**, **Por hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero también le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

7. En la página Instantánea y replicación, 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 quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad 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 las copias de seguridad basadas en copias instantáneas, debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva en el destino.  Para la replicación del sistema SAP HANA, se recomienda agregar todos los recursos del sistema SAP HANA en un grupo de recursos. Esto garantiza que se conserve la cantidad correcta de copias de seguridad.  Para la replicación del sistema SAP HANA, la cantidad total de instantáneas tomadas será igual a la retención establecida para el grupo de recursos. La eliminación de la instantánea más antigua se basa en el nodo en el que se encuentra la instantánea más antigua. Por ejemplo, la retención se establece en 7 para un grupo de recursos con replicación del sistema SAP HANA como principal y replicación del sistema SAP HANA como secundaria. Puede tomar un máximo de 7 instantáneas a la vez, incluidas la replicación principal del sistema SAP HANA y la replicación secundaria del sistema SAP HANA.

Si quieres...	Entonces...
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 instantánea.



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 las copias de seguridad basadas en copias instantáneas, en la sección Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Esta opción debe estar habilitada para la sincronización activa de SnapMirror . Si la relación de protección en ONTAP es de tipo Mirror and Vault y selecciona solo esta opción, el Snapshot creado en el servidor principal no se transferirá al destino, pero aparecerá en el destino. Si se selecciona esta instantánea desde el destino para realizar una operación de restauración, se muestra el mensaje de error La ubicación secundaria no está disponible para la copia de seguridad almacenada/duplicada seleccionada. Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Ver "Ver copias de seguridad y clones de bases de datos de SAP HANA en la página Topología" .
Actualizar SnapVault después de crear una copia de instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault). Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón Actualizar en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre SnapLock Vault, consulte "Confirmar copias de instantáneas en WORM en un destino de bóveda" Ver "Ver copias de seguridad y clones de bases de datos de SAP HANA en la página Topología" .

Para este campo...	Haz esto...
Recuento de reintentos por error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

10. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados a una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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 copias de seguridad de replicación del sistema SAP HANA, se recomienda agregar todos los recursos del sistema SAP HANA en un grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación y toma de control.
- 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 .
- No se admite agregar nuevas bases de datos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror .
- No se admite agregar nuevas bases de datos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror . Puede agregar recursos al grupo de recursos solo en estado normal o de conmutación por recuperación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.  El nombre del grupo de recursos no debe exceder los 250 caracteres.

Para este campo...	Haz esto...
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

Esto ayuda a filtrar la información en la pantalla.

- Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
- En la página Configuración de la aplicación, haga lo siguiente:

- Haga clic en la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación de instantánea del grupo de consistencia	Seleccione Urgente, Medio o Relajado para especificar el tiempo de espera para que se complete la operación de Instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

+

- Haga clic en la flecha **Scripts** e ingrese los comandos pre y post para las operaciones de inactividad, instantánea y desactivación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
- Haga clic en la flecha **Configuraciones personalizadas** e ingrese los pares clave-valor personalizados necesarios para todas las operaciones de protección de datos que utilicen este recurso.

Parámetro	Valor	Descripción
HABILITAR REGISTRO DE ARCHIVO	(T/N)	Permite que la gestión del registro de archivo elimine los registros de archivo.
RETENCIÓN DE REGISTRO DE ARCHIVO	número_de_días	Especifica el número de días que se conservan los registros de archivo. Esta configuración debe ser igual o mayor que NTAP_SNAPSHOT_RETENTIONS.
DIRECCIÓN DE REGISTRO DE ARCHIVO	directorio_de_información_de_cambio/registros	Especifica la ruta al directorio que contiene los registros de archivo.

Parámetro	Valor	Descripción
EXTRACCIÓN DEL REGISTRO DE ARCHIVO	extensión_de_archivo	Especifica la longitud de la extensión del archivo de registro de archivo. Por ejemplo, si el registro de archivo es log_backup_0_0_0_0.161518551942 9 y el valor de file_extension es 5, entonces la extensión del registro retendrá 5 dígitos, que es 16151.
ARCHIVO_REGISTRO_BÚSQUEDA_RECURSIVA ARCH	(T/N)	Permite la gestión de registros de archivo dentro de 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 complemento SAP HANA para Linux y no son compatibles con las bases de datos SAP HANA registradas como un complemento centralizado de Windows.

- c. Haga clic en la flecha **Herramienta de copia de instantáneas** para seleccionar la herramienta para crear instantáneas:

Si quieres...	Entonces...
SnapCenter para utilizar el complemento para Windows y poner el sistema de archivos en un estado consistente antes de crear una instantánea. Para los recursos de Linux, esta opción no es aplicable.	Seleccione * SnapCenter con consistencia del sistema de archivos*. Esta opción no es aplicable al complemento de SnapCenter para la base de datos SAP HANA.
SnapCenter para crear una instantánea de nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
Ingresa el comando que se ejecutará en el host para crear copias Snapshot.	Seleccione Otro y luego ingrese el comando que se ejecutará en el host para crear una instantánea.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

Las políticas se enumeran en la sección Configurar programaciones para políticas seleccionadas.

- b. En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna **Horarios aplicados**.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El servidor SMTP debe configurarse en **Configuración > Configuración global**.

9. Revise el resumen y luego haga clic en **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos de SAP HANA en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más

adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:
 - a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:
 - a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
 - b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
 - c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos de SAP HANA

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar copias de seguridad, restaurar o clonar bases de datos de SAP HANA.

Antes de empezar

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de datos única.

Pasos

1. Inicie una sesión de conexión de PowerShell mediante el cmdlet Open-SmConnection.

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

2. Cree una nueva conexión al 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 nueva credencial mediante el cmdlet Add-SmCredential.

Este ejemplo muestra cómo crear una nueva credencial llamada FinanceAdmin con credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. Agregue el host de comunicación SAP HANA al servidor SnapCenter .

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode hana
```

5. Instale el paquete y el complemento de SnapCenter para la 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. Establezca la ruta al cliente 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de las bases de datos de SAP HANA

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Antes de empezar

- Debes haber creado una política de respaldo.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el

privilegio "snapmirror all".

- Para la operación de copia de seguridad basada en instantáneas, asegúrese de que todas las bases de datos de los inquilinos sean válidas y activas.
- Para crear copias de seguridad de replicación del sistema SAP HANA, se recomienda agregar todos los recursos del sistema SAP HANA en un grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación y toma de control.

"Crear grupos de recursos y adjuntar políticas" .

"Realizar copias de seguridad de grupos de recursos"

- Si desea crear una copia de seguridad basada en archivos cuando una o más bases de datos de inquilinos están inactivas, configure el parámetro `ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT` en **YES** en el archivo de propiedades de HANA usando `Set-SmConfigSettings` cmdlet.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#)

- Para los comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Seleccionar ** y, a continuación, seleccione el nombre del host y el tipo de recurso para filtrar los recursos. Luego puedes seleccionar  para cerrar el panel de filtro.

3. Seleccione el recurso que desea respaldar.
4. En la página Recursos, seleccione **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Configuración de la aplicación, haga lo siguiente:
 - Seleccione la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia, si es necesario, y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación "Instantánea del grupo de consistencia"	Seleccione Urgente , Medio o Relajado para especificar el tiempo de espera para que finalice la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

- Seleccione la flecha **Scripts** para ejecutar comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo.

También puede ejecutar comandos previos antes de salir de la operación de copia de seguridad. Los prescriptos y posscripts se ejecutan en el servidor SnapCenter .

- Seleccione la flecha **Configuraciones personalizadas** y luego ingrese los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.
- Seleccione la flecha **Herramienta Copiar Instantánea** para seleccionar la herramienta para crear Instantáneas:

Si quieres...	Entonces...
SnapCenter para crear una instantánea a nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
SnapCenter para usar el complemento para Windows para poner el sistema de archivos en un estado consistente y luego crear una instantánea	Seleccione * SnapCenter con consistencia del sistema de archivos*.
Para ingresar el comando para crear una instantánea	Seleccione Otro y luego ingrese el comando para crear una instantánea.

6. En la página Políticas, realice los siguientes pasos:

- Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- Seleccionar *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.

policy_name es el nombre de la política que usted seleccionó.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en **Configuración > Configuración global**.

8. Revise el resumen y luego seleccione **Finalizar**.

Se muestra la página de topología de recursos.

9. Seleccione **Hacer copia de seguridad ahora**.

10. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

- En configuraciones de MetroCluster , es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

Para obtener información, consulte: ["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar.

Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese script, el comando `do_start method` inicia el servicio del complemento VMware de SnapCenter . Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

Se muestra la solicitud de nombre de usuario y contraseña.

2. Agregue recursos mediante el cmdlet `Add-SmResources`.

Este ejemplo muestra cómo agregar 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 agregar 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 volumen sin datos:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Cree una política de respaldo mediante el cmdlet Add-SmPolicy.

Este ejemplo crea una política de respaldo para una copia de seguridad basada en instantánea:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

Este ejemplo crea una política de respaldo para una copia de seguridad basada en archivos:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Proteja el recurso o agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

Este ejemplo protege un único recurso contenedor:

```
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 múltiples contenedores:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

Este ejemplo 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.sscore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sscore.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.sscore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

Este ejemplo muestra cómo realizar una copia de seguridad de un grupo de recursos:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

Este ejemplo realiza una copia de seguridad 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 del trabajo (en ejecución, completado o fallido) mediante el cmdlet `Get-smJobSummaryReport`.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Supervise los detalles del trabajo de respaldo, como la identificación y el nombre del respaldo, para realizar una operación de restauración o clonación 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de grupos de recursos

Un grupo de recursos es una colección de recursos en un host. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.

Acerca de esta tarea

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o seleccionando  , y luego seleccionando la etiqueta. Luego puedes seleccionar  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.

4. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 las bases de datos de SAP HANA

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en las bases de datos de SAP HANA en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 operaciones de copia de seguridad para SAP HANA

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter, los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de copia de seguridad.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	a. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. b. Seleccione la operación y luego haga clic en Cancelar trabajo.
Panel de actividades	a. Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Ver copias de seguridad y clones de bases de datos de SAP HANA en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario.

Acerca de esta tarea

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y

los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .



La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), puede ver los siguientes íconos adicionales:

-  El sitio de réplica está activo.
-  El sitio de réplica está inactivo.
-  No se ha restablecido la relación de espejo secundario o bóveda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página de topología del recurso seleccionado.

4. Revise la **tarjeta de resumen** para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario y secundario.

La sección **Tarjeta de resumen** muestra el número total de copias de seguridad basadas en archivos, copias de seguridad basadas en instantáneas 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración 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 respaldo de SnapCenter consultando a ONTAP los sitios principales y de réplica. Una programación semanal también realiza esta actividad para 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 Async Mirror o Async MirrorVault con el nuevo destino principal se deben configurar manualmente después de la conmutación por error. Desde ONTAP 9.15.1 en adelante, Async Mirror o Async MirrorVault se configura automáticamente en el nuevo destino principal.
- Después de la conmutación por error, se debe crear una copia de seguridad para que SnapCenter esté al tanto de la conmutación por error. Puede hacer clic en **Actualizar** sólo después de haber creado una copia de seguridad.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

7. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en

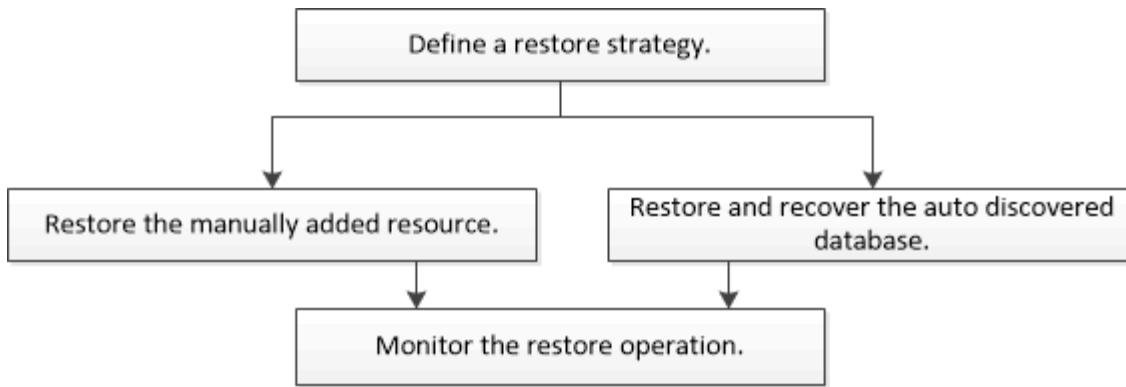
8. Si desea dividir un clon, seleccione el clon de la tabla y luego haga clic en

Restaurar bases de datos de SAP HANA

Restaurar flujo de trabajo

El flujo de trabajo de restauración y recuperación incluye la planificación, la ejecución de las operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de restauración:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

["Guía de referencia de cmdlets del software SnapCenter"](#) .

Restaurar y recuperar una copia de seguridad de un recurso agregado manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Las copias de seguridad basadas en archivos no se pueden restaurar desde SnapCenter.
- Después de actualizar a SnapCenter 4.3, las copias de seguridad realizadas en SnapCenter 4.2 se pueden restaurar, pero no se pueden recuperar. Debe utilizar HANA Studio o scripts de recuperación de HANA externos a SnapCenter para recuperar las copias de seguridad realizadas en SnapCenter 4.2.
- 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 .
- Para la operación de restauración de sincronización activa de SnapMirror , debe seleccionar la copia de seguridad de la ubicación principal.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



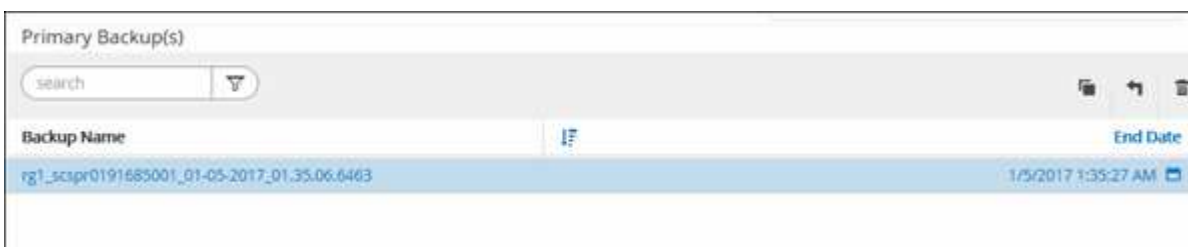
Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.



Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01:35:06.6463	1/5/2017 1:35:27 AM

6. En la página Restaurar alcance, seleccione **Recurso completo** o **Nivel de archivo**.
 - a. Si selecciona **Recurso completo**, se restauran todos los volúmenes de datos configurados de la base de datos de SAP HANA.

Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

- b. Si selecciona **Nivel de archivo**, puede seleccionar **Todos** o seleccionar los volúmenes o qtrees específicos y luego ingresar 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 el LUN completo.

Puede seleccionar varios LUN.



Si selecciona **Todos**, se restaurarán todos los archivos en los volúmenes, qtrees o LUN.

7. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no están disponibles para los recursos descubiertos automáticamente.

8. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no están disponibles para los recursos descubiertos automáticamente.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets Get-SmBackup y Get-SmBackupReport.

Este ejemplo muestra información sobre todas las copias de seguridad 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	

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet `Restore-SmBackup`.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar y recuperar una copia de seguridad de una base de datos descubierta automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los

comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:

- 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Las copias de seguridad basadas en archivos no se pueden restaurar desde SnapCenter.
- Después de actualizar a SnapCenter 4.3, las copias de seguridad realizadas en SnapCenter 4.2 se pueden restaurar, pero no se pueden recuperar. Debe utilizar HANA Studio o scripts de recuperación de HANA externos a SnapCenter para recuperar las copias de seguridad realizadas en SnapCenter 4.2.
- 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 .
- Para la operación de restauración de sincronización activa de SnapMirror , debe seleccionar la copia de seguridad de la ubicación principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scspr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. En la página Restaurar alcance, seleccione **Recurso completo** para restaurar los volúmenes de datos configurados de la base de datos de SAP HANA.



Puede seleccionar **Recurso completo** (con o sin **Reversión de volumen**) o **Base de datos de inquilinos**.

SnapCenter Server no admite la operación de recuperación para varios inquilinos cuando el usuario selecciona la opción **Base de datos de inquilinos** o **Restauración completa**. Debe utilizar HANA Studio o el script de Python de HANA para realizar la operación de recuperación.

- a. Seleccione **Volumen Revertir** si desea restaurar el volumen completo.

Esta opción está disponible para las copias de seguridad realizadas en SnapCenter 4.3 en entornos NFS.

Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina. Esto se aplica cuando se selecciona la opción **Recurso completo** con **Revertir volumen** para restaurar.

- b. Seleccione **Base de datos de inquilinos**.

Esta opción solo está disponible para los recursos de MDC.

Asegúrese de detener la base de datos del inquilino antes de realizar la operación de restauración.

Si selecciona la opción **Base de datos de inquilinos**, debe utilizar HANA Studio o usar scripts de recuperación de HANA externos a SnapCenter para realizar la operación de recuperación.

7. En la página Ámbito de recuperación, seleccione una de las siguientes opciones:

Si usted...	Haz esto...
Quiere recuperarse lo más cerca posible de la hora actual	Seleccione Recuperar al estado más reciente. Para recursos de contenedor único, especifique una o más ubicaciones de respaldo de registros y catálogos. Para los recursos de contenedor de base de datos multiinquilino (MDC), especifique una o más ubicaciones de respaldo de registros y la ubicación del catálogo de respaldo. Para los recursos de MDC, la ruta debe contener los registros de la base de datos del sistema y de la base de datos del inquilino.

Si usted...	Haz esto...
¿Quieres recuperar el punto especificado en el tiempo?	Seleccione Recuperar a punto en el tiempo. a. Seleccione la zona horaria. La zona horaria del navegador se completa de forma predeterminada. La zona horaria seleccionada junto con la hora de entrada se convierte a GMT absoluto. b. Introduzca fecha y hora. Por ejemplo, el host HANA Linux está ubicado 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 desde Raleigh, Carolina del Norte, la zona horaria predeterminada del navegador que se seleccionará en la GUI es GMT-04:00. Si el usuario desea realizar una recuperación a las 5 a. m. de Sunnyvale, CA, entonces el usuario debe configurar la zona horaria del navegador a la zona horaria del host HANA Linux, que es GMT-07:00 y especificar la fecha y hora como 5:00 a. m. Para recursos de contenedor único, especifique una o más ubicaciones de respaldo de registros y catálogos. Para los recursos de MDC, especifique una o más ubicaciones de respaldo de registros y la ubicación del catálogo de respaldo. Para los recursos de MDC, la ruta debe contener los registros de la base de datos del sistema y de la base de datos del inquilino.
¿Quieres recuperar una copia de seguridad de datos específica?	Seleccione Recuperar a la copia de seguridad de datos especificada.
No quiero recuperarme	Seleccione Sin recuperación. Debe realizar la operación de recuperación manualmente desde el estudio HANA.

Solo puede recuperar aquellas copias de seguridad que se realicen después de actualizar a SnapCenter 4.3, siempre que tanto el host como el complemento se actualicen a SnapCenter 4.3 y las copias de seguridad seleccionadas para restaurar se realicen después de que el recurso se convierta o se descubra como recurso descubierto automáticamente.

- En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no están disponibles para los recursos descubiertos automáticamente.

- En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no están disponibles para los recursos descubiertos automáticamente.

- En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

- Revise el resumen y luego haga clic en **Finalizar**.
- Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Restaurar recursos mediante cmdlets de PowerShell

Restaurar una copia de seguridad de un recurso incluye iniciar una sesión de conexión con el servidor SnapCenter , enumerar las copias de seguridad y recuperar información de las copias de seguridad, y restaurar una copia de seguridad.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

- Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

- Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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

Este ejemplo muestra información detallada sobre la copia de seguridad 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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar las operaciones de restauración de bases de datos de SAP HANA

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso

-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Clonar copias de seguridad de recursos de SAP HANA

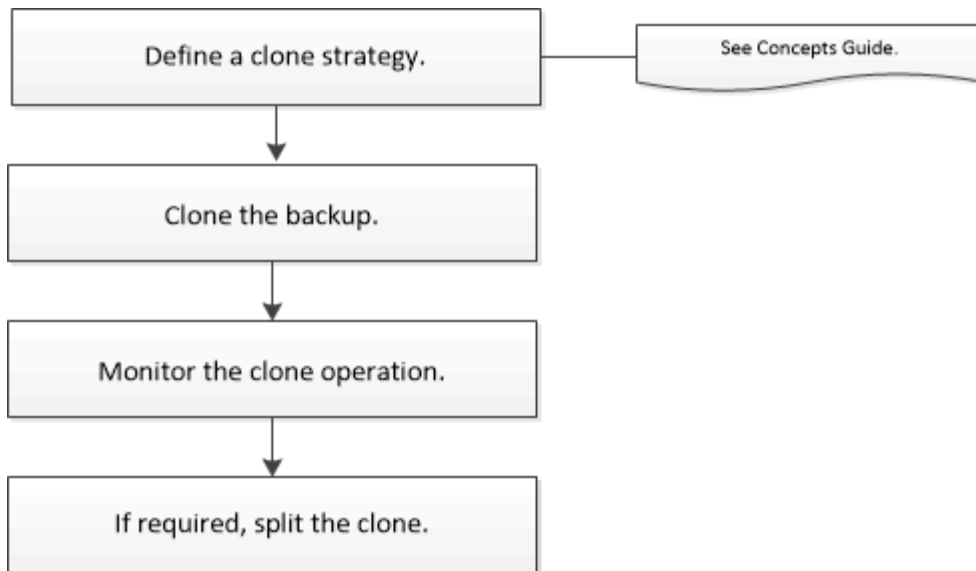
Flujo de trabajo de clonación

El flujo de trabajo de clonación incluye la realización de la operación de clonación y la supervisión de la operación.

Acerca de esta tarea

- Puede clonar en el servidor SAP HANA de origen.
- Puede clonar copias de seguridad de recursos por los siguientes motivos:
 - Para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de recursos actuales durante los ciclos de desarrollo de aplicaciones
 - Para herramientas de extracción y manipulación de datos al rellenar almacenes de datos
 - Para recuperar datos que fueron borrados o modificados por error

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de clonación:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

Clonar una copia de seguridad de la base de datos de SAP HANA

Puede utilizar SnapCenter para clonar una copia de seguridad. Puede clonar desde una copia de seguridad primaria o secundaria.

Antes de empezar

- Deberías haber realizado una copia de seguridad de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados que alojan los volúmenes estén en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- No se pueden clonar copias de seguridad basadas en archivos.
- El servidor clon de destino debe tener el mismo SID de instancia de SAP HANA que se proporciona en el campo SID del clon de destino.
- Para los comandos previos o posteriores a la clonación, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Para obtener información sobre las limitaciones de la operación de división de clones, consulte "[Guía de administración de almacenamiento lógico de ONTAP 9](#)".
- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con información como el tipo, el host, los grupos de recursos y políticas asociados y el estado.

3. Seleccione el recurso o grupo de recursos.

Debe seleccionar un recurso si selecciona un grupo de recursos.

Se muestra la página de topología de recursos o grupos de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. Seleccione la copia de seguridad de datos de la tabla y luego haga clic en  .
6. En la página Ubicación, realice las siguientes acciones:

Para este campo...	Haz esto...
Host de complementos	Seleccione el host en el que se debe montar el clon y se instalará el complemento.
SID del clon de destino	Ingrese el ID de la instancia de SAP HANA para clonar desde las copias de seguridad existentes.
Dirección IP de exportación de NFS	Introduzca las direcciones IP o los nombres de host a los que se exportarán los volúmenes clonados.
Iniciador iSCSI	Introduzca el nombre del iniciador iSCSI del host al que se exportan los LUN. Esta opción solo está disponible si seleccionó el tipo de recurso LUN.
Protocolo	Introduzca el protocolo LUN. Esta opción solo está disponible si seleccionó el tipo de recurso LUN.

Si el recurso seleccionado es un LUN y está clonando desde una copia de seguridad secundaria, se enumeran los volúmenes de destino. Un único recurso puede tener varios volúmenes de destino.



Antes de clonar, debe asegurarse de que el iniciador iSCSI o el FCP estén presentes y configurados e iniciados sesión en hosts alternativos.

7. En la página Scripts, realice los siguientes pasos:



Los scripts se ejecutan en el host del complemento.

- a. Introduzca los comandos para pre-clonar o post-clonar que deben ejecutarse antes o después de la operación de clonación, respectivamente.
 - Comando de preclonación: eliminar bases de datos existentes con el mismo nombre
 - Comando posterior a la clonación: verificar una base de datos o iniciar una base de datos.
- b. Introduzca el comando de montaje para montar un sistema de archivos en un host.

Comando de montaje para un volumen o qtree en una máquina Linux:

Ejemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

9. Revise el resumen y luego haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Recupere las copias de seguridad para realizar la operación de clonación mediante el cmdlet `Get-SmBackup`.

Este ejemplo muestra que hay dos copias de seguridad disponibles para clonar:

```
C:\PS> Get-SmBackup

      BackupId      BackupName
-----
BackupTime      BackupType
-----
1
8/4/2015 11:02:32 AM    Payroll Dataset_vise-f6_08...
                        Full Backup
2
8/4/2015 11:23:17 AM    Payroll Dataset_vise-f6_08...
```

3. Inicie una operación de clonación desde una copia de seguridad existente y especifique las direcciones IP de exportación NFS en las que se exportan los volúmenes clonados.

Este ejemplo muestra que la copia de seguridad 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 especifica NFSExportIPs, el valor predeterminado se exporta al host de destino clonado.

4. Verifique que las copias de seguridad se hayan clonado correctamente utilizando el cmdlet Get-SmCloneReport para ver los detalles del trabajo de clonación.

Puede ver detalles como el ID del clon, la fecha y hora de inicio, 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            :
```

Supervisar las operaciones de clonación de bases de datos de SAP HANA

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clone2, el clone1 es un clon intermedio y no se puede realizar la operación de división de clon en el clone1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clone2, puede realizar la operación de división de clon en el clone1 porque el clone1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone, consulte ["Dividir un volumen FlexClone de su volumen principal"](#).
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Eliminar o dividir clones de bases de datos de SAP HANA después de actualizar SnapCenter

Después de actualizar a SnapCenter 4.3, ya no verá los clones. Puede eliminar el clon o dividir los clones desde la página Topología del recurso desde el cual se crearon los clones.

Acerca de esta tarea

Si desea localizar la huella de almacenamiento de los clones ocultos, ejecute el siguiente comando: `Get-SmClone -ListStorageFootprint`

Pasos

1. Elimine las copias de seguridad de los recursos clonados mediante el cmdlet `remove-smbbackup`.
2. Elimine el grupo de recursos de los recursos clonados mediante el cmdlet `remove-smresourcegroup`.
3. Elimine la protección del recurso clonado mediante el cmdlet `remove-smprotectresource`.
4. Seleccione el recurso principal en la página Recursos.

Se muestra la página de topología de recursos.

5. Desde la vista Administrar copias, seleccione los clones de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).
6. Seleccione los clones y luego haga clic  Para eliminar clones o hacer clic  Para dividir los clones.
7. Haga clic en **Aceptar**.

Proteger las bases de datos de Oracle

Descripción general del complemento SnapCenter para Oracle Database

¿Qué puede hacer con el complemento para Oracle Database?

El complemento SnapCenter para Oracle Database es un componente del lado del host del software SnapCenter de NetApp que permite la gestión de protección de datos consciente de la aplicación de las bases de datos Oracle.

El complemento para Oracle Database automatiza la copia de seguridad, la catalogación y la descatalogación con Oracle Recovery Manager (RMAN), la verificación, el montaje, el desmontaje, la restauración, la recuperación y la clonación de bases de datos Oracle en su entorno SnapCenter. El complemento para Oracle Database instala el complemento SnapCenter para UNIX para realizar todas las operaciones de protección de datos.

Puede utilizar el complemento para Oracle Database para administrar copias de seguridad de bases de datos Oracle que ejecutan aplicaciones SAP. Sin embargo, no se admite la integración de SAP BR*Tools.

- Realizar copias de seguridad de archivos de datos, archivos de control y archivos de registro de archivo.

La copia de seguridad solo se admite en el nivel de base de datos de contenedor (CDB).

- Restauración y recuperación de bases de datos, CDB y bases de datos conectables (PDB).

No se admite la recuperación incompleta de PDB.

- Crear clones de bases de datos de producción hasta un punto en el tiempo.

La clonación solo se admite en el nivel CDB.

- Verifique las copias de seguridad inmediatamente.
- Montar y desmontar copias de seguridad de datos y registros para la operación de recuperación.
- Programar operaciones de respaldo y verificación.
- Supervisar todas las operaciones.
- Ver informes de operaciones de copia de seguridad, restauración y clonación.
- Automatiza operaciones de copia de seguridad, restauración, recuperación, verificación, montaje, desmontaje y clonación basadas en aplicaciones para bases de datos Oracle en su entorno SnapCenter.
- Admite bases de datos Oracle para SAP, sin embargo, no se proporciona integración con SAP BR*Tools

Características del complemento para Oracle Database

El complemento para Oracle Database se integra con la base de datos Oracle en el host Linux o AIX y con las tecnologías NetApp en el sistema de almacenamiento.

- Interfaz gráfica de usuario unificada

La interfaz de SnapCenter proporciona estandarización y consistencia entre complementos y entornos. La

interfaz de SnapCenter le permite completar operaciones consistentes de respaldo, restauración, recuperación y clonación en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y monitorear trabajos en todos los complementos.

- Administración central automatizada

Puede programar operaciones de copia de seguridad y clonación, configurar la retención de copias de seguridad basada en políticas y realizar operaciones de restauración. También puede supervisar su entorno de forma proactiva configurando SnapCenter para enviar alertas por correo electrónico.

- Tecnología NetApp Snapshot sin interrupciones

SnapCenter utiliza la tecnología NetApp Snapshot con el complemento para Oracle Database y el complemento para UNIX para realizar copias de seguridad de las bases de datos. Las instantáneas consumen un espacio de almacenamiento mínimo.

El complemento para Oracle Database también ofrece los siguientes beneficios:

- Soporte para flujos de trabajo de copia de seguridad, restauración, clonación, montaje, desmontaje y verificación
- Descubrimiento automático de bases de datos Oracle configuradas en el host
- Soporte para catalogar y descatalogar mediante Oracle Recovery Manager (RMAN)
- Seguridad respaldada por RBAC y delegación de roles centralizada

También puede configurar las credenciales para que los usuarios autorizados de SnapCenter tengan permisos a nivel de aplicación.

- Compatibilidad con la gestión de registros de archivo (ALM) para operaciones de restauración y clonación
- Creación de copias puntuales y con uso eficiente del espacio de bases de datos de producción para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

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

- Compatibilidad con la función de grupo de consistencia (CG) de ONTAP como parte de la creación de copias de seguridad en entornos SAN y ASM
- Verificación de copias de seguridad automatizada y sin interrupciones
- Capacidad de ejecutar múltiples copias de seguridad simultáneamente en varios hosts de bases de datos

En una sola operación, las instantáneas se consolidan cuando las bases de datos de un solo host comparten el mismo volumen.

- Soporte para 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 mapa LUN selectivo (SLM) de ONTAP

Habilitada de forma predeterminada, la función SLM descubre periódicamente los LUN que no tienen rutas optimizadas y los corrige. Puede configurar SLM modificando los parámetros en el archivo scu.properties ubicado en /var/opt/snapcenter/scu/etc.

- Puede deshabilitar esto estableciendo el valor del parámetro `ENABLE_LUNPATH_MONITORING` en falso.
- Puede especificar la frecuencia con la que las rutas LUN se repararán automáticamente asignando el valor (en horas) al parámetro `LUNPATH_MONITORING_INTERVAL`. Para obtener información sobre SLM, consulte la "[Sección de administración de SAN de ONTAP 9](#)".
- Compatibilidad con memoria no volátil express (NVMe) en Linux
 - La utilidad NVMe debe estar instalada en el host.

Debes instalar la utilidad NVMe para clonar o montar en un host alternativo.

- Las operaciones de copia de seguridad, restauración, clonación, montaje, desmontaje, catalogación, descatalogación y verificación son compatibles con el hardware NVMe, excepto en entornos virtualizados como RDM.

Las operaciones anteriores son compatibles con dispositivos sin particiones o con una sola partición.



Puede configurar la solución de múltiples rutas para dispositivos NVMe configurando la opción de múltiples rutas nativa en el kernel. No se admite la multirruta de Device Mapper (DM).

- Los flujos de trabajo de copia de seguridad, restauración, clonación, montaje, desmontaje, catalogación, descatalogación y verificación son compatibles con NVMe sobre TCP/IP.
- Los flujos de trabajo de copia de seguridad, restauración, clonación, montaje, desmontaje, catalogación, descatalogación y verificación son compatibles con el diseño VMDK creado en NVMe a través de TCP/IP.
- Admite la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios comerciales sigan funcionando incluso en caso de una falla total del sitio, permitiendo que las aplicaciones conmuten por error de manera transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una conmutación por error con la sincronización activa de SnapMirror.
- Admite cualquier usuario no predeterminado en lugar de Oracle y Grid.

Para admitir a los usuarios no predeterminados, debe configurarlos 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 establecen como oráculo y cuadrícula.

- `DB_USER=oracle`
- `DB_GROUP=desinstalar`
- `GI_USER=cuadrícula`
- `GI_GROUP=desinstalar`

Tipos de almacenamiento admitidos por el complemento para Oracle Database

SnapCenter admite una amplia gama de tipos de almacenamiento en máquinas físicas y virtuales. Debe verificar la compatibilidad con su tipo de almacenamiento antes de instalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX.

SnapCenter no admite el aprovisionamiento de almacenamiento para Linux y AIX.

Tipos de almacenamiento compatibles con Linux

La siguiente tabla enumera los tipos de almacenamiento compatibles con Linux.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • Volúmenes conectados a NFS • NVMe-FC • NVMe/TCP
VMware ESXi	• El escaneo de los adaptadores de bus de host (HBA) puede demorar mucho tiempo en completarse porque SnapCenter escanea todos los adaptadores de bus de host presentes en el host. Puede editar el archivo LinuxConfig.pm ubicado en <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> para establecer el valor del parámetro SCSI_HOSTS_OPTIMIZED_RESCAN en 1 para volver a escanear solo los HBA que figuran en <code>HBA_DRIVER_NAMES</code>. • LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creados a través de NVMe/TCP  RAC es compatible con ESX 8.0U2, que tiene soporte para VMDK compartido • Volúmenes NFS conectados directamente al sistema invitado • Almacenes de datos vVol tanto en NFS como en 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 compatibles con AIX.

Máquina	Tipo de almacenamiento
Servidor físico	- LUN conectados a FC y conectados a iSCSI. En un entorno SAN, se admiten los sistemas de archivos ASM, LVM y SAN.  NFS en AIX y otros sistemas de archivos no es compatible. - Sistema de archivos con registro mejorado (JFS2) Admite registro en línea en sistemas de archivos SAN y diseño LVM.

El "[Herramienta de matriz de interoperabilidad de NetApp](#)" Contiene la información más reciente sobre las versiones compatibles.

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el complemento de Oracle

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la "[Documentación de ONTAP](#)".

Privilegios mínimos de ONTAP necesarios para el complemento de Oracle

Los privilegios mínimos de ONTAP necesarios varían según los complementos de

SnapCenter que utilice para la protección de datos.

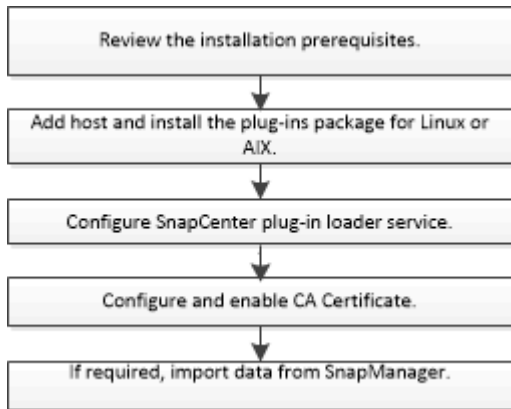
- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo
 - Mostrar atributo lun
 - lun crear
 - eliminar lun
 - geometría lun
 - agregar igroup lun
 - crear igroup lun
 - eliminar igroup lun
 - Cambiar nombre de igroup lun
 - Programa de igroup de Lun
 - Asignación de LUN a nodos de informes adicionales
 - creación de mapeo LUN
 - eliminar mapeo lun
 - Mapeo de LUN: eliminar nodos de informes
 - espectáculo de mapeo de lun
 - modificar lun
 - volumen de movimiento de LUN
 - lun sin conexión
 - lun en línea
 - lun reserva persistente clara
 - cambio de tamaño de lun
 - serie lun
 - espectáculo de almuerzo
 - regla de adición de política de SnapMirror
 - regla de modificación de política de SnapMirror
 - regla de eliminación de política de SnapMirror
 - Mostrar política de Snapmirror
 - restauración de SnapMirror
 - espectáculo de Snapmirror
 - historial de programas de Snapmirror
 - actualización de SnapMirror
 - actualización-ls-set de snapmirror

- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- vserver
- CIFs de vserver
- Mostrar copia de sombra de CIF de vserver
- espectáculo vserver
- interfaz de red
- Mostrar interfaz de red
- espectáculo del metrocluster

Instalar el complemento de SnapCenter para la base de datos Oracle

Flujo de trabajo de instalación del complemento SnapCenter para Oracle Database

Debe instalar y configurar el complemento SnapCenter para Oracle Database si desea proteger las bases de datos Oracle.



Requisitos previos para agregar hosts e instalar el paquete de complementos para Linux o AIX

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos.

- Si está utilizando iSCSI, el servicio iSCSI debe estar ejecutándose.
- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.

El complemento SnapCenter para Oracle Database puede ser instalado por un usuario que no sea root. Sin embargo, debe configurar los privilegios de sudo para que el usuario no root pueda instalar e iniciar el proceso del complemento. Después de instalar el complemento, los procesos se ejecutarán como un usuario no root efectivo.

- Si está instalando el paquete de complementos de SnapCenter para AIX en un host AIX, debe haber resuelto manualmente los enlaces simbólicos de nivel de directorio.

El paquete de complementos de SnapCenter para AIX resuelve automáticamente el enlace simbólico a nivel de archivo, pero no los enlaces simbólicos a nivel de directorio para obtener la ruta absoluta `JAVA_HOME`.

- Cree credenciales con modo de autenticación como Linux o AIX para el usuario de instalación.
- Debe tener instalado Java 11 en su host Linux o AIX.
 - Java de Oracle y OpenJDK es compatible con Linux
 - IBM Java para AIX. Puedes descargarlo desde ["Descargas de IBM Semeru Runtimes"](#)



Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux.

- Para las bases de datos Oracle que se ejecutan en un host Linux o AIX, debe instalar el complemento SnapCenter para Oracle Database y el complemento SnapCenter para UNIX.



También puede utilizar el complemento para Oracle Database para administrar bases de datos Oracle para SAP. Sin embargo, no se admite la integración de SAP BR*Tools.

- Si está utilizando la base de datos Oracle 11.2.0.3 o posterior, debe instalar el parche Oracle 13366202.



SnapCenter no admite la asignación de UUID en el archivo `/etc/fstab`.

- Debe tener **bash** como el shell predeterminado para la instalación del complemento.

Requisitos del host Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de complementos de SnapCenter para Linux.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux Si utiliza una base de datos Oracle en LVM en sistemas operativos Oracle Linux o Red Hat Enterprise Linux 6.6 o 7.0, debe instalar la última versión de Logical Volume Manager (LVM). • Servidor empresarial SUSE Linux (SLES)
RAM mínima para el complemento SnapCenter en el host	2 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.

Artículo	Requisitos
Paquetes de software necesarios	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 última versión, debe asegurarse de que la opción JAVA_HOME ubicada en <code>/var/opt/snapcenter/spl/etc/spl.properties</code> esté configurada en la versión de JAVA correcta y en la ruta correcta.

Para obtener la información más reciente sobre las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Configurar privilegios de sudo para usuarios no root para el host Linux

SnapCenter 2.0 y versiones posteriores permiten que un usuario no root instale el paquete de complementos de SnapCenter para Linux e inicie el proceso de complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el permiso 555. De lo contrario, la instalación del complemento podría fallar.
- Para el usuario no root, asegúrese de que el nombre del usuario no root y el grupo del usuario sean los mismos.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- /inicio/*USUARIO_LINUX*/sc_netapp/snapcenter_linux_host_plugin.bin
- /ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar
- /ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl

Pasos

1. Inicie sesión en el host Linux en el que desea instalar el paquete de complementos de SnapCenter para Linux.
2. Agregue las siguientes líneas al archivo /etc/sudoers utilizando la utilidad visudo para 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/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, 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 RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host AIX

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de complementos de SnapCenter para AIX.



El complemento SnapCenter para UNIX, que forma parte del paquete de complementos SnapCenter para AIX, no admite grupos de volúmenes simultáneos.

Artículo	Requisitos
Sistemas operativos	AIX 7.1 o posterior
RAM mínima para el complemento SnapCenter en el host	4 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 IBM Java Si ha actualizado JAVA a la última versión, debe asegurarse de que la opción JAVA_HOME ubicada en <code>/var/opt/snapcenter/spl/etc/spl.properties</code> esté configurada en la versión de JAVA correcta y en la ruta correcta.

Para obtener la información más reciente sobre las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Configurar privilegios de sudo para usuarios no root para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no root instale el paquete de complementos de SnapCenter para AIX e inicie el proceso de complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el permiso 555. De lo contrario, la instalación del complemento podría fallar.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- /inicio/*USUARIO_AIX*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar
- /ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl

Pasos

1. Inicie sesión en el host AIX en el que desea instalar el paquete de complementos de SnapCenter para AIX.
2. Agregue las siguientes líneas al archivo /etc/sudoers utilizando la utilidad visudo para 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/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



Si tiene una configuración RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Configurar credenciales

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar el paquete de complemento en hosts Linux o AIX.

Acerca de esta tarea

Las credenciales se crean para el usuario root o para un usuario no root que tenga privilegios de sudo para instalar e iniciar el proceso del complemento.

Para obtener información, consulte: [Configurar privilegios de sudo para usuarios no root para el host Linux](#) o [Configurar privilegios de sudo para usuarios no root para el host AIX](#)

Mejor práctica: Si bien se le permite crear credenciales después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, ingrese la información de la credencial:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. - Administrador de dominio Especifique el administrador del dominio en el sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: <i>NetBIOS\Nombre de usuario</i> <i>Dominio FQDN\Nombre de usuario</i> - 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>NombreDeUsuario</i>
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar. Dependiendo del sistema operativo del host del complemento, seleccione Linux o AIX.
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no sea root.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página **Usuario y acceso**.

Configurar credenciales para una base de datos Oracle

Debe configurar las credenciales que se utilizan para realizar operaciones de protección de datos en las bases de datos de Oracle.

Acerca de esta tarea

Debe revisar los diferentes métodos de autenticación compatibles con la base de datos Oracle. Para obtener

más información, consulte ["Métodos de autenticación para sus credenciales"](#) .

Si configura 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 de respaldo.

Si ha habilitado la autenticación de la base de datos de Oracle, se muestra un ícono de candado rojo en la vista de recursos. Debe configurar las credenciales de la base de datos para poder proteger la base de datos o agregarla al grupo de recursos para realizar operaciones de protección de datos.



Si especifica detalles incorrectos al crear una credencial, se mostrará un mensaje de error. Debes hacer clic en **Cancelar** y luego volver a intentarlo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista **Ver**.
3. Hacer clic  y luego seleccione el nombre del host y el tipo de base de datos para filtrar los recursos.

Luego puedes hacer clic  para cerrar el panel de filtro.

4. Seleccione la base de datos y luego haga clic en **Configuración de la base de datos > Configurar base de datos**.
5. En la sección Configurar parámetros de base de datos, en la lista desplegable **Usar credencial existente**, seleccione la credencial que se debe utilizar para realizar trabajos de protección de datos en la base de datos Oracle.



El usuario de Oracle debe tener privilegios sysdba.

También puede crear una credencial haciendo clic en  .

6. En la sección Configurar ajustes de ASM, en la lista desplegable **Usar credencial existente**, seleccione la credencial que se debe usar para realizar trabajos de protección de datos en la instancia de ASM.



El usuario ASM debe tener privilegios sysasm.

También puede crear una credencial haciendo clic en  .

7. En la sección Configurar parámetros del catálogo RMAN, en la lista desplegable **Usar credencial existente**, seleccione la credencial que se debe utilizar para realizar trabajos de protección de datos en la base de datos del catálogo de Oracle Recovery Manager (RMAN).

También puede crear una credencial haciendo clic en  .

En el campo **TNSName**, ingrese el nombre del archivo de sustrato de red transparente (TNS) que utilizará el servidor SnapCenter para comunicarse con la base de datos.

8. En el campo **Nodos RAC preferidos**, especifique los nodos del clúster de aplicaciones reales (RAC) preferidos para la copia de seguridad.

Los nodos preferidos podrían ser uno o todos los nodos del clúster donde están presentes las instancias

de la base de datos RAC. La operación de copia de seguridad se activa solo en estos nodos preferidos en el orden de preferencia.

En RAC One Node, solo se incluye un nodo en los nodos preferidos, y este nodo preferido es el nodo donde se encuentra alojada actualmente la base de datos.

Después de una conmutación por error o reubicación de la base de datos de RAC One Node, la actualización de los recursos en la página Recursos de SnapCenter eliminará el host de la lista **Nodos RAC preferidos** donde la base de datos estaba alojada anteriormente. El nodo RAC donde 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"](#) .

9. Haga clic en **Aceptar**.

Agregue hosts e instale el paquete de complementos para Linux o AIX mediante GUI

Puede utilizar la página Agregar host para agregar hosts y luego instalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX. Los complementos se instalan automáticamente en los hosts remotos.

Acerca de esta tarea

Puede agregar un host e instalar paquetes de complementos para un host individual o para un clúster. Si está instalando el complemento en un clúster (Oracle RAC), el complemento se instala en todos los nodos del clúster. Para Oracle RAC One Node, debe instalar el complemento en los nodos activos y pasivos.



Solo se admite la autenticación basada en contraseña cuando se instala el complemento en un Oracle RAC. No se admite la autenticación basada en clave SSH.

Se le debe asignar un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .



No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione Linux o AIX como tipo de host. El servidor SnapCenter agrega el host y luego instala el complemento para Oracle Database y el complemento para UNIX si los complementos aún no están instalados en el host.
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar 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)  No se admite el VIP del nodo ni la IP de escaneo Si está agregando un host mediante SnapCenter y el host es parte de un subdominio, debe proporcionar el FQDN.
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección Seleccionar complementos para instalar, seleccione los complementos que desea instalar.
6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.
Ruta de instalación	La ruta predeterminada es <code>/opt/ NetApp/snapcenter</code>. Opcionalmente puedes personalizar la ruta.
Agregar todos los hosts en Oracle RAC	Seleccione esta casilla de verificación para agregar todos los nodos del clúster en un Oracle RAC. En una configuración de Flex ASM, se agregarán todos los nodos, independientemente de si son nodos centrales o de hoja.
Omitir comprobaciones de preinstalación opcionales	Seleccione esta casilla de verificación si ya ha instalado los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla de verificación Omitir comprobaciones previas, se valida el host para verificar si cumple con los requisitos para instalar el complemento.



El script de verificación previa no valida el estado del firewall del puerto del complemento si está especificado en las reglas de rechazo del firewall.

Se muestran mensajes de error o advertencia apropiados si no se cumplen los requisitos mínimos. 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo `web.config`, debe actualizar el archivo en ambos nodos.

8. Verifique la huella digital y luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.



SnapCenter no admite el algoritmo ECDSA.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

Los archivos de registro específicos de la instalación se encuentran en `/custom_location/snapcenter/logs`.

Resultado

Todas las bases de datos del host se descubren automáticamente y se muestran en la página Recursos. Si no se muestra nada, haga clic en **Actualizar recursos**.

Supervisar el estado de la instalación

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 complementos para Linux o AIX

También puede instalar el paquete de complementos para Linux o AIX manualmente utilizando los cmdlets o las CLI.

Antes de instalar el complemento manualmente, debe validar la firma del paquete binario utilizando la clave **snapcenter_public_key.pub** y **snapcenter_linux_host_plugin.bin.sig** ubicadas en *C:\ProgramData\NetApp\ SnapCenter\Package Repository*.



Asegúrese de que **OpenSSL 1.0.2g** esté instalado en el host donde desea instalar el complemento.

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 el host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

Instalar en varios hosts remotos mediante cmdlets

Debe utilizar el cmdlet de PowerShell *Install-SmHostPackage* para instalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX en varios hosts.

Lo que necesitarás

Debe iniciar sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar el paquete de complemento.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet *Open-SmConnection* y luego ingrese sus credenciales.
3. Instale el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX utilizando el cmdlet *Install-SmHostPackage* y los parámetros necesarios.

Puede utilizar la opción *-skipprecheck* cuando ya haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.



El script de verificación previa no valida el estado del firewall del puerto del complemento si está especificado en las reglas de rechazo del firewall.

4. Introduzca sus credenciales para la instalación remota.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Instalar en el host del clúster

Debe instalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX en ambos 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 respectivos nodos y la segunda IP será la IP del cluster que se comparte entre ambos nodos.

Pasos

1. Instale el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX en ambos nodos del host del clúster.
2. Valide que los valores correctos para los parámetros `SNAPCENTER_SERVER_HOST`, `SPL_PORT`, `SNAPCENTER_SERVER_PORT` y `SPL_ENABLED_PLUGINS` estén especificados en el archivo `spl.properties` ubicado en `/var/opt/snapcenter/spl/etc/`.

Si `SPL_ENABLED_PLUGINS` no se especifica en `spl.properties`, puede agregarlo y asignar el valor `SCO,SCU`.
3. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet *Open-SmConnection* y luego ingrese sus credenciales.
4. En cada uno de los nodos, configure las IP preferidas del nodo utilizando el comando `sccli Set-PreferredHostIPsInStorageExportPolicy` 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. Agregue el nodo al servidor SnapCenter mediante el cmdlet *Add-SmHost* especificando la IP del clúster para el nombre del host.

Descubra la base de datos de Oracle en el nodo 1 (asumiendo que la IP del clúster está alojada en el nodo 1) y cree una copia de seguridad de la base de datos. Si ocurre una conmutación por error, puede utilizar la copia de seguridad creada en el nodo 1 para restaurar la base de datos en el nodo 2. También puede utilizar la copia de seguridad creada en el nodo 1 para crear un clon en el nodo 2.



Habrán volúmenes, directorios y archivos de bloqueo obsoletos si la conmutación por error ocurre mientras se ejecutan otras operaciones de SnapCenter .

Instalar el paquete de complementos para Linux en modo silencioso

Puede instalar el paquete de complementos de SnapCenter para Linux en modo silencioso mediante la interfaz de línea de comandos (CLI).

Lo que necesitarás

- Debe revisar los requisitos previos para instalar el paquete de complementos.
- Debe asegurarse de que la variable de entorno `DISPLAY` no esté configurada.

Si la variable de entorno `DISPLAY` está configurada, debe ejecutar `unset DISPLAY` y luego intentar instalar el complemento manualmente.

Acerca de esta tarea

Debe proporcionar la información de instalación necesaria durante la instalación en modo consola, mientras

que en la instalación en modo silencioso no es necesario proporcionar ninguna información de instalación.

Pasos

1. Descargue el paquete de complementos de SnapCenter para Linux desde la ubicación de instalación del servidor SnapCenter .

La ruta de instalación predeterminada es *C:\ProgramData\ NetApp\ SnapCenter\PackageRepository*. Se puede acceder a esta ruta desde el host donde está instalado el servidor SnapCenter .

2. Desde el símbolo del sistema, navegue hasta el directorio donde descargó el archivo de instalación.
3. Correr

```
./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 agregar *SPL_ENABLED_PLUGINS=SCO,SCU* y luego reinicie el servicio SnapCenter Plug-in Loader .



La instalación del paquete de complementos registra los complementos en el host y no en el servidor SnapCenter . Debe registrar los complementos en el servidor SnapCenter agregando el host mediante la GUI de SnapCenter o el cmdlet de PowerShell. Al agregar el host, seleccione “Ninguno” como credencial. Una vez agregado el host, los complementos instalados se descubren automáticamente.

Instalar el paquete de complementos para AIX en modo silencioso

Puede instalar el paquete de complementos de SnapCenter para AIX en modo silencioso mediante la interfaz de línea de comandos (CLI).

Lo que necesitarás

- Debe revisar los requisitos previos para instalar el paquete de complementos.
- Debe asegurarse de que la variable de entorno *DISPLAY* no esté configurada.

Si la variable de entorno *DISPLAY* está configurada, debe ejecutar *unset DISPLAY* y luego intentar instalar el complemento manualmente.

Pasos

1. Descargue el paquete de complementos de SnapCenter para AIX desde la ubicación de instalación del servidor SnapCenter .

La ruta de instalación predeterminada es *C:\ProgramData\ NetApp\ SnapCenter\PackageRepository*. Se puede acceder a esta ruta desde el host donde está instalado el servidor SnapCenter .

2. Desde el símbolo del sistema, navegue hasta el directorio donde descargó el archivo de instalación.
3. Correr

```
./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 agregar `SPL_ENABLED_PLUGINS=SCO,SCU` y luego reinicie el servicio SnapCenter Plug-in Loader .



La instalación del paquete de complementos registra los complementos en el host y no en el servidor SnapCenter . Debe registrar los complementos en el servidor SnapCenter agregando el host mediante la GUI de SnapCenter o el cmdlet de PowerShell. Al agregar el host, seleccione “Ninguno” como credencial. Una vez agregado el host, los complementos instalados se descubren automáticamente.

Configurar el servicio de Loader de complementos de SnapCenter

El servicio Loader de complementos de SnapCenter carga el paquete de complementos para Linux o AIX para interactuar con el servidor SnapCenter . El servicio Loader de complementos de SnapCenter se instala cuando instala el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX.

Acerca de esta tarea

Después de instalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX, el servicio SnapCenter Plug-in Loader se inicia automáticamente. Si el servicio SnapCenter Plug-in Loader no se inicia automáticamente, debe:

- Asegúrese de que el directorio donde está funcionando el complemento no se elimine
- Aumentar el espacio de memoria asignado a la máquina virtual Java

El archivo `spl.properties`, que se encuentra en `/custom_location/ NetApp/snapcenter/spl/etc/`, contiene los siguientes parámetros. A estos parámetros se les asignan valores predeterminados.

Nombre del parámetro	Descripción
NIVEL DE REGISTRO	Muestra los niveles de registro admitidos. Los valores posibles son TRACE, DEBUG, INFO, WARN, ERROR y FATAL.
PROTOCOLO SPL	Muestra el protocolo compatible con SnapCenter Plug-in Loader. Sólo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.
PROTOCOLO DEL SERVIDOR SNAPCENTER	Muestra el protocolo compatible con SnapCenter Server. Sólo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.

Nombre del parámetro	Descripción
SALTAR ACTUALIZACIÓN DE JAVAHOME	De forma predeterminada, el servicio SPL detecta la ruta de Java y actualiza el parámetro JAVA_HOME. Por lo tanto, el valor predeterminado se establece en FALSO. Puede establecerlo en VERDADERO si desea deshabilitar el comportamiento predeterminado y corregir manualmente la ruta de Java.
CONTRASEÑA DEL ALMACÉN DE LLAVES SPL	Muestra la contraseña del archivo del almacén de claves. Puede cambiar este valor solo si cambia la contraseña o crea un nuevo archivo de almacén de claves.
SPL_PORT	Muestra el número de puerto en el que se ejecuta el servicio SnapCenter Plug-in Loader . Puede agregar el valor si falta el valor predeterminado.  No debe cambiar el valor después de instalar los complementos.
HOST DEL SERVIDOR SNAPCENTER	Muestra la dirección IP o el nombre de host del servidor SnapCenter .
RUTA DEL ALMACÉN DE LLAVES SPL	Muestra la ruta absoluta del archivo del almacén de claves.
PUERTO DEL SERVIDOR SNAPCENTER	Muestra el número de puerto en el que se ejecuta el servidor SnapCenter .

Nombre del parámetro	Descripción
CONTEO MÁXIMO DE REGISTROS	Muestra la cantidad de archivos de registro del Loader de complementos de SnapCenter que se conservan en la carpeta <code>/custom_location/snapcenter/spl/logs</code>. El valor predeterminado se establece en 5000. Si el recuento es mayor que el valor especificado, se conservan los últimos 5000 archivos modificados. La verificación de la cantidad de archivos se realiza automáticamente cada 24 horas desde que se inicia el servicio SnapCenter Plug-in Loader .  Si elimina manualmente el archivo <code>spl.properties</code>, la cantidad de archivos que se conservarán se establecerá en 9999.
JAVA_HOME	Muestra la ruta absoluta del directorio JAVA_HOME que se utiliza para iniciar el servicio SPL. Esta ruta se determina durante la instalación y como parte del inicio de SPL.
TAMAÑO MÁXIMO DE REGISTRO	Muestra el tamaño máximo del archivo de registro de trabajo. Una vez que se alcanza el tamaño máximo, el archivo de registro se comprime y los registros se escriben en el nuevo archivo de ese trabajo.
RETENCIÓN DE REGISTROS DE LOS ÚLTIMOS DÍAS	Muestra el número de días que se conservan los registros.
HABILITAR VALIDACIÓN DE CERTIFICADO	Se muestra como verdadero cuando la validación del certificado CA está habilitada para el host. Puede habilitar o deshabilitar este parámetro editando <code>spl.properties</code> o utilizando la GUI o el cmdlet de SnapCenter .

Si alguno de estos parámetros no está asignado 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 cualquier problema relacionado con los valores asignados a los parámetros. Después de modificar el archivo `spl.properties`, debe reiniciar el servicio SnapCenter Plug-in Loader .

Pasos

1. Realice una de las siguientes acciones, según sea necesario:
 - Inicie el servicio SnapCenter Plug-in Loader :

- Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
- Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- Detener el servicio de Loader de complementos de SnapCenter :
 - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



Puede utilizar la opción `-force` con el comando `stop` para detener a la fuerza el servicio SnapCenter Plug-in Loader . Sin embargo, debe tener cuidado antes de hacerlo porque también termina las operaciones existentes.

- Reinicie el servicio del Loader de complementos de SnapCenter :
 - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Encuentre el estado del servicio Loader de complementos 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`
- Encuentre el cambio en el servicio SnapCenter Plug-in Loader :
 - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurar el certificado de CA con el servicio SnapCenter Plug-in Loader (SPL) en el host Linux

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



SPL utiliza el archivo 'keystore.jks', que se encuentra en '/var/opt/snapcenter/spl/etc' como almacén de confianza y almacén de claves.

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

Pasos

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

Es el valor correspondiente a la clave 'SPL_KEYSTORE_PASS'.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave
privada en el almacén de claves a 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.

3. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves SPL y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para el almacén de confianza SPL

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

Pasos

1. Navegue a la carpeta que contiene el almacén de claves SPL: */var/opt/snapcenter/spl/etc*.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
. Agregar un certificado raíz o intermedio:
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza SPL.
```



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

Configurar el par de claves firmadas de CA para el almacén de confianza SPL

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

Pasos

1. Navegue a la carpeta que contiene el almacén de claves de SPL `/var/opt/snapcenter/spl/etc`.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
. Agregue el certificado CA que tenga clave privada y pública.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Enumere los certificados agregados en el almacén de claves.
```

```
keytool -list -v -keystore keystore.jks
. Verifique que el almacén de claves contenga el alias correspondiente
al nuevo certificado de CA, que se agregó al almacén de claves.
. Cambie la contraseña de clave privada agregada para el certificado de
CA a la contraseña del almacén de claves.
```

La contraseña del almacén de claves SPL predeterminada es el valor de la clave `SPL_KEYSTORE_PASS` en el archivo `spl.properties`.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Si el nombre de alias en el certificado de CA es largo y contiene
espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a
un nombre simple:
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure el nombre de alias desde el almacén de claves ubicado en el
archivo spl.properties.
```

Actualice este valor con la clave `SPL_CERTIFICATE_ALIAS`.

4. Reinicie el servicio después de configurar el par de claves firmadas por 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 para SPL es `/var/opt/snapcenter/spl/etc/crl`.

Pasos

1. Puede modificar y actualizar el directorio predeterminado en el archivo `spl.properties` contra la clave `SPL_CRL_PATH`.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet `run Set-SmCertificateSettings`.
- Puede mostrar el estado del certificado de los complementos mediante `Get-SmCertificateSettings`.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Importar datos de SnapManager para Oracle y SnapManager para SAP a SnapCenter

La importación de datos de SnapManager para Oracle y SnapManager para SAP a SnapCenter le permite seguir utilizando sus datos de versiones anteriores.

Puede importar datos de SnapManager para Oracle y SnapManager para SAP a SnapCenter ejecutando la herramienta de importación desde la interfaz de línea de comandos (CLI del host de Linux).

La herramienta de importación crea políticas y grupos de recursos en SnapCenter. Las políticas y los grupos de recursos creados en SnapCenter corresponden a los perfiles y operaciones realizadas utilizando esos perfiles en SnapManager para Oracle y SnapManager para SAP. La herramienta de importación de SnapCenter interactúa con las bases de datos del repositorio SnapManager para Oracle y SnapManager para SAP y con la base de datos que desea importar.

- Recupera todos los perfiles, programaciones y operaciones realizadas utilizando los perfiles.
- Crea una política de respaldo de SnapCenter para cada operación única y cada programación asociada 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`. Cuando instala el paquete de complementos de SnapCenter para Linux en el host de base de datos que desea importar, el script `sc-migrate` se copia en `/opt/NetApp/snapcenter/spl/bin`.



La importación de datos no es compatible desde la interfaz gráfica de usuario (GUI) de SnapCenter .

SnapCenter no es compatible con Data ONTAP funcionando en modo 7. Puede utilizar la herramienta de transición de 7 modos para migrar datos y configuraciones almacenados en un sistema que ejecuta Data ONTAP en modo 7 a un sistema ONTAP .

Configuraciones admitidas para la importación de datos

Antes de importar datos de SnapManager 3.4.x para Oracle y SnapManager 3.4.x para SAP a SnapCenter, debe tener en cuenta las configuraciones compatibles con el complemento de SnapCenter para Oracle Database.

Las configuraciones compatibles con el complemento SnapCenter para Oracle Database se enumeran en la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Qué se importa a SnapCenter

Puede importar perfiles, programaciones y operaciones realizadas utilizando los perfiles.

De SnapManager para Oracle y SnapManager para SAP	A SnapCenter
Perfiles sin operaciones ni horarios	Se crea una política con el tipo de copia de seguridad predeterminado como En línea y el alcance de copia de seguridad como Completo.
Perfiles con una o más operaciones	Se crean múltiples políticas basadas en una combinación única de un perfil y operaciones realizadas utilizando ese perfil. Las políticas creadas en SnapCenter contienen los detalles de retención y poda del registro de archivo recuperados del perfil y las operaciones correspondientes.
Perfiles con configuración de Oracle Recovery Manager (RMAN)	Las políticas se crean con la opción Copia de seguridad del catálogo con Oracle Recovery Manager habilitada. Si se utilizó la catalogación RMAN externa en SnapManager, debe configurar los ajustes del catálogo RMAN en SnapCenter. Puede seleccionar la credencial existente o crear una nueva. Si RMAN se configuró a través del archivo de control en SnapManager, entonces no es necesario configurar RMAN en SnapCenter.
Horario adjunto a un perfil	Se crea una política solo para el cronograma.
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 después de 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 respaldo.

Cuando los perfiles, programaciones y cualquier operación realizada mediante los perfiles de SnapManager para Oracle y SnapManager para SAP se importan a SnapCenter, también se importan los diferentes valores de los parámetros.

Parámetros y valores de SnapManager para Oracle y SnapManager para SAP	Parámetros y valores de SnapCenter	Notas
Alcance de respaldo • Lleno • Datos • Registro	Alcance de respaldo • Lleno • Datos • Registro	
Modo de respaldo • Auto • En línea • Sin conexión	Tipo de copia de seguridad • En línea • Apagado sin conexión	Si el modo de copia de seguridad es Automático, la herramienta de importación verifica el estado de la base de datos cuando se realizó la operación y establece adecuadamente el tipo de copia de seguridad como Apagado en línea o Apagado fuera de línea.
Retención • Días • Condes	Retención • Días • Condes	SnapManager para Oracle y SnapManager para SAP utilizan días y recuentos para establecer la retención. En SnapCenter, hay Días O Recuentos. Por lo tanto, la retención se establece con respecto a los días, ya que los días tienen preferencia sobre los recuentos en SnapManager para Oracle y SnapManager para SAP.
Poda para programaciones • Todo • número de cambio del sistema (SCN) • Fecha • Registros creados antes de horas, días, semanas y meses específicos	Poda para programaciones • Todo • Registros creados antes de horas y días específicos	SnapCenter no admite la poda basada en SCN, fecha, semanas y meses.

Parámetros y valores de SnapManager para Oracle y SnapManager para SAP	Parámetros y valores de SnapCenter	Notas
Notificación • Correos electrónicos enviados solo para operaciones exitosas • Correos electrónicos enviados solo para operaciones fallidas • Correos electrónicos enviados tanto para operaciones exitosas como fallidas	Notificación • Siempre • En caso de fallo • Advertencia • Error	Se importan las notificaciones por correo electrónico. Sin embargo, debe actualizar manualmente el servidor SMTP mediante la GUI de SnapCenter . El asunto del correo electrónico se deja en blanco para que lo configures.

Qué no se importa a SnapCenter

La herramienta de importación no importa todo a SnapCenter.

No puedes importar lo siguiente a SnapCenter:

- Metadatos de respaldo
- Copias de seguridad parciales
- Copias de seguridad relacionadas con el mapeo de dispositivos sin procesar (RDM) y la consola de almacenamiento virtual (VSC)
- Roles o cualquier credencial disponible en el repositorio de SnapManager para Oracle y SnapManager para SAP
- Datos relacionados con las operaciones de verificación, restauración y clonación
- Poda para operaciones
- Detalles de replicación especificados en el perfil de SnapManager para Oracle y SnapManager para SAP

Después de importar, debe editar manualmente la política correspondiente creada en SnapCenter para incluir los detalles de replicación.

- Información de respaldo catalogada

Prepárese para importar datos

Antes de importar datos a SnapCenter, debe realizar ciertas tareas para ejecutar la operación de importación correctamente.

Pasos

1. Identifique la base de datos que desea importar.
2. Usando SnapCenter, agregue el host de la base de datos e instale el paquete de complementos de SnapCenter para Linux.
3. Mediante SnapCenter, configure las conexiones para las máquinas virtuales de almacenamiento (SVM) utilizadas por las bases de datos en el host.
4. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.

5. En la página Recursos, asegúrese de que la base de datos que se va a importar esté detectada y se muestre.

Cuando desee ejecutar la herramienta de importación, la base de datos debe ser accesible; de lo contrario, la creación del grupo de recursos fallará.

Si la base de datos tiene credenciales configuradas, debe crear una credencial correspondiente en SnapCenter, asignar la credencial a la base de datos y luego volver a ejecutar la detección de la base de datos. Si la base de datos reside en la Administración automática de almacenamiento (ASM), debe crear credenciales para la instancia de ASM y asignarlas a la base de datos.

6. Asegúrese de que el usuario que ejecuta la herramienta de importación tenga privilegios suficientes para ejecutar los comandos CLI de SnapManager para Oracle o SnapManager para SAP (como el comando para suspender programaciones) desde el host de SnapManager para Oracle o SnapManager para SAP.
7. Ejecute los siguientes comandos en el host SnapManager para Oracle o SnapManager para SAP para suspender las programaciones:

- a. Si desea suspender las programaciones en el host 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 en el host.

- b. Si desea suspender las programaciones en el host 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 en el host.

8. Asegúrese de que el nombre de dominio completo (FQDN) del host de la base de datos se muestre cuando ejecute `hostname -f`.

Si no se muestra el FQDN, debe modificar `/etc/hosts` para especificar 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 respaldo de SnapCenter que se crean después de la importación tienen diferentes formatos de nombres:

- Las políticas creadas para los perfiles sin ninguna operación ni programación tienen el formato `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED`.

Cuando no se realiza ninguna operación utilizando un perfil, se crea la política correspondiente con el tipo de copia de seguridad predeterminado en línea y el alcance de la copia de seguridad 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 desea 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 establece una conexión con SnapCenter.

4. Ingrese los detalles de la base de datos del repositorio SnapManager para Oracle o SnapManager para SAP.

La base de datos del repositorio enumera las bases de datos que están disponibles en el host.

5. Introduzca los detalles de la base de datos de destino.

Si desea importar todas las bases de datos del host, ingrese all.

6. Si desea generar un registro del sistema o enviar mensajes ASUP para operaciones fallidas, debe habilitarlos ejecutando el comando `Add-SmStorageConnection` o `Set-SmStorageConnection`.



Si desea cancelar una operación de importación, ya sea mientras ejecuta la herramienta de importación o después de la importación, debe eliminar manualmente las políticas, credenciales y grupos de recursos de SnapCenter que se crearon como parte de la operación de importación.

Resultados

Las políticas de respaldo de SnapCenter se crean para perfiles, programaciones y operaciones realizadas mediante los perfiles. También se crean grupos de recursos para cada base de datos de destino.

Después de importar los datos exitosamente, las programaciones asociadas con la base de datos importada se suspenden en SnapManager para Oracle y SnapManager para SAP.



Después de importar, debe administrar la base de datos o el sistema de archivos importado mediante 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 errores de importación y solucionarlos.

Instalar el SnapCenter Plug-in for VMware vSphere

Si su base de datos o sistema de archivos está almacenado en máquinas virtuales (VM), o si desea proteger las VM y los almacenes de datos, debe implementar el SnapCenter Plug-in for VMware vSphere .

Para obtener información sobre la implementación, consulte ["Descripción general de la implementación"](#) .

Implementar certificado de CA

Para configurar el certificado CA con el SnapCenter Plug-in for VMware vSphere, consulte ["Crear o importar certificado SSL"](#) .

Configurar el archivo CRL

El SnapCenter Plug-in for VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL para el SnapCenter Plug-in for VMware vSphere es `/opt/netapp/config/crl`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Prepárese para proteger las bases de datos de Oracle

Antes de realizar cualquier operación de protección de datos, como copias de seguridad, clonación o restauración, debe definir su estrategia y configurar el entorno. También puede configurar el servidor SnapCenter para utilizar la tecnología SnapMirror y SnapVault .

Para aprovechar la tecnología SnapVault y SnapMirror , debe configurar e inicializar una relación de protección de datos entre los volúmenes de origen y destino en el dispositivo de almacenamiento. Puede utilizar NetAppSystem Manager o puede utilizar la línea de comandos de la consola de almacenamiento para realizar estas tareas.

Antes de utilizar el complemento para Oracle Database, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server. ["Más información"](#)
- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento. ["Más información"](#)



SnapCenter no admite varias SVM con el mismo nombre en diferentes clústeres. Cada SVM registrado con SnapCenter mediante el registro SVM o el registro de clúster debe ser único.

- Cree credenciales con modo de autenticación como Linux o AIX para el usuario de instalación. ["Más información"](#)

- Agregue hosts, instale los complementos y descubra los recursos.
- Si utiliza SnapCenter Server para proteger bases de datos de Oracle que residen en LUN o VMDK de VMware RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter.
- Instale Java en su host Linux o AIX.

Ver ["Requisitos del host Linux"](#) o ["Requisitos del host AIX"](#) Para más información.

- Debe establecer el valor de tiempo de espera del firewall de la aplicación en 3 horas o más.
- Si tiene bases de datos Oracle en entornos NFS, debe haber configurado al menos un LIF de datos NFS para el almacenamiento primario o secundario para realizar operaciones de montaje, clonación, verificación y restauración.
- Si tiene varias rutas de datos (LIF) o una configuración 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 agregan a la política de exportación de almacenamiento NFS en la máquina virtual de almacenamiento (SVM) para los volúmenes clonados. Si desea tener una dirección IP específica o restringirla a un subconjunto de direcciones IP, ejecute la CLI `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 guía de referencia de comandos tiene más información.
- Si tiene bases de datos 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 ONTAP"](#)
 - ["Configuraciones de host afectadas por las utilidades de host de AIX"](#)
- Si tiene bases de datos Oracle en LVM en sistemas operativos Oracle Linux o RHEL, instale la última versión de Logical Volume Management (LVM).
- Si está utilizando SnapManager para Oracle y desea migrar al complemento SnapCenter para Oracle Database, puede migrar los perfiles a las políticas y grupos de recursos de SnapCenter mediante el comando `sccli sc-migrate`.
- Configure SnapMirror y SnapVault en ONTAP, si desea replicación de respaldo

Para los usuarios de SnapCenter 4.1.1, la documentación del SnapCenter Plug-in for VMware vSphere 4.1.1 tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, NetApp Data Broker 1.0 y 1.0.1, la documentación tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados mediante el SnapCenter Plug-in for VMware vSphere que proporciona el dispositivo virtual NetApp Data Broker basado en Linux (formato Open Virtual Appliance). Para los usuarios de SnapCenter 4.3.x, la documentación del SnapCenter Plug-in for VMware vSphere 4.3 tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual basado en Linux del SnapCenter Plug-in for VMware vSphere (formato Open Virtual Appliance).

Encuentre más información

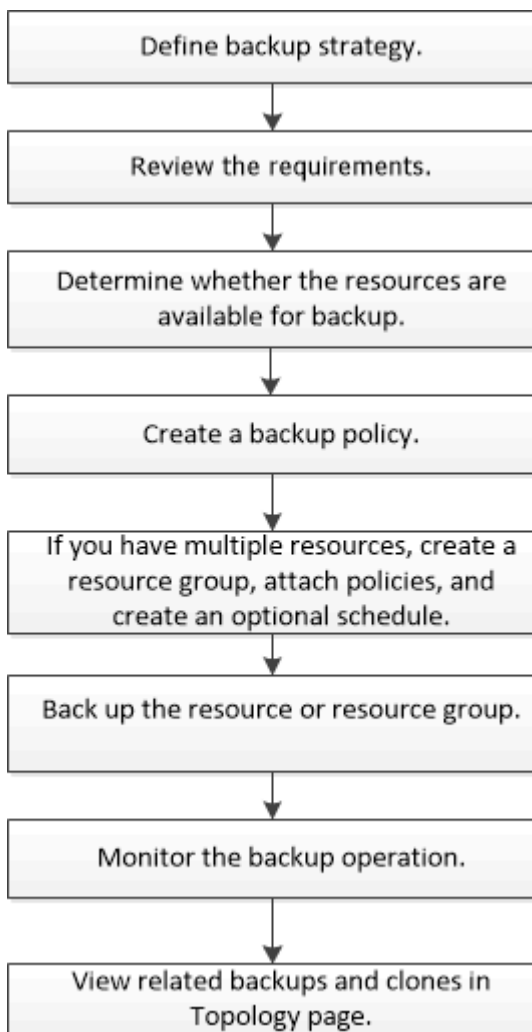
- ["Herramienta de matriz de interoperabilidad"](#)
- ["Documentación del SnapCenter Plug-in for VMware vSphere"](#)
- ["La operación de protección de datos falla en un entorno sin rutas múltiples en RHEL 7 y versiones"](#)

Realizar copias de seguridad de bases de datos de Oracle

Descripción general del procedimiento de copia de seguridad

Puede crear una copia de seguridad de un recurso (base de datos) o de un grupo de recursos. El procedimiento de copia de seguridad incluye la planificación, la identificación de los recursos para la copia de seguridad, la creación de políticas de copia de seguridad, la creación de grupos de recursos y la asociación de políticas, la creación de copias de seguridad y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



Al crear una copia de seguridad para las bases de datos Oracle, se crea un archivo de bloqueo operativo (*.sm_lock_dbsid*) en el host de la base de datos Oracle en el directorio */var/opt/snapcenter/sco/lock* para evitar que se ejecuten múltiples operaciones en la base de datos. Una vez realizada la copia de seguridad de la base de datos, el archivo de bloqueo operativo se elimina automáticamente.

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 siguiente operación de copia de seguridad pase a la cola de espera. Es posible que eventualmente se cancele si no se elimina el archivo *.sm_lock_dbsid*. En tal escenario, debe

eliminar manualmente el archivo de bloqueo operativo realizando los siguientes pasos:

1. Desde el símbolo del sistema, navegue a `/var/opt/snapcenter/sco/lock`.
2. Eliminar el bloqueo operativo: `rm -rf .sm_lock_dbid.`

Información de configuración de la copia de seguridad

Configuraciones de base de datos Oracle compatibles para copias de seguridad

SnapCenter admite la copia de seguridad de diferentes configuraciones de bases de datos de Oracle.

- Oracle independiente
- Clústeres de aplicaciones reales de Oracle (RAC)
- Oracle Standalone Legacy
- Base de datos de contenedores independiente de Oracle (CDB)
- Oracle Data Guard en espera

Solo puede crear copias de seguridad de montaje sin conexión de bases de datos en espera de Data Guard. No se admiten copias de seguridad con apagado sin conexión, copias de seguridad solo del registro de archivo ni copias de seguridad completas.

- Oracle Active Data Guard en espera

Solo puede crear copias de seguridad en línea de las bases de datos en espera de Active Data Guard. No se admiten solo copias de seguridad del registro de archivo ni copias de seguridad completas.

Antes de crear una copia de seguridad de la base de datos en espera de Data Guard o de la base de datos en espera de Data Guard activa, se detiene el proceso de recuperación administrada (MRP) y, una vez creada la copia de seguridad, 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 admitidos para las bases de datos Oracle, solo puede realizar una restauración de conexión y copia de bases de datos ASM RAC en VMDK.

- ASM independiente y ASM RAC en mapeo de dispositivos Raw (RDM) + Puede realizar operaciones de respaldo, restauración y clonación en bases de datos Oracle en ASM, con o sin ASMLib.
- Controlador de filtro Oracle ASM (ASMFD)

No se admiten operaciones de migración de PDB ni de clonación de PDB.

- Oracle Flex ASM

Para obtener la información más reciente sobre las versiones compatibles de Oracle, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Tipos de copia de seguridad compatibles con las bases de datos Oracle

El tipo de copia de seguridad especifica el tipo de copia de seguridad que desea crear.

SnapCenter admite tipos de copias de seguridad en línea y fuera de línea para bases de datos Oracle.

Copia de seguridad en línea

Una copia de seguridad que se crea cuando la base de datos está en estado en línea se denomina copia de seguridad en línea. También llamada copia de seguridad en caliente, una copia de seguridad en línea le permite crear una copia de seguridad de la base de datos sin apagarla.

Como parte de la copia de seguridad en línea, puede crear una copia de seguridad de los siguientes archivos:

- Solo archivos de datos y archivos de control
- Solo archivar archivos de registro (la base de datos no pasa al modo de copia de seguridad en este escenario)
- Base de datos completa que incluye archivos de datos, archivos de control y archivos de registro de archivo

Copia de seguridad sin conexión

Una copia de seguridad creada cuando la base de datos está en un estado montado o apagado se denomina copia de seguridad sin conexión. Una copia de seguridad fuera de línea también se denomina copia de seguridad en frío. Puede incluir únicamente archivos de datos y archivos de control en las copias de seguridad sin conexión. Puede crear una copia de seguridad de montaje sin conexión o de apagado sin conexión.

- Al crear una copia de seguridad de montaje sin conexión, debe asegurarse de que la base de datos esté en un estado montado.

Si la base de datos está en cualquier otro estado, la operación de copia de seguridad falla.

- Al crear una copia de seguridad de apagado sin conexión, la base de datos puede estar en cualquier estado.

El estado de la base de datos se cambia al estado requerido para crear una copia de seguridad. Después de crear la copia de seguridad, el estado de la base de datos vuelve al estado original.

Cómo SnapCenter descubre bases de datos de Oracle

Los recursos son bases de datos Oracle en el host que mantiene SnapCenter. Puede agregar estas bases de datos a grupos de recursos para realizar operaciones de protección de datos después de descubrir las bases de datos que están disponibles.

Las siguientes secciones describen el proceso que SnapCenter utiliza para descubrir diferentes tipos y versiones de bases de datos de Oracle.

Para las versiones de Oracle 11g a 12cR1

Base de datos RAC

Las bases de datos RAC se descubren únicamente en función de las entradas de `/etc/oratab`. Debes tener las entradas de la base de datos en el archivo `/etc/oratab`.

Autónomo

Las bases de datos independientes se descubren únicamente sobre la base de las entradas `/etc/oratab`.

ASM

La entrada de la instancia de ASM debe estar disponible en el archivo `/etc/oratab`.

RAC Un Nodo

Las bases de datos de RAC One Node se descubren únicamente en función de las entradas `/etc/oratab`. Las bases de datos deben estar en estado `nomount`, `mount` o `open`. Debes 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 renombrado o eliminado si la base de datos ya está descubierta y hay copias de seguridad asociadas con ella.

Debe realizar los siguientes pasos si se reubica la base de datos:

1. Agregue manualmente la entrada de base de datos reubicada en el archivo `/etc/oratab` en el nodo RAC conmutado por error.
2. Actualizar manualmente los recursos.
3. Seleccione la base de datos RAC One Node desde la página de recursos y luego haga clic en Configuración de la base de datos.
4. Configure la base de datos para establecer los nodos de clúster preferidos en el nodo RAC que actualmente aloja la base de datos.
5. Realizar las operaciones de SnapCenter .
6. Si ha reubicado una base de datos de un nodo a otro y la entrada `oratab` en el nodo anterior no se elimina, elimine manualmente la entrada `oratab` para evitar que la misma base de datos se muestre dos veces.

Para las versiones de Oracle 12cR2 a 18c, 19c o 21c

Base de datos RAC

Las bases de datos RAC se descubren mediante el comando `srvctl config`. Debes tener las entradas de la base de datos en el archivo `/etc/oratab`.

Autónomo

Las bases de datos independientes se descubren en función de las entradas en el archivo `/etc/oratab` y la salida del comando `srvctl config`.

ASM

La entrada de la instancia de ASM no necesita estar en el archivo `/etc/oratab`.

RAC Un Nodo

Las bases de datos de RAC One Node se descubren utilizando únicamente 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 renombrado o eliminado si la base de datos ya está descubierta y hay copias de seguridad asociadas con ella.

Debe realizar los siguientes pasos si se reubica la base de datos: . Actualizar manualmente los recursos. . Seleccione la base de datos RAC One Node desde la página de recursos y luego haga clic en Configuración de la base de datos. . Configure la base de datos para establecer los nodos de clúster preferidos en el nodo RAC que actualmente aloja la base de datos. . Realizar las operaciones de SnapCenter .



Si hay entradas de base de datos Oracle 12cR2 y 18c en el archivo `/etc/oratab` y la misma base de datos está registrada con el comando `srvctl config`, SnapCenter eliminará las entradas de base de datos duplicadas. Si hay entradas obsoletas en la base de datos, se descubrirá la base de datos, pero no se podrá acceder a ella y el estado será fuera de línea.

Nodos preferidos en la configuración de RAC

En la configuración de Oracle Real Application Clusters (RAC), puede especificar los nodos preferidos que SnapCenter utiliza para realizar la operación de copia de seguridad. Si no especifica el nodo preferido, SnapCenter asigna automáticamente un nodo como preferido y se crea una copia de seguridad en ese nodo.

Los nodos preferidos podrían ser uno o todos los nodos del clúster donde están presentes las instancias de la base de datos RAC. La operación de copia de seguridad se activa solo en estos nodos preferidos en el orden de preferencia.

Ejemplo

La base de datos RAC `cdbrac` tiene tres instancias: `cdbrac1` en el `nodo1`, `cdbrac2` en el `nodo2` y `cdbrac3` en el `nodo3`.

Las instancias `node1` y `node2` están configuradas para ser los nodos preferidos, con `node2` como la primera preferencia y `node1` como la segunda preferencia. Cuando se realiza una operación de copia de seguridad, la operación se intenta primero en el `nodo 2` porque es el primer nodo preferido.

Si el `nodo 2` no está en estado de realizar una copia de seguridad, lo que podría deberse a varias razones, como que el agente del complemento no se está ejecutando en el `host`, la instancia de la base de datos en el `host` no está en el estado requerido para el tipo de copia de seguridad especificado o la instancia de la base de datos en el `nodo 2` en una configuración FlexASM no está siendo atendida por la instancia de ASM local; entonces se intentará la operación en el `nodo 1`.

El `nodo3` no se utilizará para la copia de seguridad porque no está en la lista de nodos preferidos.

Configuración de Flex ASM

En una configuración Flex ASM, los nodos Leaf no aparecerán como nodos preferidos si la cardinalidad es menor que la cantidad de nodos en el clúster RAC. Si hay algún cambio en los roles de los nodos del clúster Flex ASM, debe descubrirlo manualmente para que se actualicen los nodos preferidos.

Estado de la base de datos requerido

Las instancias de la base de datos RAC en los nodos preferidos deben estar en el estado requerido para que la copia de seguridad finalice correctamente:

- Una de las instancias de la base de datos RAC en los nodos preferidos configurados debe estar en estado abierto para crear una copia de seguridad en línea.
- Una de las instancias de la base de datos RAC en los nodos preferidos configurados debe estar en el estado de montaje, y todas las demás instancias, incluidos otros nodos preferidos, deben estar en el estado de montaje o inferior para crear una copia de seguridad de montaje sin conexión.
- Las instancias de base de datos RAC pueden estar en cualquier estado, pero debe especificar los nodos preferidos para crear una copia de seguridad de apagado sin conexión.

Cómo catalogar copias de seguridad con Oracle Recovery Manager

Puede catalogar las copias de seguridad de las bases de datos Oracle utilizando Oracle Recovery Manager (RMAN) para almacenar la información de copia de seguridad en el repositorio Oracle RMAN.

Las copias de seguridad catalogadas se pueden utilizar más adelante para operaciones de restauración a nivel de bloque o de recuperación de puntos en el tiempo del espacio de tabla. Cuando no necesite estas copias de seguridad catalogadas, puede eliminar la información del catálogo.

La base de datos debe estar montada o en un estado superior para poder catalogar. Puede realizar la catalogación de copias de seguridad de datos, copias de seguridad de registros de archivo y copias de seguridad completas. Si la catalogación está habilitada para una copia de seguridad de un grupo de recursos que tiene varias bases de datos, la catalogación se realiza para cada base de datos. Para las bases de datos Oracle RAC, la catalogación se realizará en el nodo preferido donde la base de datos esté al menos en estado montado.

Si desea catalogar copias de seguridad de una base de datos RAC, asegúrese de que no haya ningún otro trabajo en ejecución para esa base de datos. Si se está ejecutando otro trabajo, la operación de catalogación falla en lugar de ponerse 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 agregar una base de datos de catálogo externa, puede configurarla especificando la credencial y el nombre del sustrato de red transparente (TNS) del catálogo externo mediante el asistente de configuración de base de datos desde la interfaz gráfica de usuario (GUI) de SnapCenter . También puede configurar la base de datos del catálogo externo desde la CLI ejecutando el comando `Configure-SmOracleDatabase` con las opciones `-OracleRmanCatalogCredentialName` y `-OracleRmanCatalogTnsName`.

Comando RMAN

Si habilitó la opción de catalogación al crear una política de respaldo de Oracle desde la GUI de SnapCenter , los respaldos se catalogan utilizando Oracle RMAN como parte de la operación de respaldo. También puede realizar una catalogación diferida de copias de seguridad ejecutando el `Catalog-SmBackupWithOracleRMAN` dominio.

Después de catalogar las copias de seguridad, puede ejecutar el `Get-SmBackupDetails` comando para obtener la información de respaldo catalogada, como la etiqueta de los archivos de datos catalogados, la ruta del catálogo de archivos de control y las ubicaciones de los registros de archivo catalogados.

Formato de nombres

Si el nombre del grupo de discos ASM es mayor o igual a 16 caracteres, a partir de SnapCenter 3.0, el formato de nombre utilizado para la copia de seguridad es `SC_HASHCODEofDISKGROUP_DBSID_BACKUPID`. Sin embargo, si el nombre del grupo de discos tiene menos de 16 caracteres, el formato de nombre utilizado para la copia de seguridad es `DISKGROUPNAME_DBSID_BACKUPID`, que es el mismo formato utilizado en SnapCenter 2.0.

El `HASHCODEofDISKGROUP` es un número generado automáticamente (de 2 a 10 dígitos) único para cada grupo de discos ASM.

Operaciones de verificación cruzada

Puede realizar comprobaciones cruzadas para actualizar información obsoleta del repositorio RMAN sobre las copias de seguridad cuyos registros del repositorio no coinciden con su estado físico. Por ejemplo, si un usuario elimina registros archivados del disco con un comando del sistema operativo, el archivo de control aún indica que los registros están en el disco, cuando en realidad no es así.

La operación de verificación cruzada le permite actualizar el archivo de control con la información. Puede habilitar la verificación cruzada ejecutando el comando `Set-SmConfigSettings` y asignando el valor `TRUE` al parámetro `ENABLE_CROSSCHECK`. El valor predeterminado se establece en `FALSO`.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Eliminar información del catálogo

Puede eliminar la información del catálogo ejecutando el comando `Uncatalog-SmBackupWithOracleRMAN`. No es posible eliminar la información del catálogo mediante la GUI de SnapCenter. Sin embargo, la información de una copia de seguridad catalogada se elimina al eliminar la copia de seguridad o al eliminar el grupo de retención y recursos asociados con esa copia de seguridad catalogada.



Cuando se fuerza la eliminación del host de SnapCenter, la información de las copias de seguridad catalogadas asociadas con ese host no se elimina. Debe eliminar la información de todas las copias de seguridad catalogadas para ese host antes de forzar la eliminación del host.

Si la catalogación y descatalogación falla porque el tiempo de operación excedió el valor de tiempo de espera especificado para 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 el servicio SnapCenter Plug-in Loader (SPL) ejecutando 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 prescript y postscript específicos de copia de seguridad

SnapCenter le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript mientras crea políticas de respaldo. Esta funcionalidad es compatible con todas las configuraciones de Oracle excepto VMDK.

SnapCenter predefine los valores de los parámetros que serán directamente accesibles en el entorno donde 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 respaldo

- **SC_JOB_ID** especifica el ID del trabajo de la operación.

Ejemplo: 256

- **SC_ORACLE_SID** especifica el identificador del sistema de la base de datos.

Si la operación involucra múltiples bases de datos, el parámetro contendrá los nombres de las bases de datos separados por barras verticales.

Este parámetro se completará para los volúmenes de la aplicación.

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 en el que se realiza la copia de seguridad.

Este parámetro se completará para los volúmenes de la aplicación.

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 del sistema operativo 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 (completa en línea, datos en línea, registro en línea, apagado sin conexión, montaje sin conexión)

Ejemplos:

- Para una copia de seguridad completa: ONLINEFULL
- copia de seguridad de solo datos: ONLINEDATA
- Solo para copia de seguridad de registros: ONLINELOG

- **SC_BACKUP_NAME** especifica el nombre de la copia de seguridad.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplo: DATOS@RG2_scspr2417819002_20-07-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_20-07-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_20-07-2021_12.16.48.9267

- **SC_BACKUP_ID** especifica el ID de la copia de seguridad.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplo: DATOS@203|LOG@205|AV@207

- **SC_ORACLE_HOME** especifica la ruta del directorio de inicio 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 política.

Ejemplos:

- Para una copia de seguridad completa: Cada hora | DATOS @ DÍAS: 3 | REGISTRO @ RECuento: 4
- Solo para copias de seguridad de datos bajo demanda: Ondemand|DATA@COUNT:2
- Para copias de seguridad de registros solo a pedido: 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 padre para luns 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:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- Para una única base de datos con archivos de datos distribuidos en varios volúmenes:
buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_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 padre para luns y qtrees.

Ejemplos:

- Para una sola instancia de base de datos: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- Para múltiples instancias de base de datos:
NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_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 sola instancia de base de datos:
buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Para varias instancias de base de datos:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1

- **SC_PRIMARY_SNAPSHOT_NAMES** especifica los nombres de las instantáneas principales creadas durante la copia de seguridad.

Ejemplos:

- Para una sola instancia de base de datos: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Para varias instancias de base 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_scspr2417819002_07-21-2021_02.28.26.3973_1
- Para mantener la coherencia, el grupo de instantáneas que involucra 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 padre inmediato del archivo respaldado. Para una configuración ASM, es el nombre del grupo de discos.

Los datos se formatearán como

<db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

Ejemplos:

- Para una sola instancia de base de datos: /mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
- Para múltiples instancias de base de datos:
NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_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 sola instancia de 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 múltiples instancias de base de datos: NFSB32@RG2_scspr2417819002_21-07-2021_02.28.26.3973_0:/mnt/nfsb32_data, RG2_scspr2417819002_21-07-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_21-07-2021_02.28.26.3973_0:/mnt/nfsb31_data, RG2_scspr2417819002_21-07-2021_02.28.26.3973_1:/mnt/nfsb32_log

- **SC_ARCHIVELOGS_LOCATIONS** especifica la ubicación del directorio de registros de archivo.

Los nombres de directorio serán el padre inmediato de los archivos de registro de archivo. Si los registros de archivo se colocan en más de una ubicación, se capturarán todas las ubicaciones. Esto también incluye los escenarios FRA. Si se utilizan enlaces suaves para el directorio, se completarán los mismos.

Ejemplos:

- Para una sola base de datos en NFS: /mnt/nfsdb2_log
- Para múltiples bases de datos en NFS y para los registros de archivo de base de datos NFSB31 que se ubican 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 de registros de rehacer.

Los nombres de directorio serán el padre inmediato de los archivos de registro de rehacer. Si se utilizan enlaces suaves para el directorio, se completarán los mismos.

Ejemplos:

- Para una única base de datos en NFS: /mnt/nfsdb2_data/newdb1
- Para múltiples bases de datos en NFS:
NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
- Para ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** especifica la ubicación del directorio de archivos de control.

Los nombres de directorio serán el padre inmediato de los archivos de control. Si se utilizan enlaces suaves para el directorio, se completarán los mismos.

Ejemplos:

- Para una sola base de datos en NFS: /mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
- Para múltiples bases de datos en NFS:
NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_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 padre inmediato de los archivos de datos. Si se utilizan enlaces suaves para el directorio, se completarán los mismos.

Ejemplos:

- Para una sola base de datos en NFS: /mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
- Para múltiples bases de datos en NFS:

NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile

- Para ASM: +DATA2DG/ASMDB2/ARCHIVO DE DATOS,+DATA2DG/ASMDB2/ARCHIVO TEMPORAL

- **SC_SNAPSHOT_LABEL** especifica el nombre de las etiquetas secundarias.

Ejemplos: Por hora, por día, por semana, por mes o etiqueta personalizada.

Delimitadores admitidos

- **:** se utiliza para separar el nombre de SVM y el nombre del volumen

Ejemplo: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1

- **@** se utiliza para separar los datos de su nombre de base de datos y para separar el valor de su clave.

Ejemplos:

- NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1
- 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:

- DATOS@203|REGISTRO@205
- Cada hora|DATOS@DÍAS:3|REGISTRO@CONTADOR:4
- DATOS@RG2_scspr2417819002_20-07-2021_12.16.48.9267_0|REGISTRO@RG2_scspr2417819002_20-07-2021_12.16.48.9267_1

- **/** se utiliza para separar el nombre del volumen de su instantánea para los parámetros SC_PRIMARY_SNAPSHOT_NAMES y SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

Ejemplo: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1

- **,** se utiliza para separar conjuntos de variables para la misma base de datos.

Ejemplo: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_21-07-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_21-07-2021_02.28.26.3973_1

Opciones de retención de copias de seguridad

Puede elegir la cantidad de días durante los cuales desea conservar copias de seguridad o especificar la cantidad de copias de seguridad que desea conservar, hasta un máximo de 255 copias en ONTAP . Por ejemplo, su organización podría exigirle que conserve 10 días de copias de seguridad o 130 copias de seguridad.

Al crear una política, puede especificar las opciones de retención para el tipo de copia de seguridad y el tipo de programación.

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

SnapCenter elimina las copias de seguridad retenidas que tienen etiquetas de retención que coinciden con el tipo de programación. Si se modificó el tipo de programación del recurso o del grupo de recursos, es posible que las copias de seguridad con la etiqueta del tipo de programación anterior aún permanezcan en el sistema.



Para la retención a largo plazo de copias de seguridad, debe utilizar la copia de seguridad SnapVault .

Programaciones de copias de seguridad

La frecuencia de copia de seguridad (tipo de programación) se especifica en las políticas; una programación de copia de seguridad se especifica en la configuración del grupo de recursos. El factor más crítico a la hora de determinar la frecuencia o el cronograma de una copia de seguridad es la tasa de cambio del recurso y la importancia de los datos. Es posible que haga una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que haga una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su Acuerdo de Nivel de Servicio (SLA) y su Objetivo de Punto de Recuperación (RPO).

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso para un recurso muy utilizado, no es necesario ejecutar una copia de seguridad completa más de una o dos veces al día. Por ejemplo, las copias de seguridad periódicas del registro de transacciones podrían ser suficientes para garantizar que tenga las copias de seguridad que necesita. Cuanto más a menudo realice copias de seguridad de sus bases de datos, menos registros de transacciones tendrá que utilizar SnapCenter en el momento de la restauración, lo que puede generar operaciones de restauración más rápidas.

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de respaldo

La frecuencia de las copias de seguridad (con qué frecuencia se deben realizar las copias de seguridad), denominada *tipo de programación* para algunos complementos, es parte de una configuración de políticas. Puede seleccionar la frecuencia de respaldo para la política: horaria, diaria, semanal o mensual. Si no

selecciona ninguna de estas frecuencias, la política creada será solo a pedido. Puede acceder a las políticas haciendo clic en **Configuración > Políticas**.

- Programaciones de copias de seguridad

Las programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad) son parte de la configuración de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para realizar copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos > Grupos de recursos**.

Convenciones de nombres de copias de seguridad

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

```
resourcegroupname_hostname_timestamp
```

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, `customtext_resourcegroup_policy_hostname` o `resourcegroup_hostname`. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Requisitos para realizar una copia de seguridad de una base de datos Oracle

Antes de realizar una copia de seguridad de una base de datos de Oracle, debe asegurarse de que se cumplan los requisitos previos.

- Debe haber creado un grupo de recursos con una política adjunta.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.
- Debe haber asignado el agregado que utiliza la operación de respaldo a la máquina virtual de almacenamiento (SVM) utilizada por la base de datos.

- Debería haber verificado que todos los volúmenes de datos y volúmenes de registro de archivo que pertenecen a la base de datos estén protegidos si la protección secundaria está habilitada para esa base de datos.
- Debería haber verificado que la base de datos que tiene archivos en los grupos de discos ASM esté en estado "MOUNT" o "OPEN" para verificar sus copias de seguridad utilizando la utilidad Oracle DBVERIFY.
- Deberías haber verificado que la longitud del punto de montaje del volumen no exceda los 240 caracteres.
- Debe aumentar el valor de RESTTimeout a 86400000 ms en el archivo *C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config* en el host del servidor SnapCenter, si la base de datos de la que se está realizando una copia de seguridad es grande (tamaño en TB).

Al modificar los valores, asegúrese de que no haya trabajos en ejecución y reinicie el servicio SnapCenter SMCORE después de aumentar el valor.

Descubra las bases de datos Oracle disponibles para realizar copias de seguridad

Los recursos son bases de datos Oracle en el host que son administradas por SnapCenter. Puede agregar estas bases de datos a grupos de recursos para realizar operaciones de protección de datos después de descubrir las bases de datos que están disponibles.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter, agregar hosts, crear conexiones del sistema de almacenamiento y agregar credenciales.
- Si las bases de datos residen en un disco de máquina virtual (VMDK) o en una asignación de dispositivos sin procesar (RDM), debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter.

Para obtener más información, consulte ["Implementar el SnapCenter Plug-in for VMware vSphere"](#).

- Si las bases de datos residen en un sistema de archivos VMDK, debe haber iniciado sesión en vCenter y haber navegado a **Opciones de VM > Avanzado > Editar configuración** para establecer el valor de *disk.enableUUID* en verdadero para la VM.
- Debes haber revisado el proceso que sigue SnapCenter para descubrir diferentes tipos y versiones de bases de datos de Oracle.

Paso 1: Evitar que SnapCenter detecte entradas que no sean de la base de datos

Puede evitar que SnapCenter descubra entradas que no sean de base de datos agregadas en el archivo *oratab*.

Pasos

1. Después de instalar el complemento para Oracle, el usuario root debe crear el archivo **sc_oratab.config** en el directorio */var/opt/snapcenter/sco/etc/*.

Otorgue permiso de escritura al propietario y al grupo del binario de Oracle para que el archivo pueda mantenerse en el futuro.

2. El administrador de la base de datos debe agregar las entradas que no son de 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 simplemente agregar la cadena de entidad que no es de base de datos.



La cadena distingue entre mayúsculas y minúsculas. Cualquier texto con `#` al principio se trata como un comentario. El comentario se puede agregar después del nombre que no pertenece a 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. Descubra los recursos.

Las entradas que no sean de base de datos agregadas en `sc_oratab.config` no aparecerán en la página Recursos.



Siempre se recomienda realizar una copia de seguridad del archivo `sc_oratab.config` antes de actualizar el complemento SnapCenter .

Paso 2: Descubrir recursos

Después de instalar el complemento, todas las bases de datos de ese host se descubren automáticamente y se muestran en la página Recursos.

Las bases de datos deben estar al menos en el estado montado o superior para que el descubrimiento de las bases de datos sea exitoso. En un entorno de Oracle Real Application Clusters (RAC), la instancia de base de datos de RAC en el host donde se realiza el descubrimiento debe estar al menos en el estado montado o superior para que el descubrimiento de la instancia de base de datos sea exitoso. Sólo las bases de datos que se descubren correctamente se pueden agregar a los grupos de recursos.

Si ha eliminado una base de datos Oracle en el host, SnapCenter Server no lo sabrá y mostrará 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista **Ver**.

Hacer clic  icono de filtro] y, a continuación, seleccione el nombre del host y el tipo de base de datos para filtrar los recursos. Luego puede hacer clic en el `icono imagfilter_icon.gif[filter icon]_icon.png[]` para

cerrar el panel de filtro.

3. Haga clic en **Actualizar recursos**.

En un escenario de RAC One Node, la base de datos se descubre como la base de datos RAC en el nodo donde está alojada actualmente.

Resultados

Las bases de datos se muestran junto con información como el tipo de base de datos, el nombre del host o clúster, los grupos de recursos y políticas asociados, y el estado.



Debe 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 que no es NetApp, la interfaz de usuario muestra un mensaje No disponible para respaldo en la columna Estado general.

No se pueden realizar operaciones de protección de datos en una base de datos que se encuentra en un sistema de almacenamiento que no sea NetApp.

- Si la base de datos está en un sistema de almacenamiento NetApp y no está protegida, la interfaz de usuario muestra un mensaje No protegido en la columna Estado general.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, la interfaz de usuario muestra un mensaje Disponible para respaldo en la columna Estado general.



Si ha habilitado una autenticación de base de datos Oracle, se muestra un ícono de candado rojo en la vista de recursos. Debe configurar las credenciales de la base de datos para poder proteger la base de datos o agregarla al grupo de recursos para realizar operaciones de protección de datos.

Crear políticas de respaldo para bases de datos de Oracle

Antes de utilizar SnapCenter para realizar copias de seguridad de los recursos de base de datos de Oracle, debe crear una política de copia de seguridad para el recurso o el grupo de recursos que desea respaldar. Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad. También puede especificar la configuración de replicación, script y tipo de copia de seguridad. La creación de una política ahorra tiempo cuando desea reutilizarla en otro recurso o grupo de recursos.

Antes de empezar

- Debes haber definido tu estrategia de backup.
- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, descubrir bases de datos y crear conexiones del sistema de almacenamiento.
- Si está replicando instantáneas en un espejo o almacenamiento secundario de bóveda, el administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino.
- Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios prescript y postscript.

- Revise los requisitos previos y las limitaciones específicos de la sincronización activa de SnapMirror . Para obtener información, consulte ["Límites de objetos para la sincronización activa de SnapMirror"](#) .

Acerca de esta tarea

Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.

+ Especificar un período de bloqueo de instantáneas evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas que la cantidad especificada 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Seleccione **Oracle Database** de la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Nombre, ingrese el nombre y los detalles de la política.
6. En la página Tipo de política, realice los siguientes pasos:

a. Seleccione su tipo de almacenamiento.

b. Seleccione el alcance de la política:

- Si desea **crear una copia de seguridad en línea**, seleccione **Copia de seguridad en línea**.

Debe especificar si desea realizar una copia de seguridad de todos los archivos de datos, archivos de control y archivos de registro de archivo, solo de los archivos de datos y archivos de control, o solo de los archivos de registro de archivo.

- 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 esté en estado montado, seleccione **Montar**.
- Si desea crear una copia de seguridad de apagado sin conexión cambiando la base de datos al estado de apagado, seleccione **Apagado**.

Si tiene bases de datos conectables (PDB) y desea guardar el estado de las PDB antes de crear la copia de seguridad, debe seleccionar **Guardar estado de las PDB**. Esto le permite llevar los PDB a su estado original después de crear la copia de seguridad.

- c. Si desea catalogar la copia de seguridad mediante Oracle Recovery Manager (RMAN), seleccione **Catalogar copia de seguridad con Oracle Recovery Manager (RMAN)**.

Puede realizar la catalogación diferida para una copia de seguridad a la vez utilizando la GUI o el comando CLI de SnapCenter Catalog-SmBackupWithOracleRMAN.



Si desea catalogar copias de seguridad de una base de datos RAC, asegúrese de que no haya ningún otro trabajo en ejecución para esa base de datos. Si se está ejecutando otro trabajo, la operación de catalogación falla en lugar de ponerse en cola.

d. Si desea podar registros de archivo después de la copia de seguridad, seleccione **Podar registros de archivo después de la copia de seguridad**.



Se omitirá la poda de registros de archivo del destino de registro de archivo que no esté configurado en la base de datos.



Si utiliza Oracle Standard Edition, puede utilizar los parámetros LOG_ARCHIVE_DEST y LOG_ARCHIVE_DUPLEX_DEST al realizar la copia de seguridad del registro de archivo.

- Puede eliminar registros de archivo solo si ha seleccionado los archivos de registro de archivo como parte de su copia de seguridad.



Debe asegurarse de que todos los nodos en un entorno RAC puedan acceder a todas las ubicaciones del registro de archivo para que la operación de eliminación sea exitosa.

Si quieres...	Entonces...
Eliminar todos los registros de archivo	Seleccione Eliminar todos los registros de archivo .
Eliminar registros de archivo que sean más antiguos	Seleccione Eliminar registros de archivo anteriores a y, a continuación, especifique la antigüedad de los registros de archivo que se eliminarán en días y horas.
Eliminar registros de archivo de todos los destinos	Seleccione Eliminar registros de archivo de todos los destinos .
Eliminar los registros de archivo de los destinos de registro que forman parte de la copia de seguridad	Seleccione Eliminar registros de archivo de los destinos que forman parte de la copia de seguridad .

+



Prune archive logs after backup

Prune log retention setting

☐ Delete all archive logs

☒ Delete archive logs older than

Prune log destination setting

☐ Delete archive logs from all the destinations

☒ Delete archive logs from the destinations which are part of backup

7. En la página Instantánea y replicación, realice los siguientes pasos:

- a. Especifique la frecuencia de programación seleccionando **A pedido**, **Cada hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.



Puede especificar la programación (fecha de inicio y fecha de finalización) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

- a. En la sección Configuración de retención de instantáneas de datos, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página Tipo de copia de seguridad:

Si quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.  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 subyacente de ONTAP .  Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva en el destino.
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 Configuración de retención de instantáneas del registro de archivo, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página Tipo de copia de seguridad:

Si quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.  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 subyacente de ONTAP .  Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva en el destino.
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 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.

8. En la sección Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:



Debe seleccionar las opciones de replicación secundaria para que el **Período de bloqueo de copia de instantánea secundaria** sea efectivo.

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una instantánea local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Esta opción debe estar habilitada para la sincronización activa de SnapMirror . Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP.

Para este campo...	Haz esto...
Actualizar SnapVault después de crear una instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault). Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón Actualizar en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre SnapLock Vault, consulte "Confirmar copias de instantáneas en WORM en un destino de bóveda" Ver "Ver copias de seguridad y clones de bases de datos de Oracle en la página Topología" .
Recuento de reintentos de error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

9. En la página Script, ingrese la ruta y los argumentos del prescript o postscript que desea ejecutar antes o después de la operación de respaldo, respectivamente.

Debes almacenar los prescripts y posscripts en `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha creado alguna carpeta dentro de esta ruta 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 le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript. ["Más información"](#)

10. En la página de Verificación, realice los siguientes pasos:

- a. Seleccione la programación de copia de seguridad para la que desea realizar la operación de verificación.
- b. En la sección Comandos de script de verificación, ingrese la ruta y los argumentos del script prescript o postscript que desea ejecutar antes o después de la operación de verificación, respectivamente.

Debes almacenar los prescripts y posscripts en `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha creado alguna carpeta dentro de esta ruta 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.

11. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas para bases de datos de Oracle

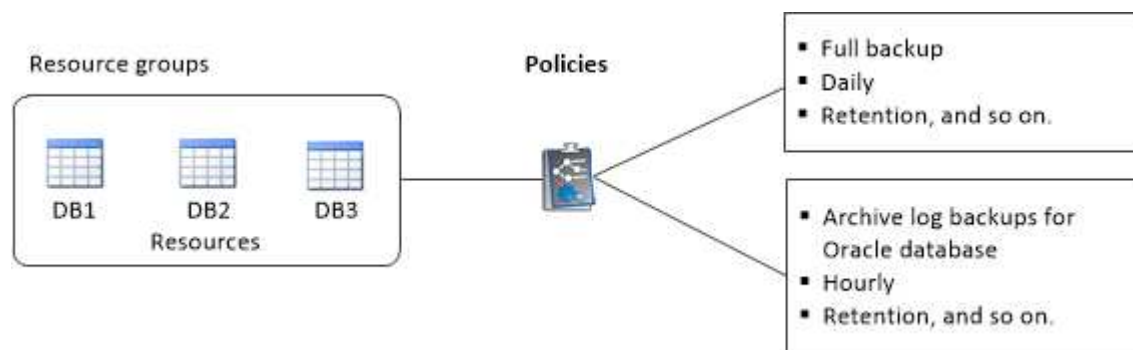
Un grupo de recursos es un contenedor donde se agregan recursos que desea respaldar y proteger. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados a una aplicación determinada simultáneamente.

Acerca de esta tarea

- Una base de datos con archivos en grupos de discos ASM debe estar en estado "MONTAR" o "ABIERTO" para verificar sus copias de seguridad mediante la utilidad Oracle DBVERIFY.

Adjunte una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

La siguiente imagen ilustra la relación entre recursos, grupos de recursos y políticas para bases de datos:



- Para las políticas habilitadas para SnapLock , para ONTAP 9.12.1 y versiones anteriores, si especifica un período de bloqueo de instantáneas, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de vencimiento de SnapLock . El administrador de almacenamiento debe limpiar manualmente los clones después del tiempo de vencimiento de SnapLock .
- No se admite agregar nuevas bases de datos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror .
- No se admite agregar nuevas bases de datos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror . Puede agregar recursos al grupo de recursos solo en estado normal o de conmutación por recuperación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más

adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



Debe utilizar exactamente el mismo destino que se configuró en Oracle, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione un nombre de host de base de datos Oracle de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.



Puede agregar bases de datos de hosts Linux y AIX en un solo grupo de recursos.

6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.

- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. En la página de Verificación, realice los siguientes pasos:

- a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
- b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
- c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

10. Revise el resumen y luego haga clic en **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos de Oracle en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene

habilitada la capacidad **SecondaryProtection**.

- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:

- a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:

- a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
- b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
- c. En el cuadro de diálogo Agregar programaciones de verificación *policy_name*, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema

de almacenamiento secundario.

e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Realizar copias de seguridad de los recursos de Oracle

Si un recurso no forma parte de ningún grupo de recursos, puedes realizar una copia de seguridad del recurso desde la página Recursos.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista Ver.
3. Hacer clic  y luego seleccione el nombre del host y el tipo de base de datos para filtrar los recursos.

Luego puedes hacer clic  para cerrar el panel de filtro.

4. Seleccione la base de datos que desea respaldar.

Se muestra la página Proteger base de datos.

5. En la página Recursos, realice los siguientes pasos:
 - a. Seleccione la casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, `customtext_policy_hostname` o `resource_hostname`. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- b. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.

6. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.

Puede crear una política haciendo clic en .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b.

Hacer clic  en la columna Configurar programaciones para configurar una programación para la política que desee.

- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione OK .

policy_name es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Verificación, realice los siguientes pasos:

- a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para verificar el almacenamiento secundario.

- b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política. + En el cuadro de diálogo Agregar programaciones de verificación *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 de la lista desplegable.



En una configuración de Flex ASM, no se puede realizar una operación de verificación en los nodos Leaf si la cardinalidad es menor que la cantidad de nodos en el clúster RAC.

- e. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el almacenamiento secundario.

- f. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

8. En la página de Notificación, seleccione los escenarios en los que desea enviar los correos electrónicos desde la lista desplegable **Preferencia de correo electrónico**.

Debe especificar las direcciones de correo electrónico del remitente y del destinatario, así como el asunto del correo electrónico. Si desea adjuntar el informe de la operación de respaldo realizada en el recurso, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell. `Set-SmSmtServer` .

9. Revise el resumen y luego haga clic en **Finalizar**.

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

10. Haga clic en **Hacer copia de seguridad ahora**.

11. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si ha aplicado varias políticas al recurso, en la lista desplegable Política, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación

de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

Después de terminar

- En la configuración de AIX, puede utilizar el `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 hizo una copia de seguridad.

Bloquear o cambiar el nombre de los dispositivos no afectará la operación de restauración cuando restaure utilizando esa copia de seguridad.

- Si la operación de copia de seguridad falla porque el tiempo de ejecución de la consulta de la base de datos excedió el valor de tiempo de espera, debe cambiar el valor de los parámetros `ORACLE_SQL_QUERY_TIMEOUT` y `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` ejecutando el comando `Set-SmConfigSettings cmdlet`:

Después de modificar el valor de los parámetros, reinicie el servicio SnapCenter Plug-in Loader (SPL) ejecutando el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si el archivo no es accesible y el punto de montaje no está disponible durante el proceso de verificación, la operación podría fallar con el código de error DBV-00100 del archivo especificado. 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 el servicio SnapCenter Plug-in Loader (SPL) ejecutando el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- En configuraciones de MetroCluster , es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.
- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar.

Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese guión, el `do_start method` El comando inicia el servicio del complemento VMware de SnapCenter . Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

Encuentra más información

- ["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)
- ["La base de datos Oracle RAC One Node se omite para realizar operaciones de SnapCenter"](#)
- ["No se pudo cambiar el estado de una base de datos Oracle 12c ASM"](#)
- ["Parámetros personalizables para operaciones de copia de seguridad, restauración y clonación en sistemas AIX"](#)(Requiere iniciar sesión)

Realizar copias de seguridad de los grupos de recursos de bases de datos de Oracle

Un grupo de recursos es una colección de recursos en un host o clúster. La operación de copia de seguridad se realiza en todos los recursos definidos en el grupo de recursos.

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se crean de acuerdo con la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
3. Ingrese el nombre del grupo de recursos en el cuadro de búsqueda o haga clic en  y seleccione la etiqueta.

Hacer clic  para cerrar el panel de filtro.

4. En la página Grupo de recursos, seleccione el grupo de recursos que desea respaldar.



Si tiene un grupo de recursos federado con dos bases de datos y una tiene datos en un almacenamiento que no es de NetApp, la operación de respaldo se cancela incluso si la otra base de datos está en un almacenamiento de NetApp.

5. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si tiene varias políticas asociadas con el grupo de recursos, seleccione la política de respaldo que desea utilizar en la lista desplegable **Política**.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

- b. Seleccione **Copia de seguridad**.
6. Supervise el progreso seleccionando **Monitor > Trabajos**.

Después de terminar

- En la configuración de AIX, puede utilizar el `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 hizo una copia de seguridad.

Bloquear o cambiar el nombre de los dispositivos no afectará la operación de restauración cuando restaure utilizando esa copia de seguridad.

- Si la operación de copia de seguridad falla porque el tiempo de ejecución de la consulta de la base de datos excedió el valor de tiempo de espera, debe cambiar el valor de los parámetros `ORACLE_SQL_QUERY_TIMEOUT` y `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` ejecutando el comando `Set-SmConfigSettings cmdlet`:

Después de modificar el valor de los parámetros, reinicie el servicio SnapCenter Plug-in Loader (SPL) ejecutando el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si el archivo no es accesible y el punto de montaje no está disponible durante el proceso de verificación, la operación podría fallar con el código de error DBV-00100 del archivo especificado. 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 el servicio SnapCenter Plug-in Loader (SPL) ejecutando el siguiente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

Supervisar la copia de seguridad de la base de datos Oracle

Aprenda a supervisar el progreso de las operaciones de respaldo y de protección de datos.

Supervisar las operaciones de copia de seguridad de la base de datos Oracle

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desee verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 respaldo

Realizar copias de seguridad de bases de datos Oracle mediante comandos UNIX

El flujo de trabajo de respaldo incluye la planificación, la identificación de los recursos para el respaldo, la creación de políticas de respaldo, la creación de grupos de recursos y la asociación de políticas, la creación de respaldos y la supervisión de las operaciones.

Lo que necesitarás

- Debería haber agregado las conexiones del sistema de almacenamiento y creado la credencial utilizando los comandos *Add-SmStorageConnection* y *Add-SmCredential*.
- Debería haber establecido la sesión de conexión con el servidor SnapCenter mediante el comando *Open-SmConnection*.

Solo puede tener una sesión de inicio de sesión de cuenta de SnapCenter y el token se almacena en el directorio de inicio del usuario.



La sesión de conexión es válida sólo por 24 horas. Sin embargo, puedes crear un token con la opción *TokenNeverExpires* para crear un token que nunca caduque y la sesión siempre será válida.

Acerca de esta tarea

Debe ejecutar los siguientes comandos para establecer la conexión con el servidor SnapCenter , descubrir las instancias de la base de datos Oracle, agregar la política y el grupo de recursos, realizar una copia de seguridad y verificar la copia de seguridad.

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. Iniciar una sesión de conexión con el servidor SnapCenter para un usuario específico: *Open-SmConnection*

2. Realizar la operación de descubrimiento de recursos del host: *Get-SmResources*
3. Configure las credenciales de la base de datos Oracle y los nodos preferidos para la operación de respaldo de una base de datos de Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Crear una política de respaldo: *Add-SmPolicy*
5. Recupere la información sobre la ubicación de almacenamiento secundaria (SnapVault o SnapMirror): *Get-SmSecondaryDetails*

Este comando recupera los detalles de mapeo de almacenamiento primario a secundario de un recurso especificado. Puede utilizar los detalles de mapeo para configurar los ajustes de verificación secundaria mientras crea un grupo de recursos de respaldo.

6. Agregar un grupo de recursos a SnapCenter: *Add-SmResourceGroup*
7. Crear una copia de seguridad: *New-SmBackup*

Puede sondear el trabajo utilizando la opción *WaitForCompletion*. Si se especifica esta opción, el comando continúa sondeando el servidor hasta que se complete el trabajo de copia de seguridad.

8. Recuperar los registros de SnapCenter: *Get-SmLogs*

Cancelar operaciones de copia de seguridad de bases de datos Oracle

Puede cancelar operaciones de copia de seguridad que estén en ejecución, en cola o que no respondan.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones de respaldo.

Acerca de esta tarea

Cuando se cancela una operación de copia de seguridad, el servidor SnapCenter detiene la operación y elimina todas las instantáneas del almacenamiento si la copia de seguridad creada no está registrada en el servidor SnapCenter. Si la copia de seguridad ya está registrada en SnapCenter Server, no revertirá la instantánea ya creada incluso después de que se active la cancelación.

- Puede cancelar únicamente las operaciones de registro o de copia de seguridad completa que estén en cola o en ejecución.
- No es posible cancelar la operación una vez iniciada la verificación.

Si cancela la operación antes de la verificación, la operación se cancelará y no se realizará la operación de verificación.

- No se puede cancelar la operación de copia de seguridad una vez iniciadas las operaciones del catálogo.
- Puede cancelar una operación de copia de seguridad desde la página Monitor o desde el panel Actividad.
- Además de utilizar la GUI de SnapCenter, puede utilizar comandos CLI para cancelar operaciones.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 2. Seleccione la operación y haga clic en Cancelar trabajo.
Panel de actividades	1. Después de iniciar el trabajo de respaldo, haga clic en  en el panel Actividad 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 vuelve al estado original.

Si la operación que canceló no responde en el estado de cancelación o ejecución, debe ejecutar `Cancel-SmJob -JobID <int> -Force` para detener a la fuerza la operación de respaldo.

Ver copias de seguridad y clones de bases de datos de Oracle en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario.

Acerca de esta tarea

En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .

La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), puede ver los siguientes íconos adicionales:

-  El sitio de réplica está activo.
-  El sitio de réplica está inactivo.
-  No se ha restablecido la relación de espejo secundario o bóveda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página Topología del recurso seleccionado.

4. Revise la tarjeta Resumen para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario y secundario.

La sección Tarjeta de resumen muestra el número total de copias de seguridad y clones y el número total de copias de seguridad 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración 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 respaldo de SnapCenter consultando a ONTAP los sitios principales y de réplica. Una programación semanal también realiza esta actividad para 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 Async Mirror o Async MirrorVault con el nuevo destino principal se deben configurar manualmente después de la conmutación por error. Desde ONTAP 9.15.1 en adelante, Async Mirror o Async MirrorVault se configura automáticamente en el nuevo destino principal.
- Después de la conmutación por error, se debe crear una copia de seguridad para que SnapCenter esté al tanto de la conmutación por error. Puede hacer clic en **Actualizar** sólo después de haber creado una copia de seguridad.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación, montaje, desmontaje, cambio de nombre, catalogación, descatalogación y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

- Si ha seleccionado una copia de seguridad de registros, solo podrá realizar operaciones de cambio de nombre, montaje, desmontaje, catalogación, descatalogación y eliminación.
- Si ha catalogado la copia de seguridad mediante Oracle Recovery Manager (RMAN), no podrá cambiar el nombre de esas copias de seguridad catalogadas.

7. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en .

Si el valor asignado a SnapmirrorStatusUpdateWaitTime es menor, las copias de seguridad de Mirror y Vault no aparecen en la página de topología, incluso si los volúmenes de datos y registros están protegidos correctamente. Debe aumentar el valor asignado a SnapmirrorStatusUpdateWaitTime mediante el cmdlet de PowerShell `Set-SmConfigSettings`.

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"](#) o ["Guía de referencia de cmdlets del software SnapCenter"](#).

Montar y desmontar copias de seguridad de bases de datos

Puede montar una o varias copias de seguridad de datos y registros únicamente si desea acceder a los archivos de la copia de seguridad. Puede montar la copia de seguridad en el mismo host donde se creó la copia de seguridad o en un host remoto que tenga el mismo tipo de Oracle y configuraciones de host. Si ha montado manualmente las copias de seguridad, deberá desmontarlas manualmente después de completar la operación. En cualquier caso, se puede montar una copia de seguridad de una base de datos en cualquiera de los hosts. Mientras realiza una operación, solo puede montar una única copia de seguridad.



En una configuración de Flex ASM, no se puede realizar una operación de montaje en nodos Leaf si la cardinalidad es menor que la cantidad de nodos en el clúster RAC.

Montar una copia de seguridad de la base de datos

Debe montar manualmente una copia de seguridad de la base de datos si desea acceder a los archivos de la copia de seguridad.

Lo que necesitarás

- Si tiene una instancia de base de datos de Administración automática de almacenamiento (ASM) en un entorno NFS y desea montar las copias de seguridad de ASM, debe haber agregado la ruta del disco ASM `/var/opt/snapcenter/sco/backup*/*/*/*` a la ruta existente definida en el parámetro `asm_diskstring`.
- Si tiene una instancia de base de datos ASM en un entorno NFS y desea montar las copias de seguridad del registro ASM como parte de una operación de recuperación, debe haber agregado la ruta del disco ASM `/var/opt/snapcenter/scu/clones/*/*_` a la ruta existente definida en el parámetro `asm_diskstring`.
- En el parámetro `asm_diskstring`, debe configurar `AFD:*` si está usando ASMFD o configurar `ORCL:*` si está usando ASMLIB.



Para obtener información sobre cómo editar el parámetro `asm_diskstring`, consulte ["Cómo agregar rutas de disco a `asm\_diskstring`"](#).

- Debe configurar las credenciales de ASM y el puerto de ASM si difieren de los del host de la base de datos de origen al montar la copia de seguridad.
- Si desea montar en un host alternativo, debe verificar que el host alternativo cumpla con los siguientes requisitos:
 - El mismo UID y GID que el host original
 - La misma versión de Oracle que la del host original
 - La misma distribución y versión del sistema operativo que la del host original
 - Para NVMe, se debe instalar la utilidad NVMe
- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup que consta de protocolos mixtos iSCSI y FC. Para obtener más información, consulte ["La operación falla con el error No se puede descubrir el dispositivo para LUN"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 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. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento primario o secundario (duplicado o reflejado).
5. Seleccione la copia de seguridad de la tabla y luego haga clic en .
6. En la página Montar copias de seguridad, 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**.

Se muestra la ruta de montaje `/var/opt/snapcenter/sco/backup_mount/backup_name/database_name`.

Si está montando la copia de seguridad de una base de datos ASM, se muestra la ruta de montaje +diskgroupname_SID_backupid.

7. Haga clic en **Montar**.

Después de terminar

- Puede ejecutar el siguiente comando para recuperar la información relacionada con la copia de seguridad montada:

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- Si ha montado una base de datos ASM, puede ejecutar el siguiente comando para recuperar la información relacionada con la copia de seguridad montada:

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- Para recuperar el ID de respaldo, ejecute el siguiente comando:

```
./sccli Get-Smbbackup-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 una copia de seguridad de la base de datos

Puede desmontar manualmente una copia de seguridad de base de datos montada cuando ya no desee acceder a los archivos de la copia de seguridad.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 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. Seleccione la copia de seguridad que está montada y luego haga clic en  .

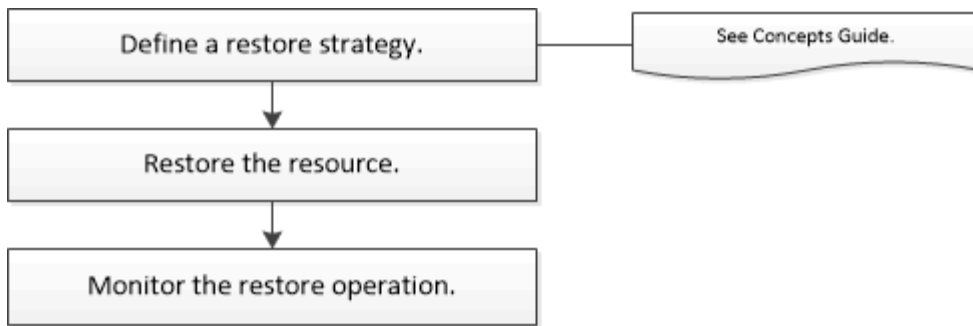
5. Haga clic en **Aceptar**.

Restaurar y recuperar bases de datos Oracle

Restaurar flujo de trabajo

El flujo de trabajo de restauración incluye la planificación, la ejecución de las operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de restauración:



Definir una estrategia de restauración y recuperación para bases de datos Oracle

Debe definir una estrategia antes de restaurar y recuperar su base de datos para poder realizar operaciones de restauración y recuperación con éxito.

Tipos de copias de seguridad compatibles con operaciones de restauración y recuperación

SnapCenter admite la restauración y recuperación de diferentes tipos de copias de seguridad de bases de datos Oracle.

- Copia de seguridad de datos en línea
- Copia de seguridad de datos de apagado sin conexión
- Copia de seguridad de datos de montaje sin conexión



Si está restaurando una copia de seguridad de datos de apagado o montaje sin conexión, SnapCenter deja la base de datos en estado sin conexión. Debe recuperar manualmente la base de datos y restablecer los registros.

- Copia de seguridad completa
- Copias de seguridad de bases de datos en espera de Data Guard montadas sin conexión
- Copias de seguridad en línea de solo datos de bases de datos en espera de Active Data Guard



No se puede realizar la recuperación de bases de datos en espera de Active Data Guard.

- Copias de seguridad de datos en línea, copias de seguridad completas en línea, copias de seguridad de montaje sin conexión y copias de seguridad de apagado sin conexión en una configuración de Real Application Clusters (RAC)
- Copias de seguridad de datos en línea, copias de seguridad completas en línea, copias de seguridad de montaje sin conexión y copias de seguridad de apagado sin conexión en una configuración de Administración automática de almacenamiento (ASM)

Tipos de métodos de restauración admitidos para bases de datos Oracle

SnapCenter admite la conexión y copia o la restauración en el lugar para bases de datos Oracle. Durante una operación de restauración, SnapCenter determina el método de restauración apropiado para el sistema de archivos que se utilizará para restaurar sin pérdida de datos.



SnapCenter no admite SnapRestore basado en volumen.

Restauración mediante conexión y copia

Si el diseño de la base de datos difiere de la copia de seguridad o si hay archivos nuevos después de crear la copia de seguridad, se realiza una restauración de conexión y copia. En el método de restauración de conexión y copia, se realizan las siguientes tareas:

Pasos

1. El volumen se clona desde la instantánea y la pila del sistema de archivos se construye en el host utilizando los LUN o volúmenes clonados.
2. Los archivos se copian de los sistemas de archivos clonados a los sistemas de archivos originales.
3. Luego, los sistemas de archivos clonados se desmontan del host y los volúmenes clonados se eliminan de ONTAP.



Para una configuración de Flex ASM (donde la cardinalidad es menor que la cantidad de nodos en el clúster RAC) o bases de datos ASM RAC en VMDK o RDM, solo se admite el método de restauración de conexión y copia.

Incluso si ha habilitado de forma forzada la restauración en el lugar, SnapCenter realiza una restauración de conexión y copia en los siguientes escenarios:

- Restaurar desde el sistema de almacenamiento secundario
- Restauración de grupos de discos ASM presentes en nodos de una configuración de Oracle RAC en la que no está configurada la instancia de base de datos
- En la configuración de Oracle RAC, en cualquiera de los nodos pares si la instancia de ASM o la instancia del clúster no se está ejecutando o si el nodo par está inactivo
- Restauración de archivos de control únicamente
- Restaurar un subconjunto de espacios de tabla que residen en un grupo de discos ASM
- El grupo de discos se comparte entre archivos de datos, archivo sp y archivo de contraseña
- El servicio SnapCenter Plug-in Loader (SPL) no está instalado o no se está ejecutando en el nodo remoto en un entorno RAC
- Se agregan nuevos nodos a Oracle RAC y el servidor SnapCenter no tiene conocimiento de los nodos recién agregados

Restauración en el lugar

Si el diseño de la base de datos es similar a la copia de seguridad y no ha sufrido ningún cambio de configuración en la pila de almacenamiento y base de datos, se realiza una restauración en el lugar, en donde la restauración del archivo o LUN se realiza en ONTAP. SnapCenter solo admite SnapRestore de archivo único (SFSR) como parte del método de restauración en el lugar.



NetApp ONTAP admite la restauración local desde una ubicación secundaria.

Si desea realizar una restauración local en la base de datos, asegúrese de tener solo archivos de datos en el grupo de discos ASM. Debe crear una copia de seguridad después de realizar cualquier cambio en el grupo de discos ASM o en la estructura física de la base de datos. Después de realizar una restauración en el lugar, el grupo de discos contendrá la misma cantidad de archivos de datos que en el momento de la copia de seguridad.

La restauración en el lugar se aplicará automáticamente cuando el grupo de discos o el punto de montaje

coincidan con los siguientes criterios:

- No se agregan nuevos archivos de datos después de la copia de seguridad (verificación de archivos externos)
- No se pueden agregar, eliminar ni recrear discos ASM ni LUN después de la copia de seguridad (verificación de cambios estructurales en el grupo de discos ASM)
- No se pueden agregar, eliminar ni recrear LUN en el grupo de discos LVM (verificación de cambios estructurales en el grupo de discos LVM)



También puede habilitar de manera forzada la restauración en el lugar mediante la GUI, la CLI de SnapCenter o el cmdlet de PowerShell para anular la verificación de archivos externos y la verificación de cambios estructurales del grupo de discos LVM.

Realizar una restauración local en ASM RAC

En SnapCenter, el nodo en el que se realiza la restauración se denomina nodo principal y todos los demás nodos del RAC en el que reside el grupo de discos ASM se denominan nodos pares. SnapCenter cambia el estado del grupo de discos ASM para desmontarlo en todos los nodos donde el grupo de discos ASM está en estado de montaje antes de realizar la operación de restauración de almacenamiento. Una vez completada la restauración del almacenamiento, SnapCenter cambia el estado del grupo de discos ASM como estaba antes de la operación de restauración.

En entornos SAN, SnapCenter elimina dispositivos de todos los nodos pares y realiza la operación de anulación de asignación de LUN antes de la operación de restauración del almacenamiento. Después de la operación de restauración del almacenamiento, SnapCenter realiza la operación de mapa LUN y construye dispositivos en todos los nodos pares. En un entorno SAN, si el diseño de Oracle RAC ASM reside en LUN, entonces, al restaurar, SnapCenter realiza operaciones de anulación de asignación de LUN, restauración de LUN y asignación de LUN en todos los nodos del clúster RAC donde reside el grupo de discos ASM. Antes de restaurar, incluso si no se utilizaron todos los iniciadores de los nodos RAC para los LUN, después de restaurar SnapCenter crea un nuevo iGroup con todos los iniciadores de todos los nodos RAC.

- Si se produce algún error durante la actividad de prerestauración en los nodos pares, SnapCenter revierte automáticamente el estado del grupo de discos ASM al que estaba antes de realizar la restauración en los nodos pares en los que la operación de prerestauración fue exitosa. No se admite la reversión para el nodo principal y el nodo par en el que falló la operación. Antes de intentar otra restauración, debe solucionar manualmente el problema en el nodo par y devolver el grupo de discos ASM en el nodo principal al estado de montaje.
- Si ocurre algún error durante la actividad de restauración, la operación de restauración falla y no se realiza ninguna reversión. Antes de intentar otra restauración, debe solucionar manualmente el problema de restauración del almacenamiento y devolver el grupo de discos ASM en el nodo principal al estado de montaje.
- Si se produce algún error durante la actividad posterior a la restauración en cualquiera de los nodos pares, SnapCenter continúa con la operación de restauración en los demás nodos pares. Debes solucionar manualmente el problema posterior a la restauración en el nodo par.

Tipos de operaciones de restauración compatibles con las bases de datos Oracle

SnapCenter le permite realizar diferentes tipos de operaciones de restauración para bases de datos Oracle.

Antes de restaurar la base de datos, se validan las copias de seguridad para identificar si faltan archivos en comparación con los archivos reales de la base de datos.

Restauración completa

- Restaura solo los archivos de datos
- Restaura solo 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 rehacer en bases de datos en espera de Data Guard y en espera de Active Data Guard

Restauración parcial

- Restaura solo los espacios de tabla seleccionados
- Restaura únicamente las bases de datos conectables (PDB) seleccionadas
- Restaura solo los espacios de tabla seleccionados de un PDB

Tipos de operaciones de recuperación compatibles con las bases de datos Oracle

SnapCenter le permite realizar diferentes tipos de operaciones de recuperación para bases de datos 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

Debe especificar la fecha y la hora de recuperación según la zona horaria del host de la base de datos.

SnapCenter también ofrece la opción Sin recuperación para bases de datos Oracle.



El complemento para la base de datos Oracle no admite la recuperación si ha realizado una restauración utilizando una copia de seguridad creada con la función de base de datos en espera. Siempre debe realizar la recuperación manual de las bases de datos físicas en espera.

Limitaciones relacionadas con la restauración y recuperación de bases de datos Oracle

Antes de realizar operaciones de restauración y recuperación, debe tener en cuenta las limitaciones.

Si está utilizando cualquier versión de Oracle desde 11.2.0.4 a 12.1.0.1, la operación de restauración quedará bloqueada cuando ejecute el comando *renamedg*. Puede aplicar el parche 19544733 de Oracle para solucionar este problema.

Las siguientes operaciones de restauración y recuperación no son compatibles:

- Restauración y recuperación de espacios de tabla de la base de datos del contenedor raíz (CDB)
- Restauración de espacios de tablas temporales y espacios de tablas temporales asociados con PDB
- Restaurar y recuperar espacios de tabla desde múltiples PDB simultáneamente
- Restauración de copias de seguridad de registros
- Restauración de copias de seguridad a una ubicación diferente
- Restauración de archivos de registro de rehacer en cualquier configuración que no sean bases de datos en espera de Data Guard o en espera de Data Guard activo
- Restauración de archivo SPFILE y contraseña

- Cuando se realiza una operación de restauración en una base de datos que se volvió a crear utilizando el nombre de base de datos preexistente en el mismo host, que fue administrada por SnapCenter y que tenía copias de seguridad válidas, la operación de restauración sobrescribe los archivos de base de datos recién creados aunque los DBID sean diferentes.

Esto se puede evitar realizando cualquiera de las siguientes acciones:

- Descubra los recursos de SnapCenter después de volver a crear la base de datos
- Crear una copia de seguridad de la base de datos recreada

Limitaciones relacionadas con la recuperación de espacios de tabla en un punto determinado del tiempo

- No se admite la recuperación en un punto en el tiempo (PITR) de los espacios de tabla SYSTEM, SYSAUX y UNDO
- La PITR de espacios de tabla no se puede realizar junto con otros tipos de restauración
- Si se cambia el nombre de un espacio de tabla y desea recuperarlo a un punto anterior al cambio de nombre, debe especificar el nombre anterior del espacio de tabla.
- Si las restricciones para las tablas en un espacio de tabla están contenidas en otro espacio de tabla, debe recuperar ambos espacios de tabla
- Si una tabla y sus índices se almacenan en diferentes espacios de tabla, entonces los índices deben eliminarse antes de realizar PITR
- PITR no se puede utilizar para recuperar el espacio de tabla predeterminado actual
- PITR no se puede utilizar para recuperar espacios de tabla que contengan cualquiera de los siguientes objetos:
 - Objetos con objetos subyacentes (como vistas materializadas) u 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 particionada se almacenan en diferentes espacios de tabla, entonces debe eliminar la tabla antes de realizar PITR o mover todas las particiones al mismo espacio de tabla antes de realizar PITR.

- Deshacer o revertir segmentos
- Colas avanzadas compatibles con Oracle 8 con múltiples 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 Oracle

Puede restaurar una base de datos de Oracle desde una copia de seguridad en el almacenamiento primario o secundario. Sólo se pueden restaurar bases de datos en la misma ubicación en la misma instancia de base de datos. Sin embargo, en la configuración de Real Application Cluster (RAC), puede restaurar bases de datos en otros nodos.

Fuentes para operaciones de restauración

Puede restaurar bases de datos desde una copia de seguridad en el almacenamiento primario o secundario. Si desea restaurar desde una copia de seguridad en el almacenamiento secundario en una configuración de espejo múltiple, puede seleccionar el espejo de almacenamiento secundario como origen.

Destinos para operaciones de restauración

Sólo se pueden restaurar bases de datos en la misma ubicación en la misma instancia de base de datos.

En una configuración RAC, puede restaurar bases de datos RAC desde cualquier nodo del clúster.

Variables de entorno predefinidas para restaurar prescript y postscript específicos

SnapCenter le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript mientras restaura una base de datos.

Variables de entorno predefinidas compatibles para restaurar una base de datos

- **SC_JOB_ID** especifica el ID del trabajo de la operación.

Ejemplo: 257

- **SC_ORACLE_SID** especifica el identificador del sistema de la base de datos.

Si la operación involucra múltiples bases de datos, esto contendrá los nombres de las bases de datos separados por barras verticales.

Ejemplo: NFSB31

- **SC_HOST** especifica el nombre de host de la base de datos.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplo: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** especifica el propietario del sistema operativo de la base de datos.

Ejemplo: oráculo

- **SC_OS_GROUP** especifica el grupo del sistema operativo de la base de datos.

Ejemplo: oinstall

- **SC_BACKUP_NAME** especifica el nombre de la copia de seguridad.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplos:

- Si la base de datos no se ejecuta 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 ejecuta 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-

- **SC_BACKUP_ID** especifica el ID de la copia de seguridad.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplos:

- Si la base de datos no se está ejecutando en modo ARCHIVELOG: DATA@203|LOG@205
- Si la base de datos se ejecuta 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 del directorio de inicio de Oracle.

Ejemplo: /ora01/app/oracle/product/18.1.0/db_1

- **SC_RECOVERY_TYPE** especifica los archivos que se recuperan y también el alcance de la recuperación.

Ejemplo:

RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Para obtener información sobre los delimitadores, consulte "[Delimitadores admitidos](#)".

Requisitos para restaurar una base de datos Oracle

Antes de restaurar una base de datos de Oracle, debe asegurarse de que se cumplan los requisitos previos.

- Deberías haber definido tu estrategia de restauración y recuperación.
- El administrador de SnapCenter debería haberle asignado las máquinas virtuales de almacenamiento (SVM) tanto para los volúmenes de origen como para los de destino si está replicando instantáneas a un espejo o bóveda.
- Si los registros de archivo se eliminan como parte de la copia de seguridad, debe haber montado manualmente las copias de seguridad de registros de archivo necesarias.
- Si desea restaurar bases de datos de Oracle que residen en un disco de máquina virtual (VMDK), debe asegurarse de que la máquina invitada tenga la cantidad necesaria de ranuras libres para asignar los VMDK clonados.
- Debe asegurarse de que todos los volúmenes de datos y volúmenes de registro de archivo 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 de RAC One Node esté en estado "sin montar" para realizar una restauración completa del archivo de control o de la base de datos.
- Si tiene una instancia de base de datos ASM en un entorno NFS, debe agregar la ruta del disco ASM `/var/opt/snapcenter/scu/clones/*/*` a la ruta existente definida en el parámetro `asm_diskstring` para montar correctamente las copias de seguridad del registro ASM como parte de la operación de recuperación.
- En el parámetro `asm_diskstring`, debe configurar `AFD:*` si está usando ASMFD o configurar `ORCL:*` si está usando ASMLIB.



Para obtener información sobre cómo editar el parámetro `asm_diskstring`, consulte ["Cómo agregar rutas de disco a `asm\_diskstring`"](#)

- Debe configurar el escucha estático en el archivo **listener.ora** disponible en `$ORACLE_HOME/network/admin` para bases de datos que no sean ASM y en `$GRID_HOME/network/admin` para bases de datos ASM si ha deshabilitado la autenticación del sistema operativo y habilitado la autenticación de base de datos Oracle para una base de datos Oracle, y desea restaurar los archivos de datos y los archivos de control de esa base de datos.
- Debe aumentar el valor del parámetro `SCORestoreTimeout` ejecutando el comando `Set-SmConfigSettings` si el tamaño de la base de datos está en terabytes (TB).
- Debe asegurarse de que todas las licencias necesarias para vCenter estén instaladas y actualizadas.

Si las licencias no están instaladas o actualizadas, se muestra un mensaje de advertencia. Si ignora la advertencia y continúa, la restauración desde RDM fallará.

- Debe asegurarse de que el LUN no esté asignado al host AIX mediante un iGroup que consta de protocolos mixtos iSCSI y FC. Para obtener más información, consulte ["La operación falla con el error No se puede descubrir el dispositivo para LUN"](#).

Restaurar y recuperar la base de datos Oracle

En caso de pérdida de datos, puede utilizar SnapCenter para restaurar datos de una o más copias de seguridad en su sistema de archivos activo y luego recuperar la base de datos.

Antes de empezar

Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios `prescript` y `postscript`.

Acerca de esta tarea

- La recuperación se realiza utilizando los registros de archivo disponibles en la ubicación del registro de archivo configurado. Si la base de datos se ejecuta en modo `ARCHIVELOG`, la base de datos Oracle guarda los grupos completos de archivos de registro de rehacer en uno o más destinos fuera de línea, conocidos colectivamente como el registro de rehacer archivado. SnapCenter identifica y monta la cantidad óptima de copias de seguridad de registros según el SCN especificado, la fecha y hora seleccionadas o la opción de todos los registros. Si los registros de archivo necesarios para la recuperación no están disponibles en la ubicación configurada, debe montar la instantánea que contiene los registros y especificar la ruta como registros de archivo externos.

Si migra la base de datos ASM de ASMLIB a ASMFD, las copias de seguridad creadas con ASMLIB no se podrán utilizar para restaurar la base de datos. Debe crear copias de seguridad en la configuración de ASMFD y usar esas copias de seguridad para restaurar. De manera similar, si la base de datos ASM se migra de ASMFD a ASMLIB, debe crear copias de seguridad en la configuración de ASMLIB para restaurarla.

Cuando se restaura una base de datos, se crea un archivo de bloqueo operativo (`.sm_lock_dbsid`) en el host de la base de datos Oracle en el directorio `/var/opt/snapcenter/sco/lock` para evitar que se ejecuten múltiples operaciones en la base de datos. Una vez restaurada la base de datos, el archivo de bloqueo operativo se elimina automáticamente.



No se admite la restauración de archivos SPFILE y de contraseña.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 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. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o reflejado).
5. Seleccione la copia de seguridad de la tabla y luego haga clic en *  *.
6. En la página Restaurar ámbito, realice las siguientes tareas:
 - a. Si ha seleccionado una copia de seguridad de una base de datos en un entorno de Real Application Clusters (RAC), seleccione el nodo RAC.
 - b. Al seleccionar datos reflejados o de bóveda:
 - Si no hay copias de seguridad de registros en el espejo o la bóveda, no se selecciona nada y los localizadores están vacíos.
 - Si existen copias de seguridad de registros en el espejo o en la bóveda, se selecciona la última copia de seguridad de registros y se muestra el localizador correspondiente.



Si la copia de seguridad del registro seleccionada existe tanto en la ubicación del espejo como en la del almacén, se muestran ambos localizadores.

- c. Realice las siguientes acciones:

Si deseas restaurar...	Haz esto...
Todos los archivos de datos de la base de datos	Seleccionar Todos los archivos de datos. Sólo se restauran los archivos de datos de la base de datos. Los archivos de control, los registros de archivo o los archivos de registro de rehacer no se restauran.

Si deseas restaurar...	Haz esto...
Espacios de tabla	Seleccione Espacios de tabla. Puede especificar los espacios de tabla que desea restaurar.
Archivos de control	Seleccione Archivos de control.  Al restaurar archivos de control, asegúrese de que la estructura del directorio exista o deba crearse con los propietarios de usuarios y grupos correctos, si los hubiera, para permitir que el proceso de restauración copie los archivos a la ubicación de destino. Si el directorio no existe, el trabajo de restauración fallará.
Archivos de registro de rehacer	Seleccione Rehacer archivos de registro. Esta opción solo está disponible para bases de datos en espera de Data Guard o en espera de Data Guard activa.  No se realiza una copia de seguridad de los archivos de registro de rehacer para bases de datos que no sean Data Guard. Para las bases de datos que no son Data Guard, la recuperación se realiza mediante registros de archivo.
Bases de datos conectables (PDB)	Seleccione Bases de datos conectables y, a continuación, especifique los PDB que desea restaurar.
Espacios de tablas de bases de datos conectables (PDB)	Seleccione Espacios de tabla de base de datos conectable (PDB) y, a continuación, especifique la PDB y los espacios de tabla de esa PDB que desea restaurar. Esta opción solo está disponible si ha seleccionado un 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, de superior a inferior, son abierto, montado, iniciado y apagado. Debe seleccionar esta casilla de verificación si la base de datos está en un estado superior pero el estado debe cambiarse a un estado inferior para realizar una operación de restauración. Si la base de datos está en un estado inferior pero el estado debe cambiarse a un estado superior para realizar la operación de restauración, el estado de la base de datos cambia automáticamente incluso si no selecciona la casilla de verificación.

Si una base de datos está en estado abierto y para restaurarla debe estar en estado montado, el estado de la base de datos se cambia solo si selecciona esta casilla de verificación.

- a. Seleccione **Forzar restauración en el lugar** si desea realizar una restauración en el lugar en los escenarios en los que se agregan nuevos archivos de datos después de la copia de seguridad o cuando se agregan, eliminan o vuelven a crear LUN en un grupo de discos LVM.

7. En la página **Ámbito de recuperación**, realice las siguientes acciones:

Si usted...	Haz esto...
¿Quieres recuperar la última transacción?	Seleccionar Todos los registros .
¿Quieres recuperar un Número de cambio de sistema (SCN) específico?	Seleccione Hasta SCN (Número de cambio del sistema) .
¿Quieres recuperar datos y tiempos específicos?	Seleccione Fecha y hora . Debe especificar la fecha y la hora de la zona horaria del host de la base de datos.
No quiero recuperarme	Seleccione Sin recuperación .

Si usted...	Haz esto...
¿Desea especificar cualquier ubicación de registro de archivo externo?	Si la base de datos se ejecuta en modo ARCHIVELOG, SnapCenter identifica y monta la cantidad óptima de copias de seguridad de registros según el SCN especificado, la fecha y hora seleccionadas o la opción de todos los registros. Si aún desea especificar la ubicación de los archivos de registro de archivo externo, seleccione Especificar ubicaciones de registros de archivo externo. Si los registros de archivo se eliminan como parte de la copia de seguridad y usted ha montado manualmente las copias de seguridad de registros de archivo necesarias, debe especificar la ruta de copia de seguridad montada como la ubicación del registro de archivo externo para la recuperación.  Debe verificar la ruta y el contenido de la ruta de montaje antes de incluirla como ubicación de registro externo. • "Protección de datos de Oracle con ONTAP" • "La operación falla con el error ORA-00308"

No se puede realizar una restauración con recuperación desde copias de seguridad secundarias si los volúmenes de registro de archivo no están protegidos, pero los volúmenes de datos sí lo están. Solo puedes restaurar seleccionando **Sin recuperación**.

Si está recuperando una base de datos RAC con la opción de base de datos abierta seleccionada, solo la instancia de RAC donde se inició la operación de recuperación vuelve al estado abierto.



La recuperación no es compatible con las bases de datos en espera de Data Guard y en espera de Data Guard activa.

- En la página PreOps, ingrese la ruta y los argumentos del script que desea ejecutar antes de la operación de restauración.

Debes almacenar los scripts en la ruta `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha creado alguna carpeta dentro de esta ruta 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 le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript. ["Más información"](#)

9. En la página PostOps, realice los siguientes pasos:

- a. Introduzca la ruta y los argumentos del postscript que desea ejecutar después de la operación de restauración.

Debes almacenar los postscripts en `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha creado alguna carpeta dentro de esta ruta para almacenar los scripts, debe especificar esas carpetas en la ruta.



Si la operación de restauración falla, los postscripts no se ejecutarán y las actividades de limpieza se activarán directamente.

- b. Seleccione la casilla de verificación si desea abrir la base de datos después de la recuperación.

Después de restaurar una base de datos contenedora (CDB) con o sin archivos de control, o después de restaurar solo los archivos de control de CDB, si especifica abrir la base de datos después de la recuperación, solo se abre la CDB y no las bases de datos conectables (PDB) en esa CDB.

En una configuración de RAC, solo se abre la instancia de RAC que se utiliza para la recuperación después de la recuperación.



Después de restaurar un espacio de tabla de usuario con archivos de control, un espacio de tabla de sistema con o sin archivos de control, o un PDB con o sin archivos de control, solo el estado del PDB relacionado con la operación de restauración cambia al estado original. El estado de los otros PDB que no se usaron para la restauración no se cambia al estado original porque el estado de esos PDB no se guardó. Debe cambiar manualmente el estado de los PDB que no se utilizaron para la restauración.

10. En la página Notificación, en la lista desplegable **Preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.

También debe especificar las direcciones de correo electrónico del remitente y del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de restauración realizada, deberá seleccionar **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell `Set-SmSmtServer`.

11. Revise el resumen y luego haga clic en **Finalizar**.
12. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Para más información

- ["La base de datos Oracle RAC One Node se omite para realizar operaciones de SnapCenter"](#)
- ["No se pudo restaurar desde una ubicación secundaria de SnapMirror o SnapVault"](#)
- ["No se pudo restaurar desde una copia de seguridad de una encarnación huérfana"](#)
- ["Parámetros personalizables para operaciones de copia de seguridad, restauración y clonación en sistemas AIX"](#)

Restaurar y recuperar espacios de tabla mediante la recuperación en un punto en el tiempo

Puede restaurar un subconjunto de espacios de tabla que se haya dañado o eliminado sin afectar a los demás espacios de tabla de la base de datos. SnapCenter utiliza RMAN para realizar la recuperación en un punto en el tiempo (PITR) de los espacios de tabla.

Antes de empezar

- Las copias de seguridad necesarias para realizar PITR de los espacios de tabla deben catalogarse y montarse.
- Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios prescript y postscript.

Acerca de esta tarea

Durante la operación PITR, RMAN crea una instancia auxiliar en el destino auxiliar especificado. El destino auxiliar podría ser un punto de montaje o un grupo de discos ASM. Si hay suficiente espacio en la ubicación de montaje, puede reutilizar una de las ubicaciones de montaje en lugar de un punto de montaje dedicado.

Debe especificar la fecha y la hora o SCN y el espacio de tabla se restaura en la base de datos de origen.

Puede seleccionar y restaurar varios espacios de tabla que residen en entornos ASM, NFS y SAN. Por ejemplo, si los espacios de tabla TS2 y TS3 residen en NFS y TS4 residen en SAN, puede realizar una única operación PITR para restaurar todos los espacios de tabla.



En una configuración RAC, puede realizar PITR de espacios de tabla desde cualquier nodo del RAC.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de tipo instancia única (multiinquilino) ya sea 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. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o reflejado).

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione la copia de seguridad catalogada y luego haga clic en *  *.
6. En la página Restaurar ámbito, realice las siguientes tareas:
 - a. Si ha seleccionado una copia de seguridad de una base de datos en un entorno de Real Application Clusters (RAC), seleccione el nodo RAC.
 - b. Seleccione **Espacios de tabla** y, a continuación, especifique los espacios de tabla que desea

restaurar.



No se puede ejecutar PITR en los espacios de tabla 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 **Ámbito de recuperación**, 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 la hora y el destino auxiliar.

SnapCenter identifica y luego monta y cataloga la cantidad óptima de copias de seguridad de datos y registros necesarios para realizar PITR según el SCN especificado o la fecha y hora seleccionadas.

8. En la página **PreOps**, ingrese la ruta y los argumentos del script que desea ejecutar antes de la operación de restauración.

Debes almacenar los scripts en la ruta `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha creado alguna carpeta dentro de esta ruta 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 le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript. ["Más información"](#)

9. En la página **PostOps**, realice los siguientes pasos:

- a. Introduzca la ruta y los argumentos del postscript que desea ejecutar después de la operación de restauración.



Si la operación de restauración falla, los postscripts no se ejecutarán y las actividades de limpieza se activarán directamente.

- b. Seleccione la casilla de verificación si desea abrir la base de datos después de la recuperación.

10. En la página **Notificación**, en la lista desplegable **Preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.

11. Revise el resumen y luego haga clic en **Finalizar**.

12. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Restaurar y recuperar bases de datos conectables mediante recuperación en un punto determinado del tiempo

Puede restaurar y recuperar una base de datos conectable (PDB) que se haya dañado o eliminado sin afectar a las otras PDB en la base de datos contenedora (CDB).

SnapCenter utiliza RMAN para realizar la recuperación en un punto en el tiempo (PITR) del PDB.

Antes de empezar

- Las copias de seguridad que se requieren para realizar PITR de un PDB deben catalogarse y montarse.



En una configuración RAC, debe cerrar manualmente el PDB (cambiando el estado a MONTADO) en todos los nodos de la configuración RAC.

- Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios prescript y postscript.

Acerca de esta tarea

Durante la operación PITR, RMAN crea una instancia auxiliar en el destino auxiliar especificado. El destino auxiliar podría ser un punto de montaje o un grupo de discos ASM. Si hay suficiente espacio en la ubicación de montaje, puede reutilizar una de las ubicaciones de montaje en lugar de un punto de montaje dedicado.

Debe especificar la fecha y la hora o SCN para realizar el PITR del PDB. RMAN puede recuperar PDB de LECTURA, ESCRITURA, SÓLO LECTURA o descartados, incluidos archivos de datos.

Puedes restaurar y recuperar únicamente:

- un PDB a la vez
- un espacio de tabla en un PDB
- múltiples espacios de tabla del mismo PDB



En una configuración RAC, puede realizar PITR de espacios de tabla desde cualquier nodo del RAC.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de tipo instancia única (multiinquilino) ya sea 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. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o reflejado).

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione la copia de seguridad catalogada y luego haga clic en *  *.
6. En la página Restaurar ámbito, realice las siguientes tareas:
 - a. Si ha seleccionado una copia de seguridad de una base de datos en un entorno de Real Application Clusters (RAC), seleccione el nodo RAC.
 - b. Dependiendo de si desea restaurar el PDB o los espacios de tabla en un PDB, realice una de las acciones:

Si quieres...	Pasos...
Restaurar un PDB	i. Seleccione Bases de datos conectables (PDB). ii. Especifique el PDB que desea restaurar.  No se puede ejecutar PITR en la base de datos PDB\$SEED.
Restaurar espacios de tabla en un PDB	i. Seleccione Espacios de tabla de bases de datos conectables (PDB). ii. Especifique el PDB. iii. Especifique un solo espacio de tabla o varios espacios de tabla que desee restaurar.  No se puede ejecutar PITR en los espacios de tabla 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 **Ámbito de recuperación**, 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 la hora y el destino auxiliar.

SnapCenter identifica y luego monta y cataloga la cantidad óptima de copias de seguridad de datos y registros necesarios para realizar PITR según el SCN especificado o la fecha y hora seleccionadas.

8. En la página **PreOps**, ingrese la ruta y los argumentos del script que desea ejecutar antes de la operación de restauración.

Debes almacenar los scripts en la ruta `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha creado alguna carpeta dentro de esta ruta 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 le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript. ["Más información"](#)

9. En la página **PostOps**, realice los siguientes pasos:

- a. Introduzca la ruta y los argumentos del postscript que desea ejecutar después de la operación de restauración.



Si la operación de restauración falla, los postscripts no se ejecutarán y las actividades de limpieza se activarán directamente.

- b. Seleccione la casilla de verificación si desea abrir la base de datos después de la recuperación.

En una configuración RAC, el PDB se abrirá solo en el nodo donde se recuperó la base de datos. Debe abrir manualmente el PDB recuperado en todos los demás nodos de la configuración de RAC.

10. En la página Notificación, en la lista desplegable **Preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.
11. Revise el resumen y luego haga clic en **Finalizar**.
12. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Restaurar y recuperar bases de datos Oracle mediante comandos UNIX

El flujo de trabajo de restauración y recuperación incluye la planificación, la ejecución de las 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 el servidor SnapCenter , enumerar las copias de seguridad y recuperar su información y restaurar la copia de seguridad.

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 la copia de seguridad de la ubicación principal.

Pasos

1. Iniciar una sesión de conexión con el servidor SnapCenter para un usuario específico: *Open-SmConnection*
2. Recupere la información sobre las copias de seguridad que desea restaurar: *Get-SmBackup*
3. Recupere la información detallada sobre la copia de seguridad especificada: *Get-SmBackupDetails*

Este comando recupera la información detallada sobre la copia de seguridad de un recurso específico con un ID de copia de seguridad determinado. La información incluye el nombre de la base de datos, la versión, el inicio, el SCN inicial y final, los espacios de tabla, las bases de datos conectables y sus espacios de tabla.

4. Restaurar datos desde la copia de seguridad: *Restore-SmBackup*

Supervisar las operaciones de restauración de la base de datos Oracle

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Cancelar operaciones de restauración de bases de datos de Oracle

Puede cancelar trabajos de restauración que estén en cola.

Debe iniciar 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.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones de restauración que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de restauración en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 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 Actividad para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

Clonar base de datos Oracle

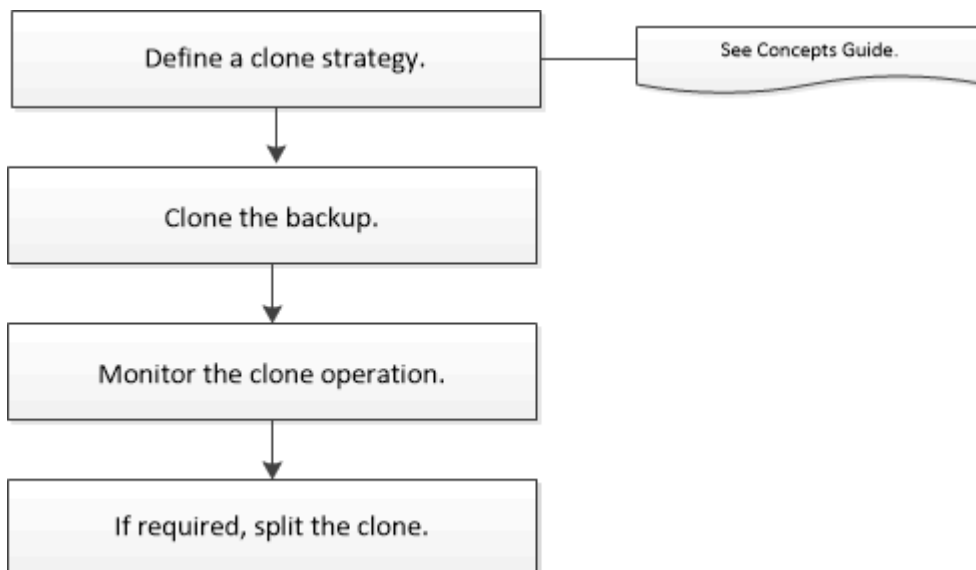
Flujo de trabajo de clonación

El flujo de trabajo de clonación incluye la planificación, la ejecución de la operación de clonación y la supervisión de la operación.

Puedes clonar bases de datos por las siguientes razones:

- Para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de la base de datos actual durante los ciclos de desarrollo de la aplicación.
- Para rellenar almacenes de datos utilizando herramientas de extracción y manipulación de datos.
- Para recuperar datos que fueron eliminados o modificados por error.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de clonación:



Definir una estrategia de clonación para bases de datos Oracle

Definir una estrategia antes de clonar su base de datos garantiza que la operación de clonación sea exitosa.

Tipos de copias de seguridad compatibles con la clonación

SnapCenter admite la clonación de diferentes tipos de copias de seguridad de bases de datos Oracle.

- Copia de seguridad de datos en línea
- Copia de seguridad completa en línea
- Copia de seguridad de montaje sin conexión
- Copia de seguridad de apagado sin conexión
- Copias de seguridad de bases de datos en espera de Data Guard y bases de datos en espera de Active Data Guard
- Copias de seguridad de datos en línea, copias de seguridad completas en línea, copias de seguridad de montaje sin conexión y copias de seguridad de apagado sin conexión en una configuración de Real Application Clusters (RAC)
- Copias de seguridad de datos en línea, copias de seguridad completas en línea, copias de seguridad de montaje sin conexión y copias de seguridad de apagado sin conexión en una configuración de Administración automática de almacenamiento (ASM)



Las configuraciones de SAN no son compatibles si la opción `user_friendly_names` en el archivo de configuración de múltiples rutas está establecida en sí.



No se admite la clonación de copias de seguridad del registro de archivo.

Tipos de clonación admitidos para bases de datos Oracle

En un entorno de base de datos Oracle, SnapCenter admite la clonación de una copia de seguridad de la base de datos. Puede clonar la copia de seguridad de los sistemas de almacenamiento primario y secundario.

El servidor SnapCenter utiliza la tecnología NetApp FlexClone para clonar copias de seguridad.

Puede actualizar un clon ejecutando el comando "Refresh-SmClone". Este comando crea una copia de seguridad de la base de datos, elimina el clon existente y crea un clon con el mismo nombre.



La operación de actualización de clonación solo se puede realizar mediante los comandos UNIX.

Convenciones de nomenclatura de clones para bases de datos Oracle

A partir de SnapCenter 3.0, la convención de nomenclatura utilizada para los clones de sistemas de archivos es diferente a la de los clones de grupos de discos 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 ASM es `SC_HASHCODEofDISKGROUP_CLONESID`.

HASHCODEofDISKGROUP es un número generado automáticamente (de 2 a 10 dígitos) que es único para cada grupo de discos ASM.

Limitaciones de la clonación de bases de datos Oracle

Debe tener en cuenta las limitaciones de las operaciones de clonación antes de clonar las bases de datos.

- Si está utilizando cualquier versión de Oracle desde 11.2.0.4 a 12.1.0.1, la operación de clonación quedará bloqueada cuando ejecute el comando *renamedg*. Puede aplicar el parche 19544733 de Oracle para solucionar este problema.
- No se admite la clonación de bases de datos desde un LUN que está conectado directamente a un host (por ejemplo, mediante el iniciador iSCSI de Microsoft en un host de Windows) a un VMDK o un LUN RDM en el mismo host de Windows u otro host de Windows, o viceversa.
- El directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- Si mueve un LUN que contiene un clon a un nuevo volumen, el clon no se podrá eliminar.

Variables de entorno predefinidas para prescript y postscript específicos de clones

SnapCenter le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript mientras clona una base de datos.

Variables de entorno predefinidas compatibles para clonar una base de datos

- **SC_ORIGINAL_SID** especifica el SID de la base de datos de origen.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplo: NFSB32

- **SC_ORIGINAL_HOST** especifica el nombre del host de origen.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplo: asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** especifica la ruta del directorio de inicio 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 completará para los volúmenes de la aplicación.

Ejemplos:

- Si la base de datos no se ejecuta 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 ejecuta 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_scspr2417819002_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: oráculo

- **SC_ORIGINAL_OS_GROUP** especifica el grupo del sistema operativo 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 clonación de PDB, el valor de este parámetro no estará predefinido.

Este parámetro se completará para los volúmenes de la aplicación.

Ejemplo: clonedb

- **SC_TARGET_HOST** especifica el nombre del host donde se clonará la base de datos.

Este parámetro se completará para los volúmenes de la aplicación.

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 clonación de PDB, el valor de este parámetro no estará predefinido.

Ejemplo: oráculo

- **SC_TARGET_OS_GROUP** especifica el grupo del sistema operativo de la base de datos clonada.

Para el flujo de trabajo de clonación de PDB, el valor de este parámetro no estará predefinido.

Ejemplo: oinstall

- **SC_TARGET_DB_PORT** especifica el puerto de la base de datos clonada.

Para el flujo de trabajo de clonación de PDB, el valor de este parámetro no estará predefinido.

Ejemplo: 1521

Para obtener información sobre los delimitadores, consulte ["Delimitadores admitidos"](#) .

Requisitos para clonar una base de datos Oracle

Antes de clonar una base de datos Oracle, debe asegurarse de que se cumplan los requisitos previos.

- Deberías haber creado una copia de seguridad de la base de datos utilizando SnapCenter.

Debe haber creado con éxito copias de seguridad de datos y registros en línea o copias de seguridad fuera de línea (montaje o apagado) para que la operación de clonación sea exitosa.

- Si desea personalizar las rutas del archivo de control o del archivo de registro de rehacer, debe haber

aprovechando previamente el sistema de archivos requerido o el grupo de discos de Administración automática de almacenamiento (ASM).

De forma predeterminada, los archivos de control y registro de rehacer de la base de datos clonada se crean en el grupo de discos ASM o en el sistema de archivos provisto por SnapCenter para los archivos de datos de la base de datos clonada.

- Si está utilizando ASM sobre NFS, debe agregar `/var/opt/snapcenter/scu/clones/*/*` a la ruta existente definida en el parámetro `asm_diskstring`.
- En el parámetro `asm_diskstring`, debe configurar `AFD:*` si está usando ASMFD o configurar `ORCL:*` si está usando ASMLIB.

Para obtener información sobre cómo editar el parámetro `asm_diskstring`, consulte ["Cómo agregar rutas de disco a asm_diskstring"](#).

- Si está creando el clon en un host alternativo, este debe cumplir los siguientes requisitos:
 - El complemento SnapCenter para Oracle Database debe instalarse en el host alternativo.
 - El host clonado debe poder descubrir LUN desde el almacenamiento primario o secundario.
 - Si está clonando desde un almacenamiento primario o secundario (Vault o Mirror) a un host alternativo, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento secundario y el host alternativo, o que esté zonificada correctamente para FC.
 - Si está clonando desde un almacenamiento Vault o Mirror al mismo host, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento Vault o Mirror y el host, o que esté zonificada correctamente para FC.
 - Si está clonando en un entorno virtualizado, asegúrese de que se establezca una sesión iSCSI entre el almacenamiento primario o secundario y el servidor ESX que aloja el host alternativo, o que esté zonificada correctamente para FC.

Para obtener más información, consulte ["documentación de utilidades del host"](#).

- Si la base de datos de origen es una base de datos ASM:
 - La instancia de ASM debe estar en funcionamiento en el host donde se realizará la clonación.
 - El grupo de discos ASM se debe aprovisionar antes de la operación de clonación si desea colocar los archivos de registro de la base de datos clonada en un grupo de discos ASM dedicado.
 - Se puede configurar el nombre del grupo de discos de datos, pero asegúrese de que ningún otro grupo de discos ASM en el host donde se realizará la clonación lo utilice.

Los archivos de datos que residen en el grupo de discos ASM se aprovisionan como parte del flujo de trabajo de clonación de SnapCenter.

- Para NVMe, se debe instalar la utilidad NVMe
- El tipo de protección para el LUN de datos y el LUN de registro, como espejo, bóveda o espejo-bóveda, debe ser el mismo para descubrir localizadores secundarios durante la clonación a un host alternativo mediante copias de seguridad de registros.
- Debe establecer el valor de `exclude_seed_cdb_view` en `FALSE` en el archivo de parámetros de la base de datos de origen para recuperar información relacionada con el PDB de semilla para clonar una copia de seguridad de la base de datos `12_c_`.

La PDB semilla es una plantilla proporcionada por el sistema que el CDB puede utilizar para crear PDB. La semilla PDB se llama `PDB$SEED`. Para obtener información sobre `PDB$SEED`, consulte el ID de



Debes establecer el valor antes de realizar una copia de seguridad de la base de datos 12_c_.

- SnapCenter admite la copia de seguridad de los sistemas de archivos administrados por el subsistema autofs. Si está clonando la base de datos, asegúrese de que los puntos de montaje de datos no estén bajo la raíz del punto de montaje autofs porque el usuario raíz del host del complemento no tiene permiso para crear directorios bajo la raíz del punto de montaje autofs.

Si los archivos de registro de control y rehacer están bajo el punto de montaje de datos, debe modificar la ruta del archivo de control y luego la ruta del archivo de registro de rehacer según corresponda.



Puede registrar manualmente los nuevos puntos de montaje clonados con el subsistema autofs. Los nuevos puntos de montaje clonados 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 uno alternativo, debe copiar la billetera (archivos de clave) en `/etc/ORACLE/WALLET/$ORACLE_SID` desde la base de datos de origen a la base de datos clonada.
- Debe establecer el valor de `use_lvmetad = 0` en `/etc/lvm/lvm.conf` y detener el servicio `lvm2-lvmetad` para realizar con éxito la clonación en entornos de red de área de almacenamiento (SAN) en Oracle Linux 7 o posterior o Red Hat Enterprise Linux (RHEL) 7 o posterior.
- Debe instalar el parche Oracle 13366202 si está utilizando la base de datos Oracle 11.2.0.3 o posterior y el ID de la base de datos para la instancia auxiliar se cambia mediante un script NID.
- Debe asegurarse de que los agregados que alojan los volúmenes estén en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Para NVMe, si se debe excluir algún puerto de destino de la conexión, debe agregar 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 que consta de protocolos mixtos iSCSI y FC. Para obtener más información, consulte ["La operación falla con el error No se puede descubrir el dispositivo para LUN"](#).

Clonar una copia de seguridad de una base de datos Oracle

Puede utilizar SnapCenter para clonar una base de datos Oracle utilizando la copia de seguridad de la base de datos.

Antes de empezar

Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios `prescript` y `postscript`.

Acerca de esta tarea

- La operación de clonación crea una copia de los archivos de datos de la base de datos y crea nuevos archivos de registro de rehacer en línea y archivos de control. La base de datos se puede recuperar opcionalmente en un tiempo específico, según las opciones de recuperación especificadas.



La clonación falla si intenta clonar una copia de seguridad creada en un host Linux en un host AIX o viceversa.

SnapCenter crea una base de datos independiente cuando se clona desde una copia de seguridad de la base de datos Oracle RAC. SnapCenter admite la creación de clones a partir de la copia de seguridad de una base de datos en espera de Data Guard y de una base de datos en espera de Data Guard activa.

Durante la clonación, SnapCenter monta la cantidad óptima de copias de seguridad de registros según SCN o fecha y hora para las operaciones de recuperación. Después de la recuperación, se desmonta la copia de seguridad del registro. Todos estos clones se montan en `/var/opt/snapcenter/scu/clones/`. Si está utilizando ASM sobre NFS, debe agregar `/var/opt/snapcenter/scu/clones/*/*` a la ruta existente definida en el parámetro `asm_diskstring`.

Al clonar una copia de seguridad de una base de datos ASM en un entorno SAN, las reglas udev para los dispositivos host clonados se crean en `/etc/udev/rules.d/999-scu-netapp.rules`. Estas reglas udev asociadas con los dispositivos host clonados se eliminan cuando elimina el clon.



En una configuración de Flex ASM, no se puede realizar una operación de clonación en nodos Leaf si la cardinalidad es menor que la cantidad de nodos en el clúster RAC.

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

Pasos

- En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
- En la página Recursos, seleccione **Base de datos** o **Grupo de recursos** en la lista **Ver**.
- Seleccione la base de datos 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.

- Desde la vista Administrar copias, seleccione las copias de seguridad de Copias locales (principales), Copias espejo (secundarias) o Copias de bóveda (secundarias).
- Seleccione la copia de seguridad de datos de la tabla y luego haga clic en *  *.
- En la página Nombre, realice una de las siguientes acciones:

Si quieres...	Pasos...
Clonar una base de datos (CDB o no CDB)	a. Especifique el SID del clon. El SID clonado no está disponible de forma predeterminada y la longitud máxima del SID es de 8 caracteres.  Debe asegurarse de que no exista ninguna base de datos con el mismo SID en el host donde se creará el clon.
Clonar una base de datos conectable (PDB)	a. Seleccione PDB Clone. b. Especifique el PDB que desea clonar. c. Especifique el nombre del PDB clonado. Para conocer los pasos detallados para clonar un PDB, consulte "Clonar una base de datos conectable" .

Al seleccionar datos reflejados o de bóveda:

- Si no hay copias de seguridad de registros en el espejo o la bóveda, no se selecciona nada y los localizadores están vacíos.
- Si existen copias de seguridad de registros en el espejo o en la bóveda, se selecciona la última copia de seguridad de registros y se muestra el localizador correspondiente.



Si la copia de seguridad del registro seleccionada existe tanto en la ubicación del espejo como en la del almacén, se muestran ambos localizadores.

7. En la página Ubicaciones, realice las siguientes acciones:

Para este campo...	Haz esto...
Host clon	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 tenga la misma versión de Oracle y sistema operativo que el host de la base de datos de origen.

Para este campo...	Haz esto...
Ubicaciones de archivos de datos	De forma predeterminada, se completa la ubicación del archivo de datos. La convención de nombres predeterminada de SnapCenter para los sistemas de archivos SAN o NFS es FileSystemNameofsourcedatabase_CLONESID. La convención de nombres predeterminada de SnapCenter para los grupos de discos ASM es SC_HASHCODEofDISKGROUP_CLONESID. El HASHCODEofDISKGROUP es un número generado automáticamente (de 2 a 10 dígitos) que es único para cada grupo de discos ASM.  Si está personalizando el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre cumpla con la longitud máxima admitida por Oracle. Si desea especificar una ruta diferente, debe ingresar los puntos de montaje del archivo de datos o los nombres de los grupos de discos ASM para la base de datos clonada. Al personalizar la ruta del archivo de datos, también debe cambiar los nombres de los grupos de discos ASM o del sistema de archivos del archivo de control y del archivo de registro de rehacer al mismo nombre utilizado para los archivos de datos o a un grupo de discos ASM o sistema de archivos existente.

Para este campo...	Haz esto...
Archivos de control	De forma predeterminada, se completa la ruta del archivo de control. Los archivos de control se colocan en el mismo grupo de discos o sistema de archivos ASM que los archivos de datos. Si desea anular la ruta del archivo de control, puede proporcionar una ruta de archivo de control diferente.  El sistema de archivos o el grupo de discos ASM debe 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. Puede 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 del archivo de control a un sistema de archivos diferente (existente) que el de la base de datos de origen.

Para este campo...	Haz esto...
Registros de rehacer	De forma predeterminada, se completan el grupo de archivos de registro de rehacer, la ruta y sus tamaños. Los registros de rehacer se colocan 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 del archivo de registro de rehacer, puede personalizar la ruta del archivo de registro de rehacer a un sistema de archivos diferente al de la base de datos de origen.  El nuevo sistema de archivos o el grupo de discos ASM debe existir en el host. De forma predeterminada, la cantidad de grupos de registros de rehacer, archivos de registros de rehacer y sus tamaños serán los mismos que los de la base de datos de origen. Puede modificar los siguientes parámetros: - Número de grupos de registros de rehacer  Se requieren un mínimo de dos grupos de registros de rehacer para clonar la base de datos. - Rehacer archivos de registro en cada grupo y su ruta Puede personalizar la ruta del archivo de registro de rehacer a un sistema de archivos diferente (existente) que el de la base de datos de origen.  Se requiere un mínimo de un archivo de registro de rehacer en el grupo de registro de rehacer para clonar la base de datos. - Tamaños del archivo de registro de rehacer

8. En la página Credenciales, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre de credencial para el usuario del sistema	Seleccione la credencial que se utilizará para definir la contraseña del usuario del sistema de la base de datos clonada. Si SQLNET.AUTHENTICATION_SERVICES está configurado como NONE en el archivo sqlnet.ora en el host de destino, no debe seleccionar Ninguno como Credencial en la GUI de SnapCenter .
Nombre de credencial de instancia de ASM	Seleccione Ninguno si la autenticación del sistema operativo está habilitada para conectarse a la instancia de ASM en el host clonado. De lo contrario, seleccione la credencial Oracle ASM configurada con el usuario "sys" o un usuario que tenga el privilegio "sysasm" aplicable al host clonado.

Los detalles de inicio, nombre de usuario y grupo de Oracle se completan automáticamente desde la base de datos de origen. Puede cambiar los valores según el entorno de Oracle del host donde se creará el clon.

9. En la página PreOps, realice los siguientes pasos:

- a. Introduzca la ruta y los argumentos del script que desea ejecutar antes de la operación de clonación.

Debes almacenar la prescripción en `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha colocado el script en alguna carpeta dentro de esta ruta, deberá proporcionar la ruta completa hasta la carpeta donde se encuentra el script.

SnapCenter le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript. ["Más información"](#)

- b. En la sección Configuración de parámetros de la base de datos, modifique los valores de los parámetros de base de datos precargados 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 ejecuta en modo de registro de archivo o desea restaurar una base de datos desde el registro de rehacer de archivo, agregue los parámetros y especifique la ruta.

- DESTINO DEL ARCHIVO DE REGISTRO
- ARCHIVO DE REGISTRO DÚPLEX DESTINO



El área de recuperación rápida (FRA) no está definida en los parámetros de la base de datos precargada. Puede configurar FRA agregando los parámetros relacionados.



El valor predeterminado de log_archive_dest_1 es \$ORACLE_HOME/clone_sid y los registros de archivo de la base de datos clonada se crearán en esta ubicación. Si ha eliminado el parámetro log_archive_dest_1, la ubicación del registro de archivo la determina Oracle. Puede definir una nueva ubicación para el registro de archivo editando log_archive_dest_1, pero asegúrese de que el sistema de archivos o el grupo de discos exista y esté disponible en el host.

- a. Haga clic en **Restablecer** para obtener la configuración de los parámetros de la base de datos predeterminada.
10. En la página PostOps, **Recuperar base de datos** y **Hasta cancelar** están seleccionados de forma predeterminada para realizar la recuperación de la base de datos clonada.

SnapCenter realiza la recuperación montando la última copia de seguridad de registro que tiene la secuencia ininterrumpida de registros de archivo después de la copia de seguridad de datos que se seleccionó para clonar. La copia de seguridad del registro y de los datos debe estar en el almacenamiento primario para realizar la clonación en el almacenamiento primario y la copia de seguridad del registro y de los datos debe estar en el almacenamiento secundario para realizar la clonación en el almacenamiento secundario.

Las opciones **Recuperar base de datos** y **Hasta cancelar** no se seleccionan si SnapCenter no logra encontrar las copias de seguridad de registros adecuadas. Puede proporcionar la ubicación del registro de archivo externo si la copia de seguridad del registro no está disponible en **Especificar ubicaciones de registro de archivo externo**. Puede especificar varias ubicaciones de registro.



Si desea clonar una base de datos de origen configurada para admitir el área de recuperación flash (FRA) y Oracle Managed Files (OMF), el destino del registro para la recuperación también debe cumplir con la estructura del directorio OMF.

La página PostOps no se muestra si la base de datos de origen es una base de datos en espera de Data Guard o una base de datos en espera de Data Guard activa. Para una base de datos en espera de Data Guard o en espera de Data Guard activa, SnapCenter no proporciona una opción para seleccionar el tipo de recuperación en la GUI de SnapCenter, pero la base de datos se recupera utilizando el tipo de recuperación Hasta cancelar sin aplicar ningún registro.

Nombre del campo	Descripción
Hasta Cancelar	SnapCenter realiza la recuperación montando la última copia de seguridad del registro que tiene la secuencia ininterrumpida de registros de archivo después de la copia de seguridad de datos que se seleccionó para clonar. 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 una fecha y hora especificadas. El formato aceptado es mm/dd/aaaa hh:mm:ss.  La hora se puede especificar en formato de 24 horas.

Nombre del campo	Descripción
Hasta SCN (Número de cambio del sistema)	SnapCenter recupera la base de datos hasta un número de cambio de sistema (SCN) especificado.
Especificar ubicaciones de registros de archivos externos	Si la base de datos se ejecuta en modo ARCHIVELOG, SnapCenter identifica y monta la cantidad óptima de copias de seguridad de registros según el SCN especificado o la fecha y hora seleccionadas. También puede especificar la ubicación del registro de archivo externo.  SnapCenter no identificará ni montará automáticamente las copias de seguridad del registro si ha seleccionado Hasta cancelar.
Crear nuevo DBID	De forma predeterminada, 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. Desmarque la casilla de verificación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En este escenario, si desea registrar la base de datos clonada con el catálogo RMAN externo donde la base de datos de origen ya está registrada, la operación falla.
Crear un archivo temporal para un espacio de tabla temporal	Seleccione la casilla de verificación si desea crear un archivo temporal para el espacio de tabla temporal predeterminado de la base de datos clonada. Si la casilla de verificación no está seleccionada, el clon de la base de datos se creará sin el archivo temporal.
Introduzca entradas SQL para aplicar cuando se crea el clon	Agregue las entradas SQL que desea aplicar cuando se crea el clon.

Nombre del campo	Descripción
Introduzca scripts para ejecutar después de la operación de clonación	Especifique la ruta y los argumentos del postscript que desea ejecutar después de la operación de clonación. Debes almacenar el postscript en <i>/var/opt/snapcenter/spl/scripts</i> o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta <i>/var/opt/snapcenter/spl/scripts</i>. Si ha colocado el script en alguna carpeta dentro de esta ruta, deberá proporcionar la ruta completa hasta la carpeta donde se encuentra el script.  Si la operación de clonación falla, los postscripts no se ejecutarán y las actividades de limpieza se activarán directamente.

- En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de clonación realizada, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell `Set-SmSmtServer`.

- Revise el resumen y luego haga clic en **Finalizar**.



Al realizar la recuperación como parte de la operación de creación de un clon, incluso si la recuperación falla, el clon se crea con una advertencia. Puede realizar una recuperación manual en este clon para que la base de datos del clon vuelva a un estado consistente.

- Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Resultado

Después de clonar la base de datos, puede actualizar la página de recursos para incluir la base de datos clonada como uno de los recursos disponibles para realizar una copia de seguridad. La base de datos clonada se puede proteger como cualquier otra base de datos utilizando el flujo de trabajo de respaldo estándar o se puede incluir en un grupo de recursos (ya sea recién creado o existente). La base de datos clonada puede ser clonada aún más (clon de clones).

Después de clonar, nunca debes cambiar el nombre de la base de datos clonada.



Si no ha realizado la recuperación durante la clonación, la copia de seguridad de la base de datos clonada podría fallar debido a una recuperación incorrecta y es posible que tenga que realizar una recuperación manual. La copia de seguridad del registro también puede fallar si la ubicación predeterminada que se completó para los registros de archivo está en un almacenamiento que no es NetApp o si el sistema de almacenamiento no está configurado con SnapCenter.

En la configuración de AIX, puede utilizar el comando `lkdev` para bloquear y el comando `rendev` para cambiar el nombre de los discos en los que residía la base de datos clonada.

El bloqueo o cambio de nombre de los dispositivos no afectará la operación de eliminación del clon. Para los diseños AIX LVM creados en dispositivos SAN, no se admitirá el cambio de nombre de los dispositivos SAN clonados.

Encuentre más información

- ["La restauración o clonación falla con el mensaje de error ORA-00308"](#)
- ["No se pudo recuperar una base de datos clonada"](#)
- ["Parámetros personalizables para operaciones de copia de seguridad, restauración y clonación en sistemas AIX"](#)

Actualizar la IP preferida en el host

Una vez completada la operación de clonación, la ruta proporcionada por la capa de acceso al almacenamiento (SAL) al clon tendrá el formato `<nfs_lif_IP>:<JunctionPath>`. Para proporcionar la IP preferida, debe configurarla en el host utilizando los comandos SCCLI.

Pasos

1. Inicie sesión en el host de la base de datos.
2. Iniciar una sesión de conexión de PowerShell con SnapCenter para un usuario específico.

Conexión abierta de Sm

3. Crea un archivo vacío.

```
toque /var/opt/snapcenter/scu/etc/storagepreference.properties
```

4. Configure el LIF de datos preferido para la SVM.

```
Add-SvmPreferredDataPath -SVM <Nombre de SVM> -DataPath <Dirección IP o FQDN>
```

5. Verificar la ruta preferida.

Obtener ruta de datos preferida de Svm

Clonar una base de datos conectable

Puede clonar una base de datos conectable (PDB) a una CDB de destino diferente o igual en el mismo host o en un host alternativo. También puede recuperar el PDB clonado en un SCN o fecha y hora deseados.

Antes de empezar

Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios prescript y postscript.

Pasos

- 1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de tipo instancia única (multiinquilino) 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. Desde la vista Administrar copias, seleccione las copias de seguridad de Copias locales (principales), Copias espejo (secundarias) o Copias de bóveda (secundarias).
- 5. Seleccione la copia de seguridad de la tabla y luego haga clic en *  *.
- 6. En la página Nombre, realice las siguientes acciones:
 - a. Seleccione **PDB Clone**.
 - b. Especifique el PDB que desea clonar.



Solo puedes clonar un PDB a la vez.

- c. Especifique el nombre del PDB clonado.

- 7. En la página Ubicaciones, realice las siguientes acciones:

Para este campo...	Haz esto...
Host clon	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 tenga la misma versión de Oracle y sistema operativo que el host de la base de datos de origen.
Objetivo CDB	Seleccione la CDB donde desea incluir el PDB clonado. Debe asegurarse de que el CDB de destino se esté ejecutando.
Estado de la base de datos	Seleccione la casilla de verificación Abrir el PDB clonado en modo LECTURA-ESCRITURA si desea abrir el PDB en modo LECTURA-ESCRITURA.

Ubicaciones de archivos de datos	De forma predeterminada, se completa la ubicación del archivo de datos. La convención de nombres predeterminada de SnapCenter para los sistemas de archivos SAN o NFS es <code>FileSystemNameofsourcedatabase_SCJOBID</code>. La convención de nombres predeterminada de SnapCenter para los grupos de discos ASM es <code>SC_HASHCODEofDISKGROUP_SCJOBID</code>. El <code>HASHCODEofDISKGROUP</code> es un número generado automáticamente (de 2 a 10 dígitos) que es único para cada grupo de discos ASM.  Si está personalizando el nombre del grupo de discos ASM, asegúrese de que la longitud del nombre cumpla con la longitud máxima admitida por Oracle. Si desea especificar una ruta diferente, debe ingresar los puntos de montaje del archivo de datos o los nombres de los grupos de discos ASM para la base de datos clonada.

Los detalles de inicio, nombre de usuario y grupo de Oracle se completan automáticamente desde la base de datos de origen. Puede cambiar los valores según el entorno de Oracle del host donde se creará el clon.

8. En la página PreOps, realice los siguientes pasos:

- a. Introduzca la ruta y los argumentos del script que desea ejecutar antes de la operación de clonación.

Debes almacenar el script en `/var/opt/snapcenter/spl/scripts` o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta `/var/opt/snapcenter/spl/scripts`. Si ha colocado el script en alguna carpeta dentro de esta ruta, deberá proporcionar la ruta completa hasta la carpeta donde se encuentra el script.

SnapCenter le permite utilizar las variables de entorno predefinidas cuando ejecuta prescript y postscript. ["Más información"](#)

- a. En la sección de configuración de parámetros de la base de datos clonada de CDB auxiliar, modifique los valores de los parámetros de base de datos precargados que se utilizan para inicializar la base de datos.

9. Haga clic en **Restablecer** para obtener la configuración de los parámetros de la base de datos predeterminada.

10. En la página PostOps, **Hasta cancelar** está seleccionado de forma predeterminada para realizar la recuperación de la base de datos clonada.

La opción **Hasta cancelar** no se selecciona si SnapCenter no puede encontrar las copias de seguridad de registros adecuadas. Puede proporcionar la ubicación del registro de archivo externo si la copia de

seguridad del registro no está disponible en **Especificar ubicaciones de registro de archivo externo**. Puede especificar varias ubicaciones de registro.



Si desea clonar una base de datos de origen configurada para admitir el área de recuperación flash (FRA) y Oracle Managed Files (OMF), el destino del registro para la recuperación también debe cumplir con la estructura del directorio OMF.

Nombre del campo	Descripción
Hasta Cancelar	SnapCenter realiza la recuperación montando la última copia de seguridad del registro que tiene la secuencia ininterrumpida de registros de archivo después de la copia de seguridad de datos que se seleccionó para clonar. La copia de seguridad del registro y de los datos debe estar en el almacenamiento primario para realizar la clonación en el almacenamiento primario y la copia de seguridad del registro y de los datos debe estar en el almacenamiento secundario para realizar la clonación 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 una fecha y hora especificadas.  La hora se puede especificar en formato de 24 horas.
Hasta SCN (Número de cambio del sistema)	SnapCenter recupera la base de datos hasta un número de cambio de sistema (SCN) especificado.
Especificar ubicaciones de registros de archivos externos	Especifique la ubicación del registro de archivo externo.
Crear nuevo DBID	De forma predeterminada, la casilla de verificación Crear nuevo DBID no está seleccionada para la base de datos de clonación auxiliar. Seleccione la casilla de verificación si desea generar un número único (DBID) para la base de datos clonada auxiliar que la diferencie de la base de datos de origen.

Nombre del campo	Descripción
Crear un archivo temporal para un espacio de tabla temporal	Seleccione la casilla de verificación si desea crear un archivo temporal para el espacio de tabla temporal predeterminado de la base de datos clonada. Si la casilla de verificación no está seleccionada, el clon de la base de datos se creará sin el archivo temporal.
Introduzca entradas SQL para aplicar cuando se crea el clon	Agregue las entradas SQL que desea aplicar cuando se crea el clon.
Introduzca scripts para ejecutar después de la operación de clonación	Especifique la ruta y los argumentos del postscript que desea ejecutar después de la operación de clonación. Debes almacenar el postscript en <code>/var/opt/snapcenter/spl/scripts</code> o en cualquier carpeta dentro de esta ruta. De forma predeterminada, se completa la ruta <code>/var/opt/snapcenter/spl/scripts</code>. Si ha colocado el script en alguna carpeta dentro de esta ruta, deberá proporcionar la ruta completa hasta la carpeta donde se encuentra el script.  Si la operación de clonación falla, los postscripts no se ejecutarán y las actividades de limpieza se activarán directamente.

11. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de clonación realizada, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell `Set-SmSmtServer`.

12. Revise el resumen y luego haga clic en **Finalizar**.
13. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Después de terminar

Si desea crear una copia de seguridad del PDB clonado, debe realizar una copia de seguridad del CDB de destino donde está clonado el PDB porque no es posible realizar una copia de seguridad solo del PDB clonado. Debe crear una relación secundaria para la CDB de destino si desea crear la copia de seguridad con una relación secundaria.

En una configuración RAC, el almacenamiento del PDB clonado se adjunta únicamente al nodo donde se realizó la clonación del PDB. Los PDB en los otros nodos del RAC están en estado MOUNT. Si desea que el PDB clonado sea accesible desde los otros nodos, debe adjuntar manualmente el almacenamiento a los otros nodos.

Encuentre más información

- ["La restauración o clonación falla con el mensaje de error ORA-00308"](#)
- ["Parámetros personalizables para operaciones de copia de seguridad, restauración y clonación en sistemas AIX"](#)

Clonar copias de seguridad de bases de datos de Oracle mediante comandos UNIX

El flujo de trabajo de clonación incluye la planificación, la ejecución de la operación de clonación y la supervisión de la operación.

Acerca de esta tarea

Debe ejecutar los siguientes comandos para crear el archivo de especificación de clonación de la base de datos Oracle e iniciar la operación de clonación.

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 Oracle a partir de una copia de seguridad especificada: *New-SmOracleCloneSpecification*



Si la política de protección de datos secundaria es espejo-bóveda unificada, especifique solo `-IncludeSecondaryDetails`. No es necesario especificar `-SecondaryStorageType`.

Este comando crea automáticamente un archivo de especificación de clonación de base de datos de Oracle para la base de datos de origen especificada y su copia de seguridad. También debe proporcionar un SID de base de datos clonada para que el archivo de especificación creado tenga los valores generados automáticamente para la base de datos clonada que creará.



El archivo de especificación de clon se crea en `/var/opt/snapcenter/sco/clone_specs`.

2. Iniciar una operación de clonación desde un grupo de recursos de clonación o una copia de seguridad existente: *New-SmClone*

Este comando inicia una operación de clonación. También debe proporcionar una ruta de archivo de especificación de clonación de Oracle para la operación de clonación. También puede especificar las opciones de recuperación, el host donde se realizará la operación de clonación, prescripts, postscripts y otros detalles.

De forma predeterminada, el archivo de destino del registro de archivo para la base de datos clonada se completa automáticamente en `$ORACLE_HOME/CLONE_SIDs`.

Dividir un clon de base de datos Oracle

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["Dividir un volumen FlexClone de su volumen principal"]
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista **Ver**.
3. Seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en .
4. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
5. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si el servicio SMCore se reinicia y las bases de datos en las que se realizó la operación de división de clones aparecen como clones en la página Recursos. Debe ejecutar el cmdlet *Stop-SmJob* para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro CloneSplitStatusCheckPollTime en el archivo SMCoreServiceHost.exe.config para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo,

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clonación solo después de que se completen las operaciones en ejecución.

Clon dividido de una base de datos conectable

Puede utilizar SnapCenter para dividir una base de datos conectable clonada (PDB).

Acerca de esta tarea

Si creó una copia de seguridad de la CDB de destino donde se clonó la PDB, cuando divide el clon de la PDB, la PDB clonada también se elimina de todas las copias de seguridad de la CDB de destino que contienen la PDB clonada.



Los clones de PDB no se muestran en la vista de inventario ni de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Seleccione la base de datos del contenedor de origen (CDB) desde la vista de recursos o del grupo de recursos.
3. Desde la vista Administrar copias, seleccione **Clones** de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).
4. Seleccione el clon PDB (targetCDB:PDBClone) y luego haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Supervisar las operaciones de clonación de bases de datos de Oracle

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego 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

Puede actualizar el clon ejecutando el comando *Refresh-SmClone*. Este comando crea una copia de seguridad de la base de datos, elimina el clon existente y crea un clon con el mismo nombre.



No es posible actualizar un clon PDB.

Lo que necesitarás

- Cree una copia de seguridad completa en línea o una política de copia de seguridad de datos fuera de línea sin copias de seguridad programadas habilitadas.
- Configure la notificación por correo electrónico en la política solo para fallas de copia de seguridad.
- Defina el recuento de retención para las copias de seguridad a pedido de manera adecuada para garantizar que no haya copias de seguridad no deseadas.
- Asegúrese de que solo una copia de seguridad completa en línea o una política de copia de seguridad de datos sin conexión esté asociada con el grupo de recursos identificado para la operación de clonación de actualización.
- Cree un grupo de recursos con una sola base de datos.
- Si se crea un trabajo cron para el comando de actualización de clonación, asegúrese de que las programaciones de SnapCenter y las programaciones de cron no se superpongan para el grupo de recursos de la base de datos.

Para un trabajo cron creado para el comando de actualización de clonación, asegúrese de ejecutar Open-SmConnection cada 24 horas.

- Asegúrese de que el SID del clon sea único para un host.

Si varias operaciones de actualización de clones usan el mismo archivo de especificación de clones o usan el archivo de especificación de clones con el mismo SID de clon, se eliminará el clon existente con el SID en el host y luego se creará el clon.

- Asegúrese de que la política de respaldo esté habilitada con protección secundaria y que el archivo de especificación de clonación se cree con “-IncludeSecondaryDetails” para crear los clones utilizando copias de seguridad secundarias.

- Si se especifica el archivo de especificación del clon principal, pero la política tiene seleccionada la opción de actualización secundaria, se creará la copia de seguridad y la actualización se transferirá a la secundaria. Sin embargo, el clon se creará a partir de la copia de seguridad principal.
- Si se especifica el archivo de especificación del clon principal y la política no tiene seleccionada la opción de actualización secundaria, la copia de seguridad se creará en el principal y el clon se creará desde el principal.

Pasos

1. Iniciar una sesión de conexión con el servidor SnapCenter para un usuario específico: *Open-SmConnection*
2. Cree una especificación de clon de base de datos Oracle a partir de una copia de seguridad especificada: *New-SmOracleCloneSpecification*



Si la política de protección de datos secundaria es espejo-bóveda unificada, especifique solo `-IncludeSecondaryDetails`. No es necesario especificar `-SecondaryStorageType`.

Este comando crea automáticamente un archivo de especificación de clonación de base de datos de Oracle para la base de datos de origen especificada y su copia de seguridad. También debe proporcionar un SID de base de datos clonada para que el archivo de especificación creado tenga los valores generados automáticamente para la base de datos clonada que creará.



El archivo de especificación de clon se crea en `/var/opt/snapcenter/sco/clone_specs`.

3. Ejecute *Refresh-SmClone*.

Si la operación falla con el mensaje de error "PL-SCO-20032: la operación canExecute falló con el error: PL-SCO-30031: existe el archivo de registro de rehacer +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log", especifique un valor más alto 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 conectable

Puede eliminar el clon de una base de datos conectable (PDB) si ya no la necesita.

Si creó una copia de seguridad de la CDB de destino donde se clonó la PDB, cuando elimina la clonación de la PDB, la PDB clonada también se elimina de la copia de seguridad de la CDB de destino.



Los clones de PDB no se muestran en la vista de inventario ni de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Seleccione la base de datos del contenedor de origen (CDB) desde la vista de recursos o del grupo de recursos.
3. Desde la vista Administrar copias, seleccione **Clones** de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).

4. Seleccione el clon PDB (targetCDB:PDBClone) y luego haga clic en  .
5. Haga clic en **Aceptar**.

Administrar volúmenes de aplicaciones

¿Qué son los volúmenes de aplicación?

Los volúmenes de aplicación son el almacenamiento donde se guarda información como configuración, instalador y otros archivos que no son datos relacionados con la base de datos de Oracle.

El complemento SnapCenter para Oracle Database le permite crear copias de seguridad consistentes de los volúmenes de aplicaciones (volúmenes que no son de datos) junto con las bases de datos Oracle.

El complemento automatiza la copia de seguridad y la clonación de volúmenes de aplicaciones.

- Proteja los volúmenes de aplicaciones junto con los volúmenes de bases de datos de Oracle en un solo grupo de recursos.
- Crear copias de seguridad de los volúmenes de aplicaciones.
- Cree copias de seguridad de bases de datos de Oracle junto con volúmenes de aplicaciones.
- Cree clones de bases de datos junto con volúmenes de aplicaciones hasta un punto en el tiempo.
- Programar operaciones de respaldo.
- Supervisar todas las operaciones.
- Ver informes de operaciones de copia de seguridad y clonación.

Agregar volúmenes de aplicaciones

SnapCenter admite la realización de copias de seguridad y la clonación de volúmenes de aplicaciones de bases de datos Oracle. Debes agregar manualmente los volúmenes de la aplicación. No se admite el descubrimiento automático de volúmenes de aplicaciones.



Los volúmenes de aplicación solo admiten conexiones NFS directas y iSCSI directas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. Haga clic en **Agregar volumen de aplicación**.
3. En la página Nombre, realice las siguientes acciones:
 - En el campo Nombre, ingrese el nombre del volumen de la aplicación.
 - En el campo Nombre de host, ingrese el nombre del host.
4. En la página Huella de almacenamiento, ingrese el nombre del sistema de almacenamiento, seleccione uno o más volúmenes y especifique los LUN o Qtrees asociados.

Puede agregar varios sistemas de almacenamiento.

5. Revise el resumen y luego haga clic en **Finalizar**.
6. En la página Recursos, seleccione **Volumen de aplicación** de la lista **Ver** para ver todos los volúmenes de aplicación que ha agregado.

Modificar el volumen de la aplicación

Puede modificar todos los valores que especificó al agregar el volumen de la aplicación, si no se crean copias de seguridad. Si se crea la copia de seguridad, solo podrá modificar los detalles del sistema de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Volumen de la aplicación** de la lista **Ver**.
3.
Hacer clic  para modificar los valores.
4.
Hacer clic  para modificar los valores.

Eliminar el volumen de la aplicación

Cuando elimina un volumen de aplicación, si hay copias de seguridad asociadas con el volumen de aplicación, este se colocará en modo de mantenimiento y no se crearán copias de seguridad nuevas ni se conservarán las copias de seguridad anteriores. Si no hay copias de seguridad asociadas, se eliminarán todos los metadatos.

Si es necesario, SnapCenter le permite deshacer la operación de eliminación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Volumen de la aplicación** de la lista **Ver**.
3. Hacer clic  Eliminar icono] para modificar los valores.

Volúmenes de aplicaciones de respaldo

Realizar una copia de seguridad del volumen de la aplicación

Si el volumen de la aplicación no es parte de ningún grupo de recursos, puede realizar una copia de seguridad del volumen de la aplicación desde la página Recursos.

Acerca de esta tarea

De forma predeterminada, se crean copias de seguridad del grupo de consistencia (CG). Si desea crear copias de seguridad basadas en volumen, debe establecer el valor de **EnableOracleNdvVolumeBasedBackup** en verdadero en el archivo *web.config*.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Volumen de la aplicación** de la lista **Ver**.
3. Haga clic en  y luego seleccione el nombre del host y el tipo de base de datos para filtrar los recursos.

Luego puedes hacer clic en  para cerrar el panel de filtro.

4. Seleccione el volumen de la aplicación que desea respaldar.

Se muestra la página Proteger volumen de la aplicación.

5. En la página Recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación y luego ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea. Por ejemplo, customtext__policy_hostname o resource_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.
Excluir destinos de registro de archivo de la copia de seguridad	Especifique los destinos de los archivos de registro de archivo que no desea respaldar.

6. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

policy_name es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto

del correo electrónico. Si desea adjuntar el informe de la operación de respaldo realizada en el recurso, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell `Set-SmSmtServer`.

8. Revise el resumen y luego haga clic en **Finalizar**.

Se muestra la página de topología del volumen de la aplicación.

9. Haga clic en **Hacer copia de seguridad ahora**.

10. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.
- b. Haga clic en **Copia de seguridad**.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Realizar una copia de seguridad del grupo de recursos de volúmenes de la aplicación

Puede realizar una copia de seguridad del grupo de recursos que contiene solo volúmenes de aplicaciones o una combinación de volúmenes de aplicaciones y bases de datos. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Si el grupo de recursos tiene varios volúmenes de aplicaciones, todos los volúmenes de aplicaciones deben tener la política de replicación SnapMirror o SnapVault.

Acerca de esta tarea

De forma predeterminada, se crean copias de seguridad del grupo de consistencia (CG). Si desea crear copias de seguridad basadas en volumen, debe establecer el valor de **EnableOracleNdvVolumeBasedBackup** en verdadero en el archivo *web.config*.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o haciendo clic en  * y luego seleccionando la etiqueta. Luego puedes hacer clic en  * para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y haga clic en **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si ha asociado varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.



La operación de verificación se realizará solo para las bases de datos y no para los volúmenes de la aplicación.

Copia de seguridad del volumen de la aplicación clonada

Puede utilizar SnapCenter para clonar las copias de seguridad del volumen de la aplicación.

Antes de empezar

Si ha instalado el complemento como un usuario no root, debe asignar manualmente los permisos de ejecución a los directorios prescript y postscript.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Volumen de la aplicación** de la lista **Ver**.
3. Seleccione el volumen de la aplicación desde la vista de detalles del volumen de la aplicación o desde la vista de detalles del grupo de recursos.

Se muestra la página de topología del volumen de la aplicación.

4. Desde la vista Administrar copias, seleccione las copias de seguridad de Copias locales (principales), Copias espejo (secundarias) o Copias de bóveda (secundarias).
5. Seleccione la copia de seguridad de la tabla y luego haga clic en *  *.
6. En la página Ubicación, realice las siguientes acciones:

Para este campo...	Haz esto...
Host de complementos	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 ejecutarán antes de la clonación, los comandos para montar un sistema de archivos y los nombres de los scripts que se ejecutarán después de la clonación.
8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de clonación realizada, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

9. Revise el resumen y luego haga clic en **Finalizar**.

Dividir un clon de volumen de aplicación

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Volumen de la aplicación** de la lista **Ver**.
3. Seleccione el recurso clonado y haga clic .
4. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
5. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Eliminar un clon de volumen de aplicación

Puedes eliminar clones si consideras que ya no son necesarios. No puedes eliminar clones que actúen como fuente para otros clones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento Oracle Database de la lista.
2. En la página Recursos, seleccione **Volumen de la aplicación** de la lista **Ver**.
3. Seleccione el recurso o grupo de recursos de la lista.

Se muestra la página de topología del recurso o del grupo de recursos.
4. Desde la vista Administrar copias, seleccione **Clones** de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).
5. Seleccione el clon y luego haga clic .
6. En la página Eliminar clon, realice las siguientes acciones:
 - a. En el campo **Eliminar antes del clon**, ingrese los nombres de los scripts que se ejecutarán antes de eliminar el clon.
 - b. En el campo **Desmontar**, ingrese los comandos para desmontar el clon antes de eliminarlo.
7. Haga clic en **Aceptar**.

Proteger los sistemas de archivos de Windows

Conceptos del complemento SnapCenter para Microsoft Windows

Descripción general del complemento SnapCenter para Microsoft Windows

El complemento SnapCenter para Microsoft Windows es un componente del lado del host del software SnapCenter de NetApp que permite la gestión de protección de datos consciente de la aplicación de los recursos del sistema de archivos de Microsoft. Además, proporciona aprovisionamiento de almacenamiento, consistencia de instantáneas y recuperación de espacio para sistemas de archivos de Windows. El complemento para Windows automatiza las operaciones de copia de seguridad, restauración y clonación del sistema de archivos en su entorno de SnapCenter .

Cuando se instala el complemento para Windows, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen y con la tecnología NetApp SnapVault para realizar replicación de copias de seguridad de disco a disco para archivado o cumplimiento de estándares.

- Habilita la protección de datos basada en aplicaciones para otros complementos que se ejecutan en hosts de Windows en su entorno de SnapCenter
- Automatiza operaciones de copia de seguridad, restauración y clonación basadas en aplicaciones para sistemas de archivos de Microsoft en su entorno de SnapCenter
- Admite aprovisionamiento de almacenamiento, consistencia de instantáneas y recuperación de espacio para hosts de Windows



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

Qué puede hacer con el complemento SnapCenter para Microsoft Windows

Cuando el complemento para Windows esté instalado en su entorno, podrá utilizar SnapCenter para realizar copias de seguridad, restaurar y clonar sistemas de archivos de Windows. También puede realizar tareas de apoyo a dichas operaciones.

- Descubra recursos
- Realizar copias de seguridad de los sistemas de archivos de Windows
- Programar operaciones de respaldo
- Restaurar copias de seguridad del sistema de archivos
- Copias de seguridad del sistema de archivos clonado
- Supervisar operaciones de copia de seguridad, restauración y clonación



El complemento para Windows no admite la realización de copias de seguridad ni la restauración de sistemas de archivos en recursos compartidos SMB.

Características del complemento SnapCenter para Windows

El complemento para Windows se integra con la tecnología NetApp Snapshot en el sistema de almacenamiento. Para trabajar con el complemento para Windows, utilice la interfaz de SnapCenter .

El complemento para Windows incluye estas características principales:

- **Interfaz gráfica de usuario unificada impulsada por SnapCenter**

La interfaz de SnapCenter le proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite completar procesos de copia de seguridad y restauración consistentes en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y monitorear trabajos en todos los complementos. SnapCenter también ofrece programación centralizada y gestión de políticas para respaldar operaciones de copia de seguridad y clonación.

- **Administración central automatizada**

Puede programar copias de seguridad rutinarias del sistema de archivos, configurar la retención de copias de seguridad basada en políticas y configurar operaciones de restauración. También puede supervisar de forma proactiva el entorno de su sistema de archivos configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología NetApp Snapshot sin interrupciones**

El complemento para Windows utiliza la tecnología NetApp Snapshot. Esto le permite realizar copias de seguridad de los sistemas de archivos en segundos y restaurarlos rápidamente sin desconectar el host. Las instantáneas consumen un espacio de almacenamiento mínimo.

Además de estas características principales, el complemento para Windows ofrece los siguientes beneficios:

- Soporte para flujos de trabajo de copia de seguridad, restauración y clonación
- Seguridad respaldada por RBAC y delegación de roles centralizada
- Creación de copias que ahorran espacio de los sistemas de archivos de producción para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

Para obtener información sobre la licencia de FlexClone , consulte "[Licencias de SnapCenter](#)" .

- Capacidad de ejecutar múltiples copias de seguridad al mismo tiempo en varios servidores
- Cmdlets de PowerShell para la creación de scripts de operaciones de copia de seguridad, restauración y clonación
- Soporte para copias de seguridad de sistemas de archivos y discos de máquinas virtuales (VMDK)
- Soporte para infraestructuras físicas y virtualizadas
- Compatibilidad con iSCSI, canal de fibra, FCoE, mapeo de dispositivos sin procesar (RDM), mapeo de LUN asimétrico (ALM), VMDK sobre NFS y VMFS, y FC virtual.
- Compatibilidad con memoria no volátil express (NVMe) en Windows Server 2022

- Flujos de trabajo de copia de seguridad, restauración, clonación y verificación en el diseño VMDK creado en NVMe a través de TCP/IP.
- Admite la versión de firmware NVMe 1.3 a partir de la actualización 2 de ESX 8.0 y requiere la versión de hardware virtual 21.
- El clúster de conmutación por error de Windows Server (WSFC) no es compatible con aplicaciones a través de VMDK en NVMe sobre TCP/IP.
- Admite la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios comerciales sigan funcionando incluso en caso de una falla total del sitio, permitiendo que las aplicaciones conmuten por error de manera transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una conmutación por error con la sincronización activa de SnapMirror .

Cómo SnapCenter realiza copias de seguridad de los sistemas de archivos de Windows

SnapCenter utiliza la tecnología Snapshot para realizar copias de seguridad de los recursos del sistema de archivos de Windows que residen en LUN, CSV (volúmenes compartidos de clúster), volúmenes RDM (asignación de dispositivos sin procesar), ALM (asignación de LUN asimétrica) en clústeres de Windows y VMDK basados en VMFS/NFS (sistema de archivos de máquina virtual VMware que utiliza NFS).

SnapCenter crea copias de seguridad mediante la creación de instantáneas de los sistemas de archivos. Las copias de seguridad federadas, en las que un volumen contiene LUN de varios hosts, son más rápidas y eficientes que las copias de seguridad de cada LUN individual porque solo se crea una instantánea del volumen en comparación con las instantáneas individuales de cada sistema de archivos.

Cuando SnapCenter crea una instantánea, todo el volumen del sistema de almacenamiento se captura en la instantánea. Sin embargo, la copia de seguridad sólo es válida para el servidor host para el que se creó.

Si los datos de otros servidores host residen en el mismo volumen, estos datos no se pueden restaurar desde la instantánea.



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 una copia de seguridad de una base de datos, debe utilizar uno de los complementos de base de datos.

Tipos de almacenamiento compatibles con el complemento SnapCenter para Microsoft Windows

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas físicas como virtuales. Debe verificar si hay soporte disponible para su tipo de almacenamiento antes de instalar el paquete para su host.

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 [https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"Herramienta de matriz de interoperabilidad de NetApp\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\) .

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Servidor físico	LUN conectados a FC	Interfaz gráfica de usuario (GUI) de SnapCenter o cmdlets de PowerShell	
Servidor físico	LUN conectados a iSCSI	GUI de SnapCenter o cmdlets de PowerShell	
Servidor físico	Recursos compartidos SMB3 (CIFS) que residen en una máquina virtual de almacenamiento (SVM)	GUI de SnapCenter o cmdlets de PowerShell	Soporte únicamente para aprovisionamiento.
Máquina virtual de VMware	LUN RDM conectados mediante un HBA FC o iSCSI	Cmdlets de PowerShell	
Máquina virtual de VMware	LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI	GUI de SnapCenter o cmdlets de PowerShell	
Máquina virtual de VMware	Sistemas de archivos de máquinas virtuales (VMFS) o almacenes de datos NFS	VMware vSphere	
Máquina virtual de VMware	Un sistema invitado conectado a recursos compartidos SMB3 que residen en una SVM	GUI de SnapCenter o cmdlets de PowerShell	Soporte únicamente para aprovisionamiento.
Máquina virtual de VMware	Almacenes de datos vVol tanto en NFS como en SAN	Herramientas ONTAP para VMware vSphere	

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Máquina virtual Hyper-V	LUN de FC virtuales (vFC) conectados mediante un conmutador de canal de fibra virtual	GUI de SnapCenter o cmdlets de PowerShell	Debe utilizar Hyper-V Manager para aprovisionar LUN de FC virtual (vFC) conectados mediante un conmutador de canal de fibra virtual.  No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .
Máquina virtual Hyper-V	LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI	GUI de SnapCenter o cmdlets de PowerShell	 No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Máquina virtual Hyper-V	Un sistema invitado conectado a recursos compartidos SMB3 que residen en una SVM	GUI de SnapCenter o cmdlets de PowerShell	Soporte únicamente para aprovisionamiento.  No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .

Privilegios mínimos de ONTAP necesarios para el complemento de Windows

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo
 - lun crear
 - eliminar lun
 - agregar igroup lun
 - crear igroup lun
 - eliminar igroup lun
 - Cambiar nombre de igroup lun
 - Programa de igroup de Lun
 - Asignación de LUN a nodos de informes adicionales
 - creación de mapeo LUN
 - eliminar mapeo lun
 - Mapeo de LUN: eliminar nodos de informes
 - espectáculo de mapeo de lun
 - modificar lun

- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen

- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFs de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIF de vserver
- Mostrar copia de sombra de CIF de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi
- Mostrar conexión iscsi de vserver
- espectáculo vserver
- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red
 - Mostrar interfaz de red
 - vserver

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Definir una estrategia de respaldo para los sistemas de archivos de Windows

Definir una estrategia de respaldo antes de crear sus copias de seguridad le proporcionará las copias de seguridad que necesita para restaurar o clonar con éxito sus sistemas de archivos. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Un SLA define el nivel de servicio que se espera y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. RPO define la estrategia para la edad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA, RTO y RPO contribuyen a la estrategia de protección de datos.

Programaciones de copias de seguridad para sistemas de archivos de Windows

La frecuencia de las copias de seguridad se especifica en las políticas; una programación de copias de seguridad se especifica en la configuración del grupo de recursos. El factor más crítico a la hora de determinar la frecuencia o el cronograma de una copia de seguridad es la tasa de cambio del recurso y la importancia de los datos. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su Acuerdo de Nivel de Servicio (SLA) y su Objetivo de Punto de Recuperación (RPO).

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso para un recurso muy utilizado, no es necesario ejecutar una copia de seguridad completa más de una o dos veces al día.

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de respaldo

La frecuencia de las copias de seguridad (con qué frecuencia se deben realizar las copias de seguridad), denominada *tipo de programación* para algunos complementos, es parte de una configuración de políticas. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual, o puede especificar **Ninguno**, lo que hace que la política sea solo a pedido. Puede acceder a las políticas haciendo clic en **Configuración > Políticas**.

- Programaciones de copias de seguridad

Las programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad) son parte de la configuración de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para realizar copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos > Grupos de recursos**.

Número de copias de seguridad necesarias para los sistemas de archivos de Windows

Los factores que determinan la cantidad de copias de seguridad que necesita incluyen el tamaño del sistema de archivos de Windows, la cantidad de volúmenes utilizados, la tasa de cambio del sistema de archivos y su Acuerdo de Nivel de Servicio (SLA).

Convención de nomenclatura de copias de seguridad para sistemas de archivos de Windows

Las copias de seguridad del sistema de archivos de Windows utilizan la convención de nombres de instantáneas predeterminada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:
resourcegroupname_hostname_timestamp

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de 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 tiempo.

Al crear una copia de seguridad, también puede agregar una etiqueta descriptiva para ayudar a identificar la copia de seguridad. Por el contrario, si desea utilizar una convención de nombres de copia de seguridad personalizada, deberá cambiar el nombre de la copia de seguridad una vez completada la operación.

Opciones de retención de copias de seguridad

Puede elegir la cantidad de días durante los cuales desea conservar copias de seguridad o especificar la cantidad de copias de seguridad que desea conservar, hasta un máximo de 255 copias en ONTAP . Por ejemplo, su organización podría exigirle que conserve 10 días de copias de seguridad o 130 copias de seguridad.

Al crear una política, puede especificar las opciones de retención para el tipo de copia de seguridad y el tipo de programación.

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

SnapCenter elimina las copias de seguridad retenidas que tienen etiquetas de retención que coinciden con el tipo de programación. Si se modificó el tipo de programación del recurso o del grupo de recursos, es posible que las copias de seguridad con la etiqueta del tipo de programación anterior aún permanezcan en el sistema.



Para la retención a largo plazo de copias de seguridad, debe utilizar la copia de seguridad SnapVault .

Orígenes y destinos de clones para sistemas de archivos de Windows

Puede clonar una copia de seguridad del sistema de archivos desde el almacenamiento primario o secundario. También puede elegir el destino que admita sus requisitos; ya sea la ubicación de respaldo original o un destino diferente en el mismo host o en un host diferente. El destino debe estar en el mismo volumen que la copia de seguridad de origen del clon.

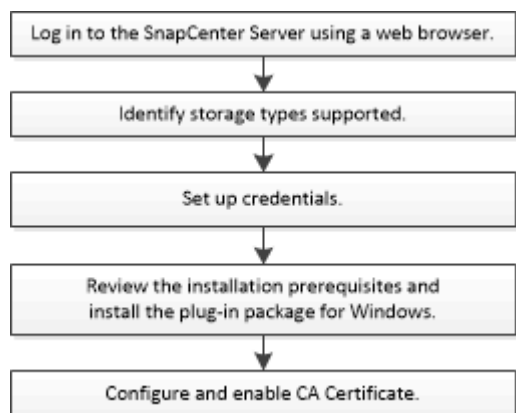
Clonar destino	Descripción
Original, fuente, ubicación	De forma predeterminada, SnapCenter almacena el clon en la misma ubicación y el mismo host que la copia de seguridad que se está clonando.
Ubicación diferente	Puede almacenar el clon en una ubicación diferente en el mismo host o en un host diferente. El host debe tener una conexión configurada a la máquina virtual de almacenamiento (SVM).

Puede cambiar el nombre del clon una vez completada la operación de clonación.

Instalar el complemento SnapCenter para Microsoft Windows

Flujo de trabajo de instalación del complemento SnapCenter para Microsoft Windows

Debe instalar y configurar el complemento SnapCenter para Microsoft Windows si desea proteger archivos de Windows que no sean archivos de base de datos.



Requisitos de instalación del complemento SnapCenter para Microsoft Windows

Debe tener en cuenta ciertos requisitos de instalación antes de instalar el complemento para Windows.

Antes de comenzar a utilizar el complemento para Windows, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas previas requeridas.

- Debe tener privilegios de administrador de SnapCenter para instalar el complemento para Windows.

El rol de administrador de SnapCenter debe tener privilegios de administrador.

- Debe tener instalado y configurado el servidor SnapCenter .
- Al instalar un complemento 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 configurar SnapMirror y SnapVault si desea replicar la copia de seguridad.

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.

Artículo	Requisitos
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Configure sus credenciales para el complemento para Windows

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en los sistemas de archivos de Windows.

Lo que necesitarás

- Debe configurar las credenciales de Windows antes de instalar complementos.
- Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador, en el host remoto.
- Si configura credenciales para grupos de recursos individuales y el usuario no tiene privilegios de administrador completos, debe asignarle al menos los privilegios de grupo de recursos y de respaldo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, haga lo siguiente:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña utilizados para la autenticación. - Administrador del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es el siguiente: UserName No utilice comillas dobles (") ni tildes invertidas (´) en las contraseñas. No debe utilizar los símbolos menor que (<) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que<!10, menos que10<!, acento grave`12.
Password	Introduzca la contraseña utilizada para la autenticación.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Configurar gMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio

administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -Effectivelmmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Añade objetos de computadora 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,...>  
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de  
servicio.
```

4. Configure el gMSA en sus hosts:
 - a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
 - b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
 - c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Agregar hosts e instalar el complemento SnapCenter para Microsoft Windows

Puede utilizar la página Agregar host de SnapCenter para agregar hosts de Windows. El complemento SnapCenter para Microsoft Windows se instala automáticamente en el host especificado. Este es el método recomendado para instalar complementos. Puede agregar un host e instalar un complemento 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 complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
 - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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 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 de ejecución.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar la cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para el sistema de archivos de Windows"](#)

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .
- complementos de Windows
 - Microsoft Windows
 - Servidor Microsoft Exchange
 - Microsoft SQL Server
 - SAP HANA
- Instalación de complementos en un clúster

Si instala complementos en un clúster (WSFC, Oracle RAC o Exchange DAG), se instalan en todos los nodos del clúster.

- Almacenamiento de la serie E

No es posible instalar el complemento para Windows en un host Windows conectado al almacenamiento de la serie E.



SnapCenter no admite la adición del mismo host (host de complemento) a SnapCenter si el host ya es parte de un grupo de trabajo y cambió a otro dominio o viceversa. Si desea agregar el mismo host, debe eliminarlo de SnapCenter y agregarlo nuevamente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Asegúrese de que **Hosts administrados** esté seleccionado en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, haga lo siguiente:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host Windows. SnapCenter Server agrega el host y luego instala el complemento para Windows si aún no está instalado en el host.

Para este campo...	Haz esto...
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el nombre de dominio completo (FQDN). Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • Agrupación en clústeres de conmutación por error de Windows Server (WSFC) Si está agregando un host mediante SnapCenter y es parte de un subdominio, debe proporcionar el FQDN.
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree las nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre cómo crear una credencial. Los detalles sobre las credenciales, incluido el nombre de usuario, el dominio y el tipo de host, se muestran al colocar el cursor sobre el nombre de la credencial proporcionada.  El modo de autenticación está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea instalar.

Para las nuevas implementaciones, no se enumeran paquetes de complementos.

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.
Ruta de instalación	La ruta predeterminada es C:\Archivos de programa\ NetApp\ SnapCenter. Opcionalmente puedes personalizar la ruta. Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\ NetApp\ SnapCenter. Sin embargo, si lo desea, puede personalizar la ruta predeterminada.
Agregar todos los hosts en el clúster	Seleccione esta casilla de verificación para agregar todos los nodos del clúster en un WSFC.
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento. Proporcione el nombre de gMSA en el siguiente formato: <i>domainName\accountName\$</i>.  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla **Omitir comprobaciones previas**, se valida el host para comprobar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell,

la versión de .NET y la ubicación se verifican según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Supervisar el progreso de la instalación.

Instalar el complemento SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell

Si desea instalar el complemento SnapCenter para Microsoft Windows en varios hosts a la vez, puede hacerlo mediante el `Install-SmHostPackage` Cmdlet de PowerShell.

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar complementos.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión utilizando el `Open-SmConnection` cmdlet y luego ingrese sus credenciales.
3. Agregue el host independiente o el clúster a SnapCenter mediante el `Add-SmHost` cmdlet y los parámetros requeridos.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

4. Instale el complemento en varios hosts mediante el `Install-SmHostPackage` cmdlet y los parámetros requeridos.

Puedes utilizar el `-skipprecheck` Opción cuando ha instalado los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.

Instale el complemento SnapCenter para Microsoft Windows de forma silenciosa desde la línea de comandos

Puede instalar el complemento de SnapCenter para Microsoft Windows localmente en un host de Windows si no puede instalar el complemento de forma remota desde la GUI de SnapCenter . Puede ejecutar el programa de instalación del complemento SnapCenter para Microsoft Windows sin supervisión, en modo silencioso, desde la línea de comandos de Windows.

Antes de empezar

- Debe tener instalado el paquete de alojamiento ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores).

- Debe tener instalado PowerShell 7.4.2 o posterior.
- Debes ser un administrador local en el host.

Pasos

1. Descargue el complemento SnapCenter para Microsoft Windows desde su ubicación de instalación.

Por ejemplo, la ruta de instalación predeterminada es C:\ProgramData\NetApp\SnapCenter\Package Repository.

Se puede acceder a esta ruta desde el host donde está instalado el servidor SnapCenter .

2. Copie el archivo de instalación en el host en el que desea instalar el complemento.
3. Desde el símbolo del sistema, navegue hasta el directorio donde descargó el archivo de instalación.
4. Ingrese el siguiente comando, reemplazando las variables con 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 pasados durante la instalación del complemento para Windows distinguen entre mayúsculas y minúsculas.

Introduzca los valores para las siguientes variables:

Variable	Valor
/debuglog"<Ruta_del_registro_de_depuración>	Especifique el nombre y la ubicación del archivo de registro del instalador de la suite, como en el siguiente ejemplo: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
PUERTO BI_SNAPCENTER	Especifique el puerto en el que SnapCenter se comunica con SMCORE.
SUITE_INSTALLDIR	Especifique el directorio de instalación del paquete del complemento de host.
BI_CUENTA DE SERVICIO	Especifique el complemento SnapCenter para la cuenta de servicio web de Microsoft Windows.

Variable	Valor
BI_SERVICEPWD	Especifique la contraseña para la cuenta de servicio web del complemento SnapCenter para Microsoft Windows.
Instalación de ISFeature	Especifique la solución que SnapCenter implementará en el host remoto.

El parámetro *debuglog* incluye la ruta del archivo de registro de SnapCenter. Escribir en este archivo de registro es el método preferido para obtener información de solución de problemas, porque el archivo contiene los resultados de las comprobaciones que realiza la instalación para verificar los requisitos previos del complemento.

Si es necesario, puede encontrar información adicional de solución de problemas en el archivo de registro del paquete SnapCenter para Windows. Los archivos de registro del paquete se enumeran (el más antiguo primero) en la carpeta *%Temp%*, por ejemplo, *C:\temp*.



La instalación del complemento para Windows registra el complemento en el host y no en el servidor SnapCenter. Puede registrar el complemento en el servidor SnapCenter agregando el host mediante la GUI de SnapCenter o el cmdlet de PowerShell. Una vez agregado el host, el complemento se descubre automáticamente.

Supervisar el estado de instalación del paquete de complementos de SnapCenter

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página **Trabajos**. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página **Trabajos** e indican el estado de la operación:

- En curso
- Completado exitosamente
- Fallido
- Completado con advertencias o no se pudo iniciar debido a advertencias
- En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.

- c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
- d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y haga clic en **Archivo > Agregar o quitar complemento**.
2. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
3. En la ventana del complemento Certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
4. Haga clic en **Consola raíz > Certificados – Equipo local > Autoridades de certificación raíz de confianza > Certificados**.
5. Haga clic con el botón derecho en la carpeta "Autoridades de certificación raíz de confianza" y luego seleccione **Todas las tareas > Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Huella digital**.
 - d. Copia los caracteres hexadecimales del cuadro.
 - e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

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

```
Get-ChildItem -Path Certificado:\LocalMachine\Mi
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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"
```

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.

3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Instalar el SnapCenter Plug-in for VMware vSphere

Si su base de datos o sistema de archivos está almacenado en máquinas virtuales (VM), o si desea proteger las VM y los almacenes de datos, debe implementar el SnapCenter Plug-in for VMware vSphere .

Para obtener información sobre la implementación, consulte ["Descripción general de la implementación"](#) .

Implementar certificado de CA

Para configurar el certificado CA con el SnapCenter Plug-in for VMware vSphere, consulte ["Crear o importar certificado SSL"](#) .

Configurar el archivo CRL

El SnapCenter Plug-in for VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL para el SnapCenter Plug-in for VMware vSphere es `/opt/netapp/config/crl`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Realizar copias de seguridad de los sistemas de archivos de Windows

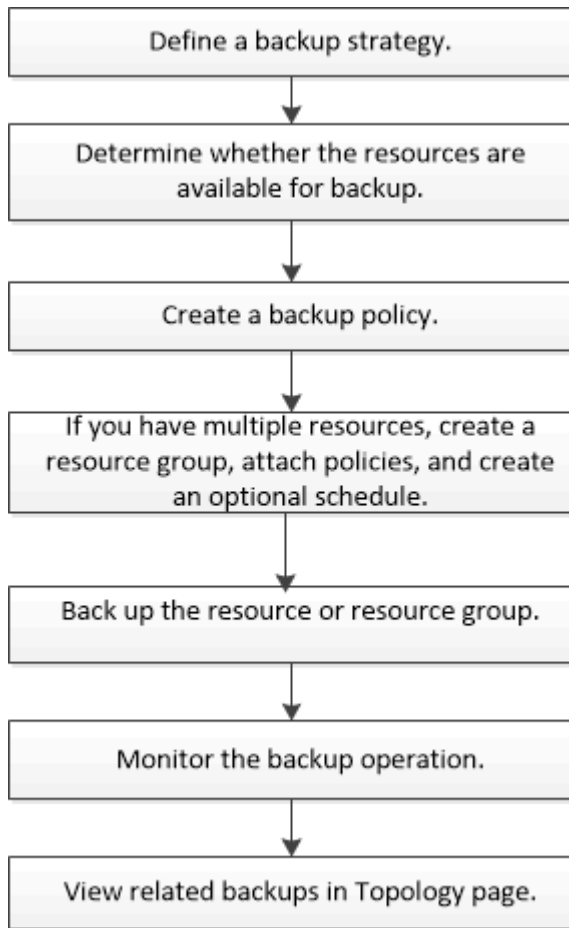
Realizar copias de seguridad de los sistemas de archivos de Windows

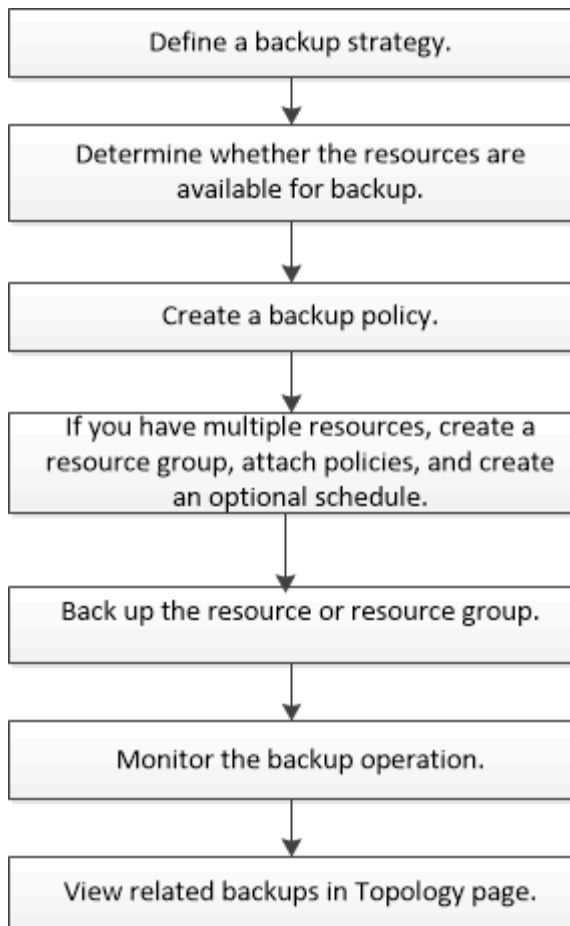
Cuando instala el complemento SnapCenter para Microsoft Windows en su entorno, puede usar SnapCenter para realizar copias de seguridad de los sistemas de archivos de Windows. Puede realizar una copia de seguridad de un solo sistema de archivos o de un grupo de recursos que contenga varios sistemas de archivos. Puede realizar copias de

seguridad a pedido o según un programa de protección definido.

Puede programar varias copias de seguridad para que se ejecuten en todos los servidores simultáneamente. Las operaciones de copia de seguridad y restauración no se pueden realizar simultáneamente en el mismo recurso.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar las operaciones de copia de seguridad:





También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter o el ["Guía de referencia de cmdlets del software SnapCenter"](#) Contiene información detallada sobre los cmdlets de PowerShell.

Determinar la disponibilidad de recursos para los sistemas de archivos de Windows

Los recursos son los LUN y componentes similares en su sistema de archivos que son mantenidos por los complementos que ha instalado. Puede agregar esos recursos a grupos de recursos para poder realizar trabajos de protección de datos en múltiples recursos, pero primero debe identificar qué recursos tiene disponibles. Al descubrir los recursos disponibles también se verifica que la instalación del complemento se haya completado correctamente.

Antes de empezar

- Ya debe haber completado tareas como instalar SnapCenter Server, agregar hosts, crear conexiones de máquinas virtuales de almacenamiento (SVM) y agregar credenciales.
- Si los archivos residen en LUN o VMDK de VMware RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter. Para obtener más información, consulte ["Documentación del SnapCenter Plug-in for VMware vSphere"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.

2. En la página Recursos, seleccione **Sistemas de archivos** de la lista.
3. Seleccione el host para filtrar la lista de recursos y luego haga clic en **Actualizar recursos**.

Los sistemas de archivos recientemente agregados, renombrados o eliminados se actualizan en el inventario de SnapCenter Server.



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

Crear políticas de respaldo para sistemas de archivos de Windows

Puede crear una nueva política de respaldo para los recursos antes de usar SnapCenter para realizar copias de seguridad de los sistemas de archivos de Windows, o puede crear una nueva política de respaldo en el momento en que crea un grupo de recursos o cuando realiza una copia de seguridad de un recurso.

Antes de empezar

- Debes haber definido tu estrategia de backup. "[Más información](#)"
- Debes estar preparado para la protección de datos.

Para prepararse para la protección de datos, debe completar tareas como instalar SnapCenter, agregar hosts, descubrir recursos y crear conexiones de máquinas virtuales de almacenamiento (SVM).

- Si está replicando instantáneas en un espejo o almacenamiento secundario de bóveda, el administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino.
- Si desea ejecutar los scripts de PowerShell en prescripts y postscripts, debe establecer el valor del parámetro usePowershellProcessforScripts en verdadero en el archivo web.config.

El valor predeterminado es falso

- Revise los requisitos previos y las limitaciones específicos de la sincronización activa de SnapMirror . Para obtener información, consulte "[Límites de objetos para la sincronización activa de SnapMirror](#)".

Acerca de esta tarea

- SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.
 - Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas

que la cantidad especificada 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 izquierdo, seleccione **Configuración**.
2. En la página de Configuración, seleccione **Políticas**.
3. Seleccione **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.
5. En la página Copia de seguridad y replicación, realice las siguientes tareas:
 - a. Seleccione una configuración de copia de seguridad.

Opción	Descripción
Copia de seguridad consistente del sistema de archivos	Elija esta opción si desea que SnapCenter suspenda la unidad de disco en la que reside el sistema de archivos antes de que comience la operación de respaldo y luego reanude la unidad de disco una vez que finalice la operación de respaldo.
Copia de seguridad consistente ante fallos del sistema de archivos	Elija esta opción si no desea que SnapCenter suspenda 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 únicamente la frecuencia de la copia de seguridad. El programa de protección específico para realizar copias de seguridad se define en el grupo de recursos. Por lo tanto, dos o más grupos de recursos pueden compartir la misma política y frecuencia de respaldo, pero tener diferentes programaciones de respaldo.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

- c. Seleccione una etiqueta de política.

Según la etiqueta de instantánea que seleccione, ONTAP aplica la política de retención de instantánea secundaria que coincide con la etiqueta.



Si ha seleccionado **Actualizar SnapMirror después de crear una copia de instantánea local**, puede especificar opcionalmente la etiqueta de política secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia de instantánea local**, debe especificar la etiqueta de política secundaria.

6. En la sección Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione esta opción para crear copias espejo de conjuntos de copias de seguridad en otro volumen (SnapMirror). Esta opción debe estar habilitada para la sincronización activa de SnapSnapMirror. Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Ver "Ver copias de seguridad y clones relacionados en la página Topología".
Actualizar SnapVault después de crear una copia de Snapshot	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco. Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón Actualizar en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre SnapLock Vault, consulte "Confirmar copias de instantáneas en WORM en un destino de bóveda".
Recuento de reintentos de error	Introduzca el número de intentos de replicación que deben ocurrir antes de que el proceso se detenga.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

- En la página Configuración de retención, especifique la configuración de retención para las copias de seguridad a pedido y para cada frecuencia de programación que haya seleccionado.

Opción	Descripción
Copias de instantáneas totales para conservar	Elija esta opción si desea especificar la cantidad de instantáneas que almacena SnapCenter antes de eliminarlas automáticamente.
Conserve copias instantáneas para	Elija esta opción si desea especificar la cantidad de días que SnapCenter conserva una copia de seguridad 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.



Debes establecer el recuento de retención en 2 o más. El valor mínimo para el recuento 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 .

- En la página Script, ingrese la ruta del prescript o postscript que desea que SnapCenter Server ejecute antes o después de la operación de respaldo, respectivamente, y un límite de tiempo que SnapCenter espera para que se ejecute el script antes de que se agote el tiempo de espera.

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



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

- Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos para sistemas de archivos de Windows

Un grupo de recursos es el contenedor al que puedes agregar múltiples sistemas de archivos que quieras proteger. También debe adjuntar una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar y luego especificar la programación de copia de seguridad.

Acerca de esta tarea

- 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 .
- No se admite agregar 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 agregar nuevos sistemas de archivos a un grupo de recursos existente en el modo de

conmutación por error de la sincronización activa de SnapMirror . Puede agregar recursos al grupo de recursos solo en estado normal o de conmutación por recuperación.

Pasos

- En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
- En la página Recursos, seleccione **Sistemas de archivos** de la lista.



Si ha agregado recientemente un sistema de archivos a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recientemente agregado.

- Haga clic en **Nuevo grupo de recursos**.
- En la página Nombre del asistente, haga lo siguiente:

Para este campo...	Haz esto...
Nombre	Introduzca el nombre del grupo de recursos. El nombre del grupo de recursos no debe exceder los 250 caracteres.
Utilice un formato de nombre personalizado para la copia de instantáneas	Opcional: Ingrese un nombre y formato de instantánea personalizados. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.
Etiqueta	Ingrese una etiqueta descriptiva para ayudar a encontrar un grupo de recursos.

- En la página Recursos, realice las siguientes tareas:
 - Seleccione el host para filtrar la lista de recursos.

Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.
 - En la sección Recursos disponibles, haga clic en los sistemas de archivos que desea respaldar y luego haga clic en la flecha derecha para moverlos a la sección Agregados.

Si selecciona la opción **Seleccionar automáticamente todos los recursos en el mismo volumen de almacenamiento**, se seleccionarán todos los recursos en el mismo volumen. Cuando los mueve a la sección Agregado, todos los recursos de ese volumen se mueven juntos.

Para agregar un solo sistema de archivos, desmarque la opción **Seleccionar automáticamente todos los recursos en el mismo volumen de almacenamiento** y luego seleccione los sistemas de archivos que desea mover a la sección Agregado.

6. En la página Políticas, realice las siguientes tareas:

- a. Seleccione una o más políticas de la lista desplegable.

Puede seleccionar cualquier política existente y hacer clic en **Detalles** para determinar si puede utilizar esa política.

Si ninguna política existente cumple con sus requisitos, puede crear una nueva política haciendo clic en *  * para iniciar el asistente de políticas.

Las políticas seleccionadas se enumeran en la columna Política de la sección Configurar programaciones para políticas seleccionadas.

- b. En la sección Configurar programaciones para políticas seleccionadas, haga clic en *  * en la columna Configurar programaciones de la política para la que desea configurar la programación.
- c. Si la política está asociada a varios tipos de programación (frecuencias), seleccione la frecuencia que desea configurar.
- d. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación especificando la fecha de inicio, la fecha de vencimiento y la frecuencia y, luego, haga clic en **Finalizar**.

Los programas configurados se enumeran en la columna Programaciones aplicadas en la sección Configurar programas para políticas seleccionadas.

No se admiten programaciones de respaldo de terceros cuando se superponen con programaciones de respaldo de SnapCenter . No debe modificar las programaciones del Programador de tareas de Windows ni del Agente SQL Server.

7. En la página de Notificación, proporcione información de notificación, de la siguiente manera:

Para este campo...	Haz esto...
Preferencia de correo electrónico	Seleccione Siempre , En caso de error o En caso de error o advertencia para enviar correos electrónicos a los destinatarios después de crear grupos de recursos de respaldo, adjuntar políticas y configurar programaciones. Ingrese el servidor SMTP, la línea de asunto del correo electrónico predeterminada y las direcciones de correo electrónico Para y De.
De	Dirección de correo electrónico
A	Correo electrónico a la dirección
Sujeto	Línea de asunto de correo electrónico predeterminada

8. Revise el resumen y luego haga clic en **Finalizar**.

Puede realizar una copia de seguridad a pedido o esperar a que se realice la copia de seguridad programada.

Cree grupos de recursos y habilite la protección secundaria para los sistemas de archivos de Windows en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource_group_policy_hostname o resource_group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:
 - a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
 - c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:
 - a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la

verificación en el almacenamiento secundario.

- b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
- c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al 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

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para

respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de administración única.

Pasos

1. Inicie una sesión de conexión de PowerShell Core mediante el cmdlet `Open-SmConnection`.

Este ejemplo abre una sesión de PowerShell:

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

2. Cree una nueva conexión al sistema de almacenamiento mediante el cmdlet `Add-SmStorageConnection`.

Este ejemplo crea una nueva conexión al sistema de almacenamiento:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una nueva credencial mediante el cmdlet `Add-SmCredential`.

Este ejemplo crea una nueva credencial llamada `FinanceAdmin` con credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realice una copia de seguridad de un único recurso a pedido para los sistemas de archivos de Windows

Si un recurso no está en un grupo de recursos, puede realizar una copia de seguridad del recurso a pedido desde la página **Recursos**.

Acerca de esta tarea

Si desea realizar una copia de seguridad de un recurso que tiene una relación `SnapMirror` con un almacenamiento secundario, la función asignada al usuario de almacenamiento debe incluir el privilegio `"snapmirror all"`. Sin embargo, si está utilizando el rol `"vsadmin"`, entonces no se requiere el privilegio `"snapmirror all"`.



Al realizar una copia de seguridad de un sistema de archivos, SnapCenter no realiza una copia de seguridad de los LUN que están montados en un punto de montaje de volumen (VMP) en el sistema de archivos que se está respaldando.



Si está trabajando en un contexto de sistema de archivos de Windows, no haga copias de seguridad de los archivos de base de datos. Al hacerlo se crea una copia de seguridad inconsistente y una posible pérdida de datos durante la restauración. 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).

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el tipo de recurso Sistema de archivos y, a continuación, seleccione el recurso que desea respaldar.
3. Si el asistente para proteger el sistema de archivos no se inicia automáticamente, haga clic en **Proteger** para iniciar el asistente.

Especifique la configuración de protección, como se describe en las tareas de creación de grupos de recursos.

4. Opcional: en la página Recursos del asistente, ingrese un formato de nombre personalizado para la instantánea.

Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Políticas, realice las siguientes tareas:

- a. Seleccione una o más políticas de la lista desplegable.

Puede seleccionar cualquier política existente y luego hacer clic en **Detalles** para determinar si puede usar esa política.

Si ninguna política existente cumple con sus requisitos, puede copiar una política existente y modificarla o puede crear una nueva política haciendo clic en  para iniciar el asistente de políticas. Si ninguna política existente cumple con sus requisitos, puede copiar una política existente y modificarla o puede crear una nueva política haciendo clic en  para iniciar el asistente de políticas.

Las políticas seleccionadas se enumeran en la columna Política de la sección Configurar programaciones para políticas seleccionadas.

- b. En la sección Configurar programaciones para políticas seleccionadas, haga clic en  en la columna Configurar programaciones de la política para la que desea configurar la programación.
- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación especificando la fecha de inicio, la fecha de vencimiento y la frecuencia y, luego, haga clic en **Finalizar**.

Los programas configurados se enumeran en la columna Programaciones aplicadas en la sección Configurar programas para políticas seleccionadas.

"Las operaciones programadas podrían fallar"

6. En la página de Notificación, realice las siguientes tareas:

Para este campo...	Haz esto...
Preferencia de correo electrónico	Seleccione Siempre, o En caso de error, o En caso de error o advertencia, para enviar correos electrónicos a los destinatarios después de crear grupos de recursos de respaldo, adjuntar políticas y configurar programaciones. Ingrese la información del servidor SMTP, la línea de asunto del correo electrónico predeterminada y las direcciones de correo electrónico "Para" y "De".
De	Dirección de correo electrónico
A	Correo electrónico a la dirección
Sujeto	Línea de asunto de correo electrónico predeterminada

7. Revise el resumen y luego haga clic en **Finalizar**.

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

8. Haga clic en **Hacer copia de seguridad ahora**.

9. En la página Copia de seguridad, realice los siguientes pasos:

- Si ha aplicado varias políticas al recurso, en la lista desplegable Política, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

- Haga clic en **Copia de seguridad**.

10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

- Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

Se muestra la solicitud de nombre de usuario y contraseña.

- Cree una política de respaldo mediante el cmdlet Add-SmPolicy.

Este ejemplo crea una nueva política de respaldo con un tipo de respaldo SQL de FullBackup:


```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Este ejemplo crea una nueva política de respaldo con un tipo de respaldo del sistema de archivos de Windows de CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra los recursos del host mediante el cmdlet Get-SmResources.

Este ejemplo descubre los recursos para el complemento de Microsoft SQL en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

Este ejemplo descubre los recursos de los sistemas de archivos de Windows en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

Este ejemplo crea un nuevo grupo de recursos de respaldo de base de datos 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"
```

Este ejemplo crea un nuevo grupo de recursos de respaldo del sistema de archivos de 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. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Vea el estado del trabajo de respaldo mediante el cmdlet Get-SmBackupReport.

Este ejemplo muestra un informe de resumen de trabajos de todos los trabajos que se ejecutaron en la fecha especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de grupos de recursos para sistemas de archivos de Windows

Un grupo de recursos es una colección de recursos en un host o clúster. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos. Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".
- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, la operación de respaldo en algunos de los hosts podría activarse tarde debido a problemas de red. Debe configurar el valor de MaxRetryForUninitializedHosts en web.config mediante el cmdlet de PowerShell Set-SmConfigSettings



Al realizar una copia de seguridad de un sistema de archivos, SnapCenter no realiza una copia de seguridad de los LUN que están montados en un punto de montaje de volumen (VMP) en el sistema de archivos que se está respaldando.



Si está trabajando en un contexto de sistema de archivos de Windows, no haga copias de seguridad de los archivos de base de datos. Al hacerlo se crea una copia de seguridad inconsistente y una posible pérdida de datos durante la restauración. 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o haciendo clic en  y seleccionando la etiqueta. Luego puedes hacer clic  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y haga clic en **Hacer copia de seguridad ahora**.



En el caso del complemento SnapCenter para Oracle Database, si tiene un grupo de recursos federados con dos bases de datos y una de las bases de datos tiene un archivo de datos en un almacenamiento que no es de NetApp, la operación de respaldo se cancela incluso si la otra base de datos está en un almacenamiento de NetApp.

4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si ha asociado varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.
 - En configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

"No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar. Para aumentar el tamaño del montón de Java, localice el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese guión, el `do_start method` El comando inicia el servicio del complemento VMware de SnapCenter. Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

Supervisar las operaciones de copia de seguridad

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar operaciones en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 operaciones de copia de seguridad

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter, los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de copia de seguridad.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	a. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. b. Seleccione la operación y luego haga clic en Cancelar trabajo.
Panel de actividades	a. Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Ver copias de seguridad y clones relacionados en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario. En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Acerca de esta tarea

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.

-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad del espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .

- La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si ha creado 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad mostradas es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad del espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), puede ver los siguientes íconos adicionales:

-  El sitio de réplica está activo.
-  El sitio de réplica está inactivo.
-  No se ha restablecido la relación de espejo secundario o bóveda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página de topología del recurso seleccionado.

4. Revise la tarjeta Resumen para ver un resumen de la cantidad de copias de seguridad y clones

disponibles en el almacenamiento primario y secundario.

La sección Tarjeta de resumen muestra el número total de copias de seguridad y clones. Solo para la base de datos Oracle, la sección Tarjeta de resumen también muestra el número total de copias de seguridad 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración 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 respaldo de SnapCenter consultando a ONTAP los sitios principales y de réplica. Una programación semanal también realiza esta actividad para 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 Async Mirror o Async MirrorVault con el nuevo destino principal se deben configurar manualmente después de la conmutación por error. Desde ONTAP 9.15.1 en adelante, Async Mirror o Async MirrorVault se configura automáticamente en el nuevo destino principal.
- Después de la conmutación por error, se debe crear una copia de seguridad para que SnapCenter esté al tanto de la conmutación por error. Puede hacer clic en **Actualizar** sólo después de haber creado una copia de seguridad.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación, cambio de nombre y eliminación.

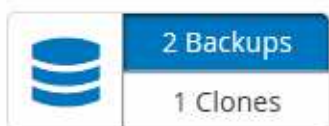


No se puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el sistema de almacenamiento secundario.

7. Si desea eliminar un clon, seleccione el clon de la tabla y haga clic en para eliminar el clon.

Ejemplo que muestra copias de seguridad y clones en el almacenamiento principal

Manage Copies



Limpiar el recuento de copias de seguridad secundarias mediante cmdlets de PowerShell

Puede utilizar el cmdlet `Remove-SmBackup` para limpiar el recuento de copias de seguridad de las copias de seguridad secundarias que no tienen instantánea. Es posible que desee utilizar este cmdlet cuando la cantidad total de instantáneas que se muestran en la topología Administrar copias no coincidan con la configuración de retención de instantáneas de almacenamiento secundario.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Limpie el recuento de copias de seguridad secundarias utilizando el parámetro `-CleanupSecondaryBackups`.

Este ejemplo limpia el recuento de copias de seguridad para copias de seguridad secundarias sin instantáneas:

```
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 de Windows

Restaurar copias de seguridad del sistema de archivos de Windows

Puede utilizar SnapCenter para restaurar copias de seguridad del sistema de archivos. La restauración del sistema de archivos es un proceso de varias fases que copia todos los datos de una copia de seguridad específica a la ubicación original del sistema de archivos.

Antes de empezar

- Debes haber realizado una copia de seguridad del sistema de archivos.
- Si una operación programada, como una operación de respaldo, está actualmente en progreso para un sistema de archivos, entonces esa operación debe cancelarse antes de poder iniciar una operación de restauración.
- Solo se puede restaurar una copia de seguridad del sistema de archivos en la ubicación original, no en una ruta alternativa.

No se puede restaurar un solo archivo desde una copia de seguridad porque el sistema de archivos restaurado sobrescribe cualquier dato en la ubicación original del sistema de archivos. Para restaurar un solo archivo desde una copia de seguridad del sistema de archivos, debe clonar la copia de seguridad y acceder al archivo en el clon.

- No es posible restaurar un sistema o un volumen de arranque.
- SnapCenter puede restaurar sistemas de archivos en un clúster de Windows sin desconectar el grupo de clústeres.

Acerca de esta tarea

- `SCRIPTS_PATH` se define utilizando la clave `PredefinedWindowsScriptsDirectory` ubicada en el archivo `SMCoreServiceHost.exe.Config` del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio `SMcore`. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: `API /4.7/configsettings`

Puede utilizar la API `GET` para mostrar el valor de la clave. La API `SET` no es compatible.

- Para la operación de restauración de sincronización activa de SnapMirror , debe seleccionar la copia de seguridad de la ubicación principal.
- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Para filtrar la lista de recursos, seleccione las opciones Sistema de archivos y Grupo de recursos.
3. Seleccione un grupo de recursos de la lista y haga clic en **Restaurar**.
4. En la página Copias de seguridad, seleccione si desea restaurar desde sistemas de almacenamiento primarios o secundarios y luego seleccione una copia de seguridad para restaurar.
5. Seleccione sus opciones en el asistente de restauración.
6. Puede ingresar la ruta y los argumentos del prescript o postscript que desea que SnapCenter ejecute antes o después de la operación de restauración, respectivamente.

Por ejemplo, puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

7. En la página de Notificación, seleccione una de las siguientes opciones:

Para este campo...	Haz esto...
Registrar eventos del servidor SnapCenter en el syslog del sistema de almacenamiento	Seleccione esta opción para registrar eventos de SnapCenter Server en el syslog del sistema de almacenamiento.
Enviar notificación de AutoSupport para operaciones fallidas al sistema de almacenamiento	Seleccione esta opción para enviar información sobre cualquier operación fallida a NetApp mediante AutoSupport.
Preferencia de correo electrónico	Seleccione Siempre , En caso de error o En caso de error o advertencia para enviar mensajes de correo electrónico a los destinatarios después de restaurar las copias de seguridad. Ingrese el servidor SMTP, la línea de asunto del correo electrónico predeterminada y las direcciones de correo electrónico de destino y de origen.

8. Revise el resumen y luego haga clic en **Finalizar**.
9. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.



Si el sistema de archivos restaurado contiene una base de datos, también deberá restaurar la base de datos. Si no restaura la base de datos, es posible que ésta se encuentre en un estado no válido. Para obtener información sobre cómo restaurar bases de datos, consulte la Guía de protección de datos correspondiente a esa base de datos.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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			

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet `Restore-SmBackup`.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar recursos mediante cmdlets de PowerShell

Restaurar una copia de seguridad de un recurso incluye iniciar una sesión de conexión con el servidor SnapCenter, enumerar las copias de seguridad y recuperar información de las copias de seguridad, y restaurar una copia de seguridad.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar las operaciones de restauración

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso

-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Cancelar operaciones de restauración

Puede cancelar trabajos de restauración que estén en cola.

Debe iniciar 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.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones de restauración que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de restauración en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 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 Actividad 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 de Windows

Clonar desde una copia de seguridad del sistema de archivos de Windows

Puede utilizar SnapCenter para clonar una copia de seguridad del sistema de archivos de Windows. Si desea una copia de un solo archivo que se eliminó o modificó por error, puede clonar una copia de seguridad y acceder a ese archivo en el clon.

Antes de empezar

- Debes estar preparado para la protección de datos completando tareas como agregar hosts, identificar recursos y crear conexiones de máquinas virtuales de almacenamiento (SVM).
- Debes tener una copia de seguridad del sistema de archivos.
- Debe asegurarse de que los agregados que alojan los volúmenes estén en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- No se puede clonar un grupo de recursos. Sólo puedes clonar copias de seguridad de sistemas de archivos individuales.
- Si una copia de seguridad reside en una máquina virtual con un disco VMDK, SnapCenter no puede clonar la copia de seguridad en un servidor físico.
- Si clona un clúster de Windows (por ejemplo, un LUN compartido o un LUN de volumen compartido de clúster (CSV)), el clon se almacena como un LUN dedicado en el host que especifique.
- Para una operación de clonación, el directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- No se puede crear un clon en un nodo que no sea el nodo de origen del agregado.
- No es posible programar operaciones de clonación recurrentes (ciclo de vida de la clonación) para sistemas de archivos de Windows; solo se puede clonar una copia de seguridad a pedido.
- Si mueve un LUN que contiene un clon a un nuevo volumen, SnapCenter ya no podrá soportar el clon. Por ejemplo, no puedes usar SnapCenter para eliminar ese clon.
- No es posible clonar entre entornos. Por ejemplo, clonar de un disco físico a un disco virtual o viceversa.

Acerca de esta tarea

- SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo

SMCoreServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.

- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Sistemas de archivos** de 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 la copia de seguridad que desea clonar y luego haga clic en el ícono de clonar.
5. En la página Opciones, haga lo siguiente:

Para este campo...	Haz esto...
Servidor clonado	Seleccione el host en el que se debe crear el clon.
“Asignar automáticamente punto de montaje” o “Asignar automáticamente punto de montaje de volumen en la ruta”	Elija si desea asignar automáticamente un punto de montaje o un punto de montaje de volumen bajo una ruta. Asignar automáticamente el punto de montaje del volumen en la ruta: el punto de montaje en una ruta le permite proporcionar un directorio específico en el que se crearán los puntos de montaje. Antes de elegir esta opción, debe verificar que el directorio esté vacío. Si hay una copia de seguridad en el directorio, la copia de seguridad estará en un estado no válido después de la operación de montaje.
Ubicación del archivo	Elija una ubicación de archivo si está clonando una copia de seguridad secundaria.

6. En la página Script, especifique los prescripts o posscripts que desea ejecutar.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

7. Revise el resumen y luego haga clic en **Finalizar**.
8. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Enumere las copias de seguridad que se pueden clonar mediante el cmdlet Get-SmBackup o Get-SmResourceGroup.

Este ejemplo muestra información sobre todas las copias de seguridad 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	

Este ejemplo muestra información sobre un grupo de recursos específico, sus recursos y 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}
HostResourceMapping : {}
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 clonación desde una copia de seguridad existente utilizando el cmdlet New-SmClone.

Este ejemplo crea un clon a partir de una copia de seguridad especificada 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\squlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

Este ejemplo crea un clon de una instancia específica de Microsoft SQL Server:

```
PS C:\> New-SmClone
-B BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-R Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-A AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-S Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Vea el estado del trabajo de clonación mediante el cmdlet Get-SmCloneReport.

Este ejemplo muestra un informe clonado para el ID de trabajo especificado:

```
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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar las operaciones de clonación

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Cancelar operaciones de clonación

Puede cancelar operaciones de clonación que estén en cola.

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones de clonación.

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 clonación en ejecución.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de clonación en cola.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de clonación en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 2. Seleccione la operación y haga clic en Cancelar trabajo.
Panel de actividades	1. Después de iniciar la operación de clonación, haga clic en  en el panel Actividad para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone, consulte ["Dividir un volumen FlexClone de su volumen principal"](#).
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en *.
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Proteger las bases de datos de Microsoft Exchange Server

Conceptos del complemento SnapCenter para Microsoft Exchange Server

Descripción general del complemento de SnapCenter para Microsoft Exchange Server

El complemento SnapCenter para Microsoft Exchange Server es un componente del lado del host del software SnapCenter de NetApp que permite la gestión de protección de datos consciente de la aplicación de las bases de datos de Exchange. El complemento para Exchange automatiza la copia de seguridad y la restauración de bases de datos de Exchange en su entorno de SnapCenter .

Cuando se instala el complemento para Exchange, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen y con la tecnología NetApp SnapVault para realizar replicación de copias de seguridad de disco a disco para fines de archivo o cumplimiento de estándares.

Si desea restaurar y recuperar correos o buzones en lugar de la base de datos de Exchange completa, puede utilizar el software de recuperación de buzón único (SMBR). NetApp® Single Mailbox Recovery llegó al final de su disponibilidad (EOA) el 12 de mayo de 2023. NetApp seguirá brindando soporte a los clientes que hayan adquirido capacidad de buzón, mantenimiento y soporte a través de los números de pieza de marketing introducidos el 24 de junio de 2020, mientras dure el derecho de soporte.

NetApp Single Mailbox Recovery es un producto asociado proporcionado por Ontrack. Ontrack PowerControls ofrece capacidades similares a las de NetApp Single Mailbox Recovery. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls de Ontrack (a través de licensingteam@ontrack.com) para la recuperación granular del buzón.

El complemento para Exchange admite la sincronización activa de SnapMirror (lanzada inicialmente como SnapMirror Business Continuity [SM-BC]) que permite que los servicios comerciales sigan funcionando incluso en caso de una falla total del sitio y permite que las aplicaciones conmuten por error de manera transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una conmutación por error con la sincronización activa de SnapMirror .

Admite el modo asimétrico, de conmutación por error o no dúplex de SnapMirror Active Sync. Esto se refiere a la solución donde la ruta optimizada es solo desde el nodo propietario del LUN del lado primario. Cualquier E/S que llega a las rutas del clúster secundario se atiende mediante un proxy al clúster principal. La replicación sincrónica es unidireccional, en dirección de primaria a secundaria.

- Automatiza las operaciones de copia de seguridad y restauración basadas en aplicaciones para bases de datos de Microsoft Exchange Server y grupos de disponibilidad de bases de datos (DAG) en su entorno de SnapCenter
- Admite servidores Exchange virtualizados en LUN RDM cuando implementa el SnapCenter Plug-in for VMware vSphere y registra el complemento con SnapCenter.

Qué puede hacer con el complemento SnapCenter para Microsoft Exchange Server

Puede utilizar el complemento para Exchange para realizar copias de seguridad y restaurar bases de datos de Exchange Server.

- Ver y administrar un inventario activo de grupos de disponibilidad de bases de datos (DAG) de Exchange, bases de datos y conjuntos de réplicas
- Definir políticas que proporcionen las configuraciones de protección para la automatización de copias de seguridad
- Asignar políticas a grupos de recursos
- Proteger DAG y bases de datos individuales
- Realizar copias de seguridad de las bases de datos de buzones de correo de Exchange principales y secundarios
- Restaurar bases de datos desde copias de seguridad primarias y secundarias

Tipos de almacenamiento compatibles con el complemento SnapCenter para Microsoft Windows y Microsoft Exchange Server

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas físicas como virtuales. Debe verificar si hay soporte disponible para su tipo de almacenamiento antes de instalar el paquete para su host.

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 <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT> [Herramienta de matriz de interoperabilidad de NetApp ^].

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Servidor físico	LUN conectados a FC	Interfaz gráfica de usuario (GUI) de SnapCenter o cmdlets de PowerShell	
Servidor físico	LUN conectados a iSCSI	GUI de SnapCenter o cmdlets de PowerShell	
Máquina virtual de VMware	LUN RDM conectados mediante un HBA 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 iSCSI	GUI de SnapCenter o cmdlets de PowerShell	 Los VMDK no son compatibles.

Máquina	Tipo de almacenamiento	Provisión utilizando	Notas de soporte
Máquina virtual Hyper-V	LUN de FC virtuales (vFC) conectados mediante un conmutador de canal de fibra virtual	GUI de SnapCenter o cmdlets de PowerShell	Debe utilizar Hyper-V Manager para aprovisionar LUN de FC virtual (vFC) conectados mediante un conmutador de canal de fibra virtual.  No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .
Máquina virtual Hyper-V	LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI	GUI de SnapCenter o cmdlets de PowerShell	 No se admiten los discos de paso de Hyper-V ni la copia de seguridad de bases de datos en VHD(x) aprovisionados en el almacenamiento de NetApp .

Privilegios mínimos de ONTAP necesarios para el complemento de Exchange

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo

- almuerzo
- lun crear
- lun crear
- lun crear
- eliminar lun
- agregar igroup lun
- crear igroup lun
- eliminar igroup lun
- Cambiar nombre de igroup lun
- Cambiar nombre de igroup lun
- Programa de igroup de Lun
- Asignación de LUN a nodos de informes adicionales
- creación de mapeo LUN
- eliminar mapeo lun
- Mapeo de LUN: eliminar nodos de informes
- espectáculo de mapeo de lun
- modificar lun
- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- lun reserva persistente clara
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen

- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- tiempo de caducidad de modificación de instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFS de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIFS de vserver
- Mostrar copia de sombra de CIFS de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi

- Mostrar conexión iscsi de vserver
- espectáculo vserver
- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red
 - Mostrar interfaz de red
 - vserver

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Definir una estrategia de respaldo para los recursos de Exchange Server

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a garantizar que tenga los respaldos que necesita para restaurar exitosamente sus bases de datos. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. El RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. El SLA, RTO y RPO contribuyen a la estrategia de respaldo.

Tipos de copias de seguridad compatibles con la base de datos de Exchange

Para realizar copias de seguridad de buzones de Exchange mediante SnapCenter es necesario elegir el tipo de recurso, como bases de datos y grupos de disponibilidad de bases de datos (DAG). Se aprovecha la tecnología de instantáneas para crear copias en línea, de solo lectura, de los volúmenes en los que residen los recursos.

Tipo de copia de seguridad	Descripción
Copia de seguridad completa y de registros	Realiza una copia de seguridad de las bases de datos y de todos los registros de transacciones, incluidos los registros truncados. Una vez completada una copia de seguridad completa, Exchange Server trunca los registros de transacciones que ya están confirmados en la base de datos. Por lo general, deberías elegir esta opción. Sin embargo, si el tiempo de respaldo es corto, puede elegir no ejecutar una copia de seguridad del registro de transacciones con una copia de seguridad completa.
Copia de seguridad completa	Realiza copias de seguridad de bases de datos y registros de transacciones. No se realiza una copia de seguridad de los registros de transacciones truncados.
Copia de seguridad del registro	Realiza una copia de seguridad de todos los registros de transacciones. Los registros truncados que ya están confirmados en la base de datos no se respaldan. Si programa copias de seguridad frecuentes del registro de transacciones entre copias de seguridad completas de la base de datos, puede elegir puntos de recuperación granulares.

Programaciones de copias de seguridad para complementos de bases de datos

La frecuencia de copia de seguridad (tipo de programación) se especifica en las políticas; una programación de copia de seguridad se especifica en la configuración del grupo de recursos. El factor más crítico a la hora de determinar la frecuencia o el cronograma de una copia de seguridad es la tasa de cambio del recurso y la importancia de los datos. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su Acuerdo de Nivel de Servicio (SLA) y su Objetivo de Punto de Recuperación (RPO).

Un SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. Un RPO define la estrategia para la antigüedad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden

después de una falla. El SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso para un recurso muy utilizado, no es necesario ejecutar una copia de seguridad completa más de una o dos veces al día. Por ejemplo, las copias de seguridad periódicas del registro de transacciones podrían ser suficientes para garantizar que tenga las copias de seguridad que necesita. Cuanto más a menudo realice copias de seguridad de sus bases de datos, menos registros de transacciones tendrá que utilizar SnapCenter en el momento de la restauración, lo que puede generar operaciones de restauración más rápidas.

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de respaldo

La frecuencia de las copias de seguridad (con qué frecuencia se deben realizar las copias de seguridad), denominada *tipo de programación* para algunos complementos, es parte de una configuración de políticas. Puede seleccionar la frecuencia de respaldo para la política: horaria, diaria, semanal o mensual. Si no selecciona ninguna de estas frecuencias, la política creada será solo a pedido. Puede acceder a las políticas haciendo clic en **Configuración > Políticas**.

- Programaciones de copias de seguridad

Las programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad) son parte de la configuración de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para realizar copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos > Grupos de recursos**.

Número de trabajos de respaldo necesarios para las bases de datos

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño del recurso, la cantidad de volúmenes utilizados, la tasa de cambio del recurso y su Acuerdo de Nivel de Servicio (SLA).

Convenciones de nombres de copias de seguridad

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

```
resourcegroupname_hostname_timestamp
```

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o

grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, `customtext_resourcegroup_policy_hostname` o `resourcegroup_hostname`. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Opciones de retención de copias de seguridad

Puede elegir la cantidad de días durante los cuales desea conservar copias de seguridad o especificar la cantidad de copias de seguridad que desea conservar, hasta un máximo de 255 copias en ONTAP . Por ejemplo, su organización podría exigirle que conserve 10 días de copias de seguridad o 130 copias de seguridad.

Al crear una política, puede especificar las opciones de retención para el tipo de copia de seguridad y el tipo de programación.

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

SnapCenter elimina las copias de seguridad retenidas que tienen etiquetas de retención que coinciden con el tipo de programación. Si se modificó el tipo de programación del recurso o del grupo de recursos, es posible que las copias de seguridad con la etiqueta del tipo de programación anterior aún permanezcan en el sistema.



Para la retención a largo plazo de copias de seguridad, debe utilizar la copia de seguridad SnapVault .

¿Durante cuánto tiempo se deben conservar las copias de seguridad del registro de transacciones en el volumen de almacenamiento de origen para Exchange Server?

El complemento SnapCenter para Microsoft Exchange Server necesita copias de seguridad del registro de transacciones para realizar operaciones de restauración actualizadas, que restauran su base de datos a un tiempo entre dos copias de seguridad completas.

Por ejemplo, si Plug-in for Exchange realizó una copia de seguridad completa del registro de transacciones a las 8:00 a. m. y otra copia de seguridad completa del registro de transacciones a las 5:00 p. m., podría usar la última copia de seguridad del registro de transacciones para restaurar la base de datos a cualquier momento entre las 8:00 a. m. y las 5:00 p. m. Si los registros de transacciones no están disponibles, Plug-in for Exchange solo puede realizar operaciones de restauración en un punto en el tiempo, que restauran una base de datos al momento en que Plug-in for Exchange completó una copia de seguridad completa.

Por lo general, se necesitan operaciones de restauración actualizadas solo por uno o dos días. 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 Exchange Server le permitirá restaurar su base de datos con éxito.

Fuentes para una operación de restauración en Exchange Server

Puede restaurar una base de datos de Exchange Server desde una copia de seguridad en el almacenamiento principal.

Puede restaurar bases de datos únicamente desde el almacenamiento principal.

Tipos de operaciones de restauración compatibles con Exchange Server

Puede utilizar SnapCenter para realizar distintos tipos de operaciones de restauración en recursos de Exchange.

- Restaurar actualizado al minuto
- Restaurar a un punto anterior en el tiempo

Restaurar al minuto

En una operación de restauración actualizada, las bases de datos se recuperan hasta el punto de falla. SnapCenter logra esto realizando la siguiente secuencia:

1. Restaura las bases de datos desde la copia de seguridad completa de la base de datos que seleccione.
2. Aplica todos los registros de transacciones que fueron respaldados, así como también cualquier registro nuevo que haya sido creado desde la copia de seguridad más reciente.

Los registros de transacciones se mueven hacia adelante y se aplican a cualquier base de datos seleccionada.

Exchange crea una nueva cadena de registro después de que se completa una restauración.

Mejor práctica: Se recomienda realizar una nueva copia de seguridad completa y del registro después de que se complete una restauración.

Una operación de restauración actualizada requiere un conjunto contiguo de registros de transacciones.

Después de realizar una restauración actualizada, la copia de seguridad que utilizó para la restauración solo estará disponible para operaciones de restauración en un momento determinado.

Si no necesita conservar la capacidad de restauración actualizada para todas las copias de seguridad, puede configurar la retención de la copia de seguridad del registro de transacciones de su sistema a través de las políticas de copia de seguridad.

Restaurar a un punto anterior en el tiempo

En una operación de restauración a un punto en el tiempo, las bases de datos se restauran únicamente a un momento específico del pasado. Una operación de restauración a un punto en el tiempo ocurre en las siguientes situaciones de restauración:

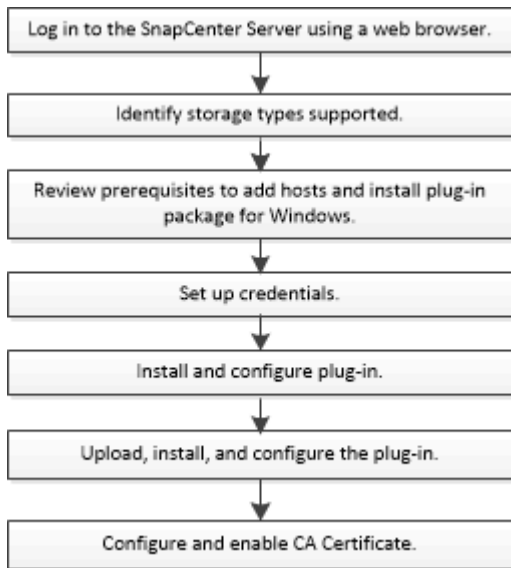
- La base de datos se restaura a un momento determinado en un registro de transacciones respaldado.
- Se restaura la base de datos y solo se le aplica un subconjunto de los registros de transacciones respaldados.

Instalar el complemento de SnapCenter para Microsoft Exchange Server

Flujo de trabajo de instalación del complemento de SnapCenter para Microsoft Exchange Server

Debe instalar y configurar el complemento SnapCenter para Microsoft Exchange Server

si desea proteger las bases de datos de Exchange.



Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para Microsoft Exchange Server

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos.

- Si está utilizando iSCSI, el servicio iSCSI debe estar ejecutándose.
- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Debe utilizar Microsoft Exchange Server 2013, 2016 o 2019 para configuraciones independientes y de grupo de disponibilidad de base de datos.
- Al instalar un complemento 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 administra nodos de clúster en SnapCenter, debe tener un usuario con privilegios administrativos para todos los nodos del clúster.
- Debe tener un usuario con permisos administrativos en el servidor Exchange.
- Si SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya están instalados, debe anular el registro del proveedor de hardware VSS utilizado por SnapDrive para Windows antes de instalar el complemento para Exchange en el mismo Exchange Server para garantizar una protección de datos exitosa mediante SnapCenter.
- Si SnapManager para Microsoft Exchange Server y el complemento para Exchange están instalados en el mismo servidor, debe suspender o eliminar del programador de Windows todas las programaciones creadas por SnapManager para Microsoft Exchange Server.
- El host debe poder resolverse al nombre de dominio completo (FQDN) desde el servidor. Si se modifica el archivo de hosts para que se pueda resolver y si tanto el nombre corto como el FQDN se especifican en el archivo de hosts, cree una entrada en el archivo de hosts de SnapCenter con el siguiente formato:
`<dirección_ip> <fqdn_de_host> <nombre_de_host>.`
- Asegúrese de que los siguientes puertos no estén bloqueados en el firewall; de lo contrario, la operación de agregar host fallará. Para resolver este problema, debe configurar el rango de puertos dinámicos. Para obtener más información, consulte "[Documentación de Microsoft](#)".

- Rango de puertos 50000 - 51000 para Windows 2016 y Exchange 2016
- Rango de puertos 6000-6500 para Windows 2012 R2 y Exchange 2013
- Rango de puertos 49152-65536 para Windows 2019



Para identificar el rango de puertos, ejecute los siguientes comandos:

- netsh int ipv4 muestra puerto dinámico tcp
- netsh int ipv4 muestra puerto dinámico udp
- netsh int ipv6 muestra puerto dinámico tcp
- netsh int ipv6 mostrar puerto dinámico udp

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.

Artículo	Requisitos
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Se requieren privilegios de Exchange Server

Para permitir que SnapCenter agregue Exchange Server o DAG, e instalar el complemento de SnapCenter para Microsoft Exchange Server en un host o DAG, debe configurar SnapCenter con credenciales para un usuario con un conjunto mínimo de privilegios y permisos.

Debe tener un usuario de dominio con privilegios de administrador local y con permisos de inicio de sesión local en el host de Exchange remoto, así como permisos administrativos en todos los nodos del DAG. El usuario del dominio requiere los siguientes permisos mínimos:

- Agregar copia de base de datos de buzón
- Desmontar base de datos
- Obtener la configuración del servidor de anuncios
- Obtener grupo de disponibilidad de base de datos
- Obtener servidor de intercambio
- Obtener base de datos del buzón
- Obtener estado de copia de la base de datos del buzón
- Obtener servidor de buzón
- Obtener estadísticas del buzón
- Obtener base de datos de carpeta pública
- Mover base de datos de buzones activos
- Mover-RutaDeBaseDeDatos -ConfiguraciónSolo:\$true
- Base de datos de montaje

- Nueva base de datos de buzones
- Nueva base de datos de carpetas públicas
- Eliminar base de datos de buzones
- Eliminar copia de la base de datos del buzón
- Eliminar base de datos de carpetas públicas
- Copia de la base de datos del buzón de currículum
- Establecer la configuración del servidor de anuncios
- Establecer-MailboxDatabase -allowfilerestore:\$true
- Copiar base de datos del buzón de correo
- Establecer-Base de datos de carpeta pública
- Suspende-Copia de base de datos de buzones
- Actualizar-Copia de base de datos del buzón

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.

Artículo	Requisitos
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Configurar credenciales para el complemento SnapCenter para Windows

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar el paquete de complemento y credenciales adicionales para realizar operaciones de protección de datos en las bases de datos.

Acerca de esta tarea

Debe configurar credenciales para instalar complementos en hosts de Windows. Si bien puede crear credenciales para Windows después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

Configure las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.

Si configura 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 de respaldo al nombre de usuario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.

Se muestra la ventana Credencial.

4. En la página Credencial, haga lo siguiente:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para la credencial.
Nombre de usuario	Introduzca el nombre de usuario utilizado para la autenticación. - Administrador del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: UserName
Password	Introduzca la contraseña utilizada para la autenticación.
Autenticación	Seleccione Windows como 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 administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Añade objetos de computadora 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,...>  
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de  
servicio.
```

4. Configure el gMSA en sus hosts:
 - a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
 - b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
 - c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Agregar hosts e instalar el complemento para Exchange

Puede utilizar la página Agregar host de SnapCenter para agregar hosts de Windows. El complemento para Exchange se instala automáticamente en el host especificado. Este es el método recomendado para instalar complementos. Puede agregar un host e instalar un complemento 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 complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
 - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el administrador de SnapCenter .
- Al instalar un complemento 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 ejecutándose.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos. Para obtener más información, consulte ["Configurar una cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para Microsoft Exchange Server"](#) .

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .
- Puede agregar un host e instalar paquetes de complementos para un host individual o para un clúster.
- Si un nodo de intercambio es parte de un DAG, no puede agregar solo un nodo al servidor SnapCenter .
- Si está instalando complementos en un clúster (DAG de Exchange), se instalan en todos los nodos del clúster incluso si algunos de ellos no tienen bases de datos en LUN de NetApp .

A partir de SnapCenter 4.6, SCE admite la función multitenencia y puede agregar un host mediante los siguientes métodos:

Agregar operación de host	4.5 y anteriores	4.6 y posteriores
Agregar DAG sin IP en dominios cruzados o diferentes	No compatible	Apoyado

Agregar operación de host	4.5 y anteriores	4.6 y posteriores
Agregue varios DAG de IP con nombres únicos, que residan en el mismo dominio o en varios dominios	Apoyado	Apoyado
Agregue varios DAG con IP o sin IP que tengan los mismos nombres de host y/o nombre de base de datos en dominios cruzados	No compatible	Apoyado
Agregue varios DAG con IP/sin IP con el mismo nombre y dominio cruzado	No compatible	Apoyado
Agregue varios hosts independientes con el mismo nombre y dominio cruzado	No compatible	Apoyado

El complemento para Exchange depende del paquete de complementos de SnapCenter para Windows y las versiones deben ser las mismas. Durante la instalación del complemento para Exchange, el paquete de complementos de SnapCenter para Windows se selecciona 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 y desea instalar el complemento para Exchange en el mismo servidor Exchange, debe anular el registro del proveedor de hardware VSS utilizado por SnapDrive para Windows porque es incompatible con el proveedor de hardware VSS instalado con el complemento para Exchange y el paquete de complementos 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 izquierdo, haga clic en **Hosts**.
2. Verifique que **Hosts administrados** esté seleccionado en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, haga lo siguiente:

Para este campo...	Haz esto...
Tipo de host	Seleccione Windows como tipo de host. SnapCenter Server agrega el host y luego instala en el host el complemento para Windows y el complemento para Exchange si aún no están instalados. El complemento para Windows y el complemento para Exchange deben ser de la misma versión. Si previamente se instaló una versión diferente del complemento para Windows, SnapCenter actualiza la versión como parte de la instalación.

Para este campo...	Haz esto...
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el nombre de dominio completo (FQDN). Una dirección IP solo es compatible con hosts de dominios no confiables si se resuelve en el FQDN. Si está agregando un host mediante SnapCenter y es parte de un subdominio, debe proporcionar el FQDN. Puede ingresar direcciones IP o el FQDN de uno de los siguientes: • Host independiente • Intercambio DAG Para un DAG de Exchange, puedes: ◦ Agregue un DAG proporcionando el nombre del DAG, la dirección IP del DAG, el nombre del nodo o la dirección IP del nodo. ◦ Agregue el clúster DAG sin IP proporcionando la dirección IP o el FQDN de uno de los nodos del clúster DAG. ◦ Agregue un DAG sin IP que resida en el mismo dominio o en uno diferente. También puedes agregar varios DAG con IP/sin IP con el mismo nombre pero con diferentes dominios.  Para un host independiente o un DAG de Exchange (entre dominios o del mismo dominio), se recomienda proporcionar el FQDN o la dirección IP del host o DAG.

Para este campo...	Haz esto...
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree las nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre cómo crear una credencial. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección Seleccionar complementos para instalar, seleccione los complementos que desea instalar.

Cuando selecciona Complemento para Exchange, el Complemento de SnapCenter para Microsoft SQL Server se deselecciona automáticamente. Microsoft recomienda que SQL Server y Exchange Server no se instalen en el mismo sistema debido a la cantidad de memoria utilizada y otros recursos que requiere Exchange.

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.
Ruta de instalación	La ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente puedes personalizar la ruta.
Agregar todos los hosts en el DAG	Seleccione esta casilla de verificación cuando agregue un DAG.

Para este campo...	Haz esto...
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento. Proporcione el nombre de gMSA en el siguiente formato: <i>domainName\accountName\$</i>.  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla "Omitir comprobaciones previas", se validará el host para determinar si cumple los requisitos para instalar el complemento. Si no se cumplen los requisitos mínimos, se mostrarán 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Supervisar el progreso de la instalación.

Configurar un puerto personalizado para la comunicación NET TCP

De forma predeterminada, a partir de la versión 6.0 de SnapCenter, el complemento de SnapCenter para Windows utiliza el puerto 909 para la comunicación NET TCP. Si el puerto 909 está en uso, puede configurar otro puerto para la comunicación NET TCP.

Pasos

- 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" />`
- 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" />`
- 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
```

Verifique que el servicio no se muestre en la lista de servicios en *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"
```

Verifique si el servicio ahora se muestra en la lista de servicios en *services.msc*.

5. Reinicie el servicio *Plug-in para Windows*.

Instalar el complemento para Exchange desde el host del servidor SnapCenter mediante cmdlets de PowerShell

Debe instalar el complemento para Exchange desde la GUI de SnapCenter . Si no desea utilizar la GUI, puede usar cmdlets de PowerShell en el host del servidor SnapCenter o en un host remoto.

Antes de empezar

- Es necesario haber instalado y configurado SnapCenter Server.
- Debe ser un administrador local en el host o un usuario con privilegios administrativos.
- Debe ser un usuario asignado a un rol que tenga permisos de complemento, instalación y desinstalación, como el administrador de SnapCenter .
- Debe haber revisado los requisitos de instalación y los tipos de configuraciones compatibles antes de instalar el complemento para Exchange.
- El host en el que desea instalar el complemento para Exchange debe ser un host Windows.

Pasos

1. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet *Open-SmConnection* y luego ingrese sus credenciales.
2. Agregue el host en el que desea instalar el complemento para Exchange mediante el cmdlet *Add-SmHost* con los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

El host puede ser un host independiente o un DAG. Si especifica un DAG, se requiere el parámetro *-IsDAG*.

3. Instale el complemento para Exchange mediante el cmdlet *Install-SmHostPackage* con los parámetros necesarios.

Este comando instala el complemento para Exchange en el host especificado y luego registra el complemento con SnapCenter.

Instale el complemento de SnapCenter para Exchange de forma silenciosa desde la línea de comandos

Debe instalar el complemento para Exchange desde la interfaz de usuario de SnapCenter . Sin embargo, si por algún motivo no puede, puede ejecutar el programa de instalación del complemento para Exchange sin supervisión en modo silencioso desde la línea de comandos de Windows.

Antes de empezar

- Debes haber realizado una copia de seguridad de los recursos de Microsoft Exchange Server.
- Debe tener instalados los paquetes de complementos de SnapCenter .
- Debe eliminar la versión anterior del complemento SnapCenter para Microsoft SQL Server antes de instalarlo.

Para obtener más información, consulte ["Cómo instalar un complemento de SnapCenter de forma manual y directa desde el host del complemento"](#) .

Pasos

1. Valide si la carpeta *C:\temp* existe en el host del complemento y si el usuario que inició sesión tiene acceso completo a ella.
2. Descargue el complemento de SnapCenter para Microsoft Windows desde *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Se puede acceder a esta ruta desde el host donde está instalado el servidor SnapCenter .

3. Copie el archivo de instalación en el host en el que desea instalar el complemento.
4. Desde un símbolo del sistema de Windows en el host local, navegue hasta el directorio donde guardó los archivos de instalación del complemento.
5. Introduzca el siguiente comando para instalar el complemento.

```
snapcenter_windows_host_plugin.exe"/silent /debuglog"<Ruta_del_registro_de_depuración>"  
/log"<Ruta_del_registro>" BI_SNAPCENTER_PORT=<Num>  
SUITE_INSTALLDIR="<Ruta_del_directorio_de_instalación>"  
BI_SERVICEACCOUNT=<dominio\administrador> BI_SERVICEPWD=<contraseña>  
ISFeatureInstall=HPPW,SCW,SCE
```

Por ejemplo:

```
C:\ProgramData\NetApp\SnapCenter\Repository de  
paquetes\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log"  
/log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Archivos de programa\NetApp\  
SnapCenter" BI_SERVICEACCOUNT=dominio\administrador BI_SERVICEPWD=contraseña  
ISFeatureInstall=HPPW,SCW,SCE
```



Todos los parámetros pasados durante la instalación del complemento para Exchange distinguen entre mayúsculas y minúsculas.

Introduzca los siguientes valores para las variables:

Variable	Valor
<code>/debuglog"<Ruta_del_registro_de_depuración></code>	Especifique el nombre y la ubicación del archivo de registro del instalador de la suite, como en el siguiente ejemplo: <code>Setup.exe</code> <code>/debuglog"C:\RutaAlRegistro\setupexe.log</code>
PUERTO BI_SNAPCENTER	Especifique el puerto en el que SnapCenter se comunica con SMCore.
SUITE_INSTALLDIR	Especifique el directorio de instalación del paquete del complemento de host.
BI_CUENTA DE SERVICIO	Especifique el complemento SnapCenter para la cuenta de servicio web de Microsoft Windows.
BI_SERVICEPWD	Especifique la contraseña para la cuenta de servicio web del complemento SnapCenter para Microsoft Windows.
Instalación de ISFeature	Especifique la solución que SnapCenter implementará en el host remoto.

- 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`.
- Supervise el directorio `%temp%` para verificar si los instaladores `msiexe.exe` están instalando el software sin errores.



La instalación del complemento para Exchange registra el complemento en el host y no en el servidor SnapCenter . Puede registrar el complemento en el servidor SnapCenter agregando el host mediante la GUI de SnapCenter o el cmdlet de PowerShell. Una vez agregado el host, el complemento se descubre automáticamente.

Supervisar el estado de instalación del paquete de complementos de SnapCenter

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido

-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Huella digital**.
 - d. Copia los caracteres hexadecimales del cuadro.
 - e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b",

después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:

- a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado recientemente instalado por el nombre del sujeto.

```
Get-ChildItem -Path Certificado:\LocalMachine\Mi
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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"
```

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado

CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Configurar SnapManager 7.x para que Exchange y SnapCenter coexistan

Para permitir que el complemento SnapCenter para Microsoft Exchange Server coexista con SnapManager para Microsoft Exchange Server, debe instalar el complemento SnapCenter para Microsoft Exchange Server en el mismo Exchange Server en el que está instalado SnapManager para Microsoft Exchange Server, deshabilitar las programaciones de SnapManager para Exchange y configurar nuevas programaciones y copias de seguridad mediante el complemento SnapCenter para Microsoft Exchange Server.

Antes de empezar

- SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya están instalados, y existen copias de seguridad de SnapManager para Microsoft Exchange Server en el sistema y en el directorio SnapInfo.
- Deberías haber eliminado o recuperado las copias de seguridad realizadas por SnapManager para Microsoft Exchange Server que ya no necesitas.
- Debería haber suspendido o eliminado todas las programaciones creadas por SnapManager para

Microsoft Exchange Server desde el programador de Windows.

- El complemento SnapCenter para Microsoft Exchange Server y SnapManager para Microsoft Exchange Server pueden coexistir en el mismo Exchange Server, pero no es posible actualizar instalaciones existentes de SnapManager para Microsoft Exchange Server a SnapCenter.

SnapCenter no ofrece una opción para la actualización.

- SnapCenter no admite la restauración de bases de datos de Exchange desde SnapManager para la copia de seguridad de Microsoft Exchange Server.

Si no desinstala SnapManager para Microsoft Exchange Server después de la instalación del complemento de SnapCenter para Microsoft Exchange Server y luego desea restaurar una copia de seguridad de SnapManager para Microsoft Exchange Server, debe realizar pasos adicionales.

Pasos

1. Mediante PowerShell en todos los nodos DAG, determine si el proveedor de hardware VSS de SnapDrive para Windows está registrado: *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. Desde el directorio SnapDrive , anule el registro del proveedor de hardware VSS de SnapDrive para Windows: *navssprv.exe -r service -u*
3. Verifique que se haya eliminado el proveedor de hardware VSS: *vssadmin list providers*
4. Agregue el host de Exchange a SnapCenter y luego instale el complemento de SnapCenter para Microsoft Windows y el complemento de SnapCenter para Microsoft Exchange Server.
5. Desde el directorio del complemento SnapCenter para Microsoft Windows en todos los nodos DAG, verifique que el proveedor de hardware VSS 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. Detener las programaciones de copia de seguridad de SnapManager para Microsoft Exchange Server.
7. Usando la GUI de SnapCenter , cree copias de seguridad a pedido, configure copias de seguridad programadas y configure ajustes de retención.
8. Desinstalar SnapManager para Microsoft Exchange Server.

Si no desinstala SnapManager para Microsoft Exchange Server ahora y más tarde desea restaurar una copia de seguridad de SnapManager para Microsoft Exchange Server:

- a. Anular el registro del complemento de SnapCenter para Microsoft Exchange Server en 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. Desde el directorio `C:\Archivos de programa\NetApp\SnapDrive\`, registre SnapDrive para Windows en todos los nodos DAG: `navssprv.exe -r service -a hostname\username -p password`

Instalar el SnapCenter Plug-in for VMware vSphere

Si su base de datos o sistema de archivos está almacenado en máquinas virtuales (VM), o si desea proteger las VM y los almacenes de datos, debe implementar el SnapCenter Plug-in for VMware vSphere .

Para obtener información sobre la implementación, consulte ["Descripción general de la implementación"](#) .

Implementar certificado de CA

Para configurar el certificado CA con el SnapCenter Plug-in for VMware vSphere, consulte ["Crear o importar certificado SSL"](#) .

Configurar el archivo CRL

El SnapCenter Plug-in for VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL para el SnapCenter Plug-in for VMware vSphere es `/opt/netapp/config/crl`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Prepárese para la protección de datos

Antes de realizar cualquier operación de protección de datos, como copias de seguridad, clonación o restauración, debe definir su estrategia y configurar el entorno. También puede configurar el servidor SnapCenter para utilizar la tecnología SnapMirror y SnapVault .

Para aprovechar la tecnología SnapVault y SnapMirror , debe configurar e inicializar una relación de protección de datos entre los volúmenes de origen y destino en el dispositivo de almacenamiento. Puede

utilizar NetAppSystem Manager o puede utilizar la línea de comandos de la consola de almacenamiento para realizar estas tareas.

Encuentre más información

["Introducción a la API REST"](#)

Requisitos previos para utilizar el complemento de SnapCenter para Microsoft Exchange Server

Antes de utilizar el complemento para Exchange, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter.
- Configure el entorno de SnapCenter agregando o asignando conexiones del sistema de almacenamiento y creando una credencial.



SnapCenter no admite varias SVM con el mismo nombre en diferentes clústeres. Cada SVM compatible con SnapCenter debe tener un nombre único.

- Agregue hosts, instale el complemento de SnapCenter para Microsoft Windows y el complemento de SnapCenter para Microsoft Exchange Server, y descubra (actualice) los recursos.
- Realice el aprovisionamiento de almacenamiento del lado del host mediante el complemento SnapCenter para Microsoft Windows.
- Si utiliza SnapCenter Server para proteger bases de datos de Exchange que residen en LUN de VMware RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter. La documentación del SnapCenter Plug-in for VMware vSphere tiene más información.



Los VMDK no son compatibles.

- Mueva una base de datos existente de Microsoft Exchange Server desde un disco local a un almacenamiento compatible mediante las herramientas de Microsoft Exchange.
- Configure las relaciones de SnapMirror y SnapVault, si desea una replicación del backup.

Para los usuarios de SnapCenter 4.1.1, la documentación del SnapCenter Plug-in for VMware vSphere 4.1.1 tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, NetApp Data Broker 1.0 y 1.0.1, la documentación tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados mediante el SnapCenter Plug-in for VMware vSphere que proporciona el dispositivo virtual NetApp Data Broker basado en Linux (formato Open Virtual Appliance). Para los usuarios de SnapCenter 4.3.x, la documentación del SnapCenter Plug-in for VMware vSphere 4.3 tiene información sobre cómo proteger bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual basado en Linux del SnapCenter Plug-in for VMware vSphere (formato Open Virtual Appliance).

["Documentación del SnapCenter Plug-in for VMware vSphere"](#)

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger Exchange Server

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de

copia de seguridad, restauración y reinicialización que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser bases de datos de buzones de correo o grupos de disponibilidad de bases de datos (DAG) de Microsoft Exchange que se respaldan con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host o DAG de Exchange, y el grupo de recursos puede incluir un DAG completo o bases de datos individuales.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

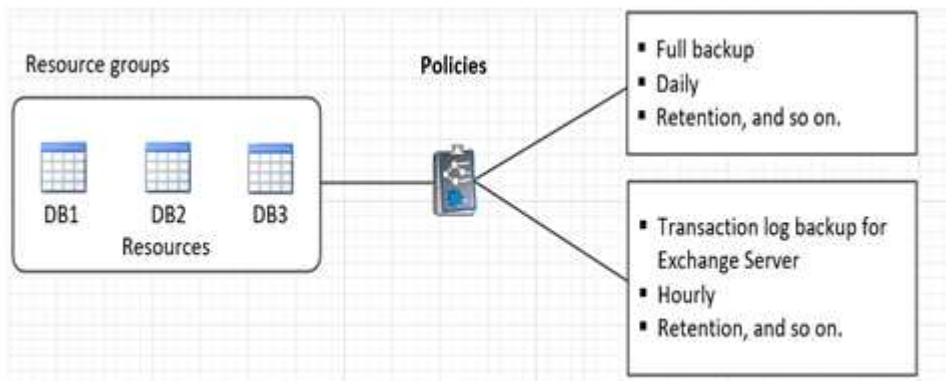
Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

Los grupos de recursos antes se conocían como conjuntos de datos.

- Las políticas especifican la frecuencia de las copias de seguridad, la retención de copias, los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede seleccionar una o más políticas cuando realiza una copia de seguridad a pedido para un solo recurso.

Piense en un grupo de recursos como si definiera *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera *cómo* desea protegerla. Si está realizando una copia de seguridad de todas las bases de datos de un host, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos del host. Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Al crear el grupo de recursos y adjuntar las políticas, puede configurar el grupo de recursos para realizar una copia de seguridad completa diariamente y otra programación que realice copias de seguridad de registros cada hora. La siguiente imagen ilustra la relación entre recursos, grupos de recursos y políticas para bases de datos:



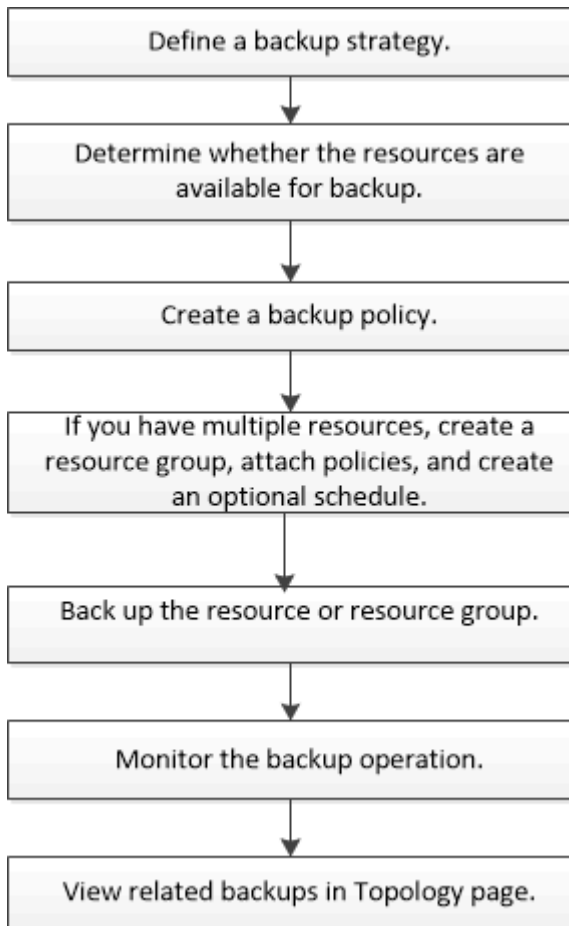
Realizar copias de seguridad de los recursos de Exchange

Flujo de trabajo de respaldo

Cuando instala el complemento de SnapCenter para Microsoft Exchange Server en su entorno, puede usar SnapCenter para realizar copias de seguridad de los recursos de Exchange.

Puede programar varias copias de seguridad para que se ejecuten en todos los servidores simultáneamente. Las operaciones de copia de seguridad y restauración no se pueden realizar simultáneamente en el mismo recurso. No se admiten copias de seguridad activas y pasivas en el mismo volumen.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



Verificación de la base de datos y de la copia de seguridad de Exchange

El complemento de SnapCenter para Microsoft Exchange Server no proporciona verificación de copias de seguridad; sin embargo, puede usar la herramienta Eseutil proporcionada con Exchange para verificar las bases de datos y las copias de seguridad de Exchange.

La herramienta Microsoft Exchange Eseutil es una utilidad de línea de comandos que se incluye con su servidor Exchange. La utilidad le permite realizar comprobaciones de coherencia para verificar la integridad de las bases de datos y copias de seguridad de Exchange.

Mejor práctica: No es necesario realizar comprobaciones de coherencia en las bases de datos que forman parte de una configuración de grupo de disponibilidad de base de datos (DAG) con al menos dos réplicas.

Para obtener información adicional, consulte ["Documentación de Microsoft Exchange Server"](#) .

Determinar si los recursos de Exchange están disponibles para realizar copias de seguridad

Los recursos son las bases de datos, los grupos de disponibilidad de bases de datos de Exchange que mantienen los complementos que ha instalado. Puede agregar esos recursos a grupos de recursos para poder realizar trabajos de protección de datos, pero primero debe identificar qué recursos tiene disponibles. La determinación de los recursos disponibles también verifica que la instalación del complemento se haya completado correctamente.

Antes de empezar

- Debe haber completado ya tareas como instalar SnapCenter Server, agregar hosts, crear conexiones al sistema de almacenamiento, agregar credenciales e instalar el complemento para Exchange.
- Para aprovechar las características del software Single Mailbox Recovery, debe haber ubicado su base de datos activa en el servidor Exchange donde está instalado el software Single Mailbox Recovery.
- Si las bases de datos residen en LUN de VMware RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter. El ["Documentación del SnapCenter Plug-in for VMware vSphere"](#) tiene más información

Acerca de esta tarea

- No se pueden realizar copias de seguridad de bases de datos cuando la opción **Estado general** en la página Detalles está configurada en No disponible para copia de seguridad. La opción **Estado general** se establece como No disponible para copia de seguridad cuando se cumple alguna de las siguientes condiciones:
 - Las bases de datos no están 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 de montaje, desmontaje, resiembra o recuperación pendiente.

- Si tiene un grupo de disponibilidad de base de datos (DAG), puede realizar una copia de seguridad de todas las bases de datos del grupo ejecutando el trabajo de copia de seguridad desde el DAG.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione **Microsoft Exchange Server** en la lista desplegable de complementos ubicada en la esquina superior izquierda de la página Recursos.
2. En la página Recursos, seleccione **Base de datos**, o **Grupo de disponibilidad de base de datos**, o **Grupo de recursos**, en la lista desplegable **Ver**.

Todas las bases de datos y DAG se muestran con su DAG o nombres de host en formato FQDN, para que pueda distinguir entre varias bases de datos.

Hacer clic  y seleccione el nombre del host y el servidor Exchange para filtrar los recursos. Luego puedes hacer clic  para cerrar el panel de filtro.

3. Haga clic en **Actualizar recursos**.

Los recursos recientemente agregados, renombrados o eliminados se actualizan en el inventario de SnapCenter Server.



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

Los recursos se muestran junto con información como el nombre del recurso, el nombre del grupo de disponibilidad de la base de datos, el servidor en el que la base de datos está actualmente activa, el servidor con copias, la hora de la última copia de seguridad y el estado general.

- Si la base de datos está en un almacenamiento que no es de NetApp , en la columna Estado general se muestra No disponible para respaldo.

En un DAG, si la copia de la base de datos activa está en un almacenamiento que no es de NetApp y si al menos una copia de la base de datos pasiva está en un almacenamiento de NetApp , se muestra No protegido en la columna **Estado general**.

No se pueden realizar operaciones de protección de datos en una base de datos que esté en un tipo de almacenamiento que no sea NetApp .

- Si la base de datos está en el almacenamiento de NetApp y no está protegida, se muestra No protegido en la columna **Estado general**.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, la interfaz de usuario muestra el mensaje "Copia de seguridad no ejecutada" en la columna **Estado general**.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, y se activa la copia de seguridad para la base de datos, la interfaz de usuario muestra el mensaje Copia de seguridad exitosa en la columna **Estado general**.

Crear políticas de copia de seguridad para bases de datos de Exchange Server

Puede crear una política de respaldo para los recursos de Exchange o para los grupos de recursos antes de usar SnapCenter para realizar copias de seguridad de los recursos de Microsoft Exchange Server, o puede crear una política de respaldo en el momento en que crea un grupo de recursos o realiza una copia de seguridad de un solo recurso.

Antes de empezar

- Debes haber definido tu estrategia de protección de datos.

Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para bases de datos de Exchange.

- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, identificar recursos y crear conexiones del sistema de almacenamiento.
- Debes haber actualizado (descubierto) los recursos de Exchange Server.
- Si está replicando instantáneas a un espejo o bóveda, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) tanto para los volúmenes de origen como para los volúmenes de destino.
- Si desea ejecutar los scripts de PowerShell en prescripts y postscripts, debe establecer el valor de `usePowershellProcessforScripts` parámetro a verdadero en el `web.config` archivo.

El valor predeterminado es falso.

- Revise los requisitos previos y las limitaciones específicos de la sincronización activa de SnapMirror . Para obtener información, consulte ["Límites de objetos para la sincronización activa de SnapMirror"](#) .

Acerca de esta tarea

- Una política de respaldo es un conjunto de reglas que regulan cómo administrar y conservar los respaldos, y con qué frecuencia se realizan respaldos del recurso o grupo de recursos. Además, puede especificar la configuración del script. Especificar opciones en una política ahorra tiempo cuando desea reutilizar la política para otro grupo de recursos.
- La retención de copias de seguridad completas es específica de una política determinada. Una base de datos o un recurso que utiliza la política A con una retención de copia de seguridad completa de 4 retiene 4 copias de seguridad completas y no tiene ningún efecto en la política B para la misma base de datos o recurso, que podría tener una retención de 3 para retener 3 copias de seguridad completas.
- La retención de copias de seguridad de registros es efectiva en todas las políticas y se aplica a todas las copias de seguridad de registros de una base de datos o un recurso. Por lo tanto, cuando se realiza una copia de seguridad completa utilizando la política B, la configuración de retención de registros afecta a las copias de seguridad de registros creadas por la política A en la misma base de datos o recurso. De manera similar, la configuración de retención de registros para la política A afecta las copias de seguridad de registros creadas por la política B en la misma base de datos.
- SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.

Mejor práctica: Es mejor que configure la política de retención secundaria en función de la cantidad general de copias de seguridad completas y de registros que desee conservar. Al configurar políticas de retención secundaria, tenga en cuenta que cuando las bases de datos y los registros están en diferentes volúmenes, cada copia de seguridad puede tener tres instantáneas, y cuando las bases de datos y los registros están en el mismo volumen, cada copia de seguridad puede tener dos instantáneas.

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.

Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas que la cantidad especificada en la política.

Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de SnapLock Vault 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.

5. En la página Tipo de copia de seguridad y replicación, realice los siguientes pasos:

a. Elija el tipo de copia de seguridad:

Si quieres...	Haz esto...
Realice una copia de seguridad de los archivos de base de datos y de los registros de transacciones necesarios	Seleccione Copia de seguridad completa y Copia de seguridad de registro. Las bases de datos se respaldan con truncamiento de registros y se respaldan todos los registros, incluidos los registros truncados.  Este es el tipo de copia de seguridad recomendado.
Realice una copia de seguridad de los archivos de base de datos y de los registros de transacciones no confirmadas	Seleccione Copia de seguridad completa. Las bases de datos se respaldan con truncamiento de registros, y los registros truncados no se respaldan.
Realice una copia de seguridad de todos los registros de transacciones	Seleccione Copia de seguridad del registro. Se realiza un respaldo de todos los registros de transacciones en el sistema de archivos activo y no se trunca ningún registro. Se crea un directorio <i>scebackupinfo</i> en el mismo disco que el registro en vivo. 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.
Realice una copia de seguridad de todos los archivos de base de datos y registros de transacciones sin truncar los archivos de registro de transacciones	Seleccione Copiar copia de seguridad. Se realizan copias de seguridad de todas las bases de datos y de todos los registros, y no se truncan los registros. Normalmente, este tipo de copia de seguridad se utiliza para volver a sembrar una réplica o para probar o diagnosticar un problema.



Debe definir el espacio necesario para las copias de seguridad de registros en función de la retención de copia de seguridad completa y no en función de la retención actualizada al minuto (UTM).



Cree políticas de bóveda independientes para registros y bases de datos cuando trabaje con volúmenes de Exchange (LUN) y configure la conservación (retención) para la política de registro al doble del número para cada etiqueta que la política de base de datos, utilizando las mismas etiquetas. Para obtener más información, consulte "[Las copias de seguridad de SnapCenter para Exchange solo conservan la mitad de las instantáneas en el volumen de registro de destino de la bóveda](#)"

b. En la sección Configuración del grupo de disponibilidad de la base de datos, seleccione una acción:

Para este campo...	Haz esto...
Realizar copias de seguridad de copias activas	Seleccione esta opción para realizar copias de seguridad únicamente de las copias activas de la base de datos seleccionada. Para los grupos de disponibilidad de bases de datos (DAG), esta opción solo realiza copias de seguridad de las copias activas de todas las bases de datos en el DAG. Las copias pasivas no están respaldadas.
Copias de seguridad en servidores que se seleccionarán en el momento de creación del trabajo de copia de seguridad	Seleccione esta opción para realizar copias de seguridad de cualquier copia de las bases de datos en los servidores seleccionados, tanto activas como pasivas. Para los DAG, esta opción realiza copias de seguridad tanto activas como pasivas de todas las bases de datos en los servidores seleccionados.



En las configuraciones de clúster, las copias de seguridad se conservan en cada nodo del clúster según la configuración de retención establecida en la política. Si el nodo propietario del clúster cambia, 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 de los tipos de frecuencia: **A pedido, Por hora, Diariamente, Semanalmente y Mensualmente.**



Puede especificar la programación (fecha de inicio, fecha de finalización) para las operaciones de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

a. Seleccione la etiqueta 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 Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una instantánea local	Seleccione esta opción para mantener copias reflejadas de los conjuntos de copias de seguridad en otro volumen (SnapMirror). Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Esta opción debe estar habilitada para la sincronización activa de SnapMirror .  La política de solo principal no se puede utilizar si la sincronización activa de SnapMirror está configurada para volúmenes de Exchange ONTAP . SnapCenter no permite esto. Debes habilitar la opción "Espejo". Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Ver "Ver copias de seguridad de Exchange en la página Topología" .
Actualizar SnapVault después de crear una instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco.
Recuento de reintentos de error	Introduzca el número de intentos de replicación que deben ocurrir antes de que el proceso se detenga.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

6. En la página Retención, configure los ajustes de retención.

Las opciones que se muestran dependen del tipo de copia de seguridad y del tipo de frecuencia que haya

seleccionado previamente.



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 subyacente de ONTAP .



Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva en el destino.

- a. En la sección Configuración de retención de copias de seguridad de registros, seleccione una de las siguientes opciones:

Si quieres...	Haz esto...
Conservar solo un número específico de copias de seguridad de registros	Seleccione Número de copias de seguridad completas para las que se conservan registros y especifique la cantidad de copias de seguridad completas para las que desea capacidad de restauración actualizada al minuto. La retención actualizada al minuto (UTM) se aplica a las copias de seguridad de registros creadas mediante copias de seguridad completas o de registros. Por ejemplo, si la configuración de retención de UTM está configurada para conservar las copias de seguridad de los registros de las últimas 5 copias de seguridad completas, entonces se conservan las copias de seguridad de los registros de las últimas 5 copias de seguridad completas. Las carpetas de registro creadas como parte de las copias de seguridad completas 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 copia de seguridad completa o completa y de registro está establecida en 1 mes y la retención de UTM está establecida en 10 días, entonces la carpeta de registro creada como parte de estas copias de seguridad se eliminará según UTM. Como resultado, solo habrá carpetas de registro de 10 días y todas las demás copias de seguridad estarán marcadas para su restauración en un punto determinado del tiempo. Puede establecer el valor de retención de UTM como 0, si no desea realizar una restauración actualizada al minuto. Esto permitirá la operación de restauración en un punto determinado del tiempo. Mejor práctica: Lo ideal es que la configuración sea igual a la configuración de Instantáneas totales (copias de seguridad completas) en la sección Configuración de retención de copia de seguridad completa. Esto garantiza que los archivos de registro se conserven para cada copia de seguridad completa.

Si quieres...	Haz esto...
Conservar las copias de seguridad durante un número específico de días	Seleccione la opción Conservar copias de seguridad del registro para el último y especifique la cantidad de días durante los cuales desea conservar las copias de seguridad del registro. Se conservan las copias de seguridad de registros hasta el mismo número de días que las copias de seguridad completas.
Período de bloqueo de instantáneas	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 **Copia de seguridad de registro** como tipo de copia de seguridad, las copias de seguridad de registro se conservan como parte de la configuración de retención actualizada para copias de seguridad completas.

- b. En la sección Configuración de retención de copias de seguridad completas, seleccione una de las siguientes opciones para copias de seguridad a pedido y, luego, seleccione una para copias de seguridad completas:

Para este campo...	Haz esto...
Conservar solo un número específico de instantáneas	Si desea especificar la cantidad de copias de seguridad completas que desea conservar, seleccione la opción Total de copias de instantáneas que desea conservar y especifique la cantidad de instantáneas (copias de seguridad completas) que desea conservar. Si el número de copias de seguridad completas excede el número especificado, se eliminan las copias de seguridad completas que exceden el número especificado, y las copias más antiguas se eliminan primero.
Conservar copias de seguridad completas durante un número específico de días	Seleccione la opción Conservar copias instantáneas durante y especifique la cantidad de días durante los cuales desea conservar las instantáneas (copias de seguridad completas).
Período de bloqueo de la instantánea principal	Seleccione Período de bloqueo de copia de instantánea principal y seleccione días, meses o años. El período de retención de SnapLock debe ser inferior a 100 años.

Para este campo...	Haz esto...
Período de bloqueo de instantáneas secundarias	Seleccione Período de bloqueo de copia de instantánea secundaria y seleccione días, meses o años.

Si tiene una base de datos con solo copias de seguridad de registros y ninguna copia de seguridad completa en un host en una configuración DAG, las copias de seguridad de registros se conservan de las siguientes maneras:

- De forma predeterminada, SnapCenter busca la copia de seguridad completa más antigua de esta base de datos en todos los demás hosts del DAG y elimina todas las copias de seguridad de registros en este host que se realizaron antes de la copia de seguridad completa.
- Puede anular el comportamiento de retención predeterminado anterior para una base de datos en un host en un DAG con solo copias de seguridad de registros agregando 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 significa que mantiene hasta 10 copias de seguridad de registros en el host.

7. En la página Script, ingrese la ruta y los argumentos del prescript o postscript que se debe ejecutar antes o después de la operación de respaldo, respectivamente.

- Los argumentos de respaldo de prescript incluyen “\$Database” y “\$ServerInstance”.
- Los argumentos de respaldo de Postscript incluyen “\$Database”, “\$ServerInstance”, “\$BackupName”, “\$LogDirectory” y “\$LogSnapshot”.

Puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o postscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

8. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas para servidores Exchange

Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar y el programa de protección.

Acerca de esta tarea

- SCRIPTS_PATH se define utilizando la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: API /4.7/configsettings

Puede utilizar la API GET para mostrar el valor de la clave. La API SET no es compatible.

- 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 .
- No se admite agregar nuevas bases de datos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror .
- No se admite agregar nuevas bases de datos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror . Puede agregar recursos al grupo de recursos solo en estado normal o de conmutación por recuperación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento Microsoft Exchange Server de la lista.
2. En la página Recursos, seleccione **Base de datos** de la lista **Ver**.



Si ha agregado recientemente un recurso a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recién agregado.

3. Haga clic en **Nuevo grupo de recursos**.
4. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca el nombre del grupo de recursos.  El nombre del grupo de recursos no debe exceder los 250 caracteres.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.
Utilice un formato de nombre personalizado para la copia de instantáneas	Opcional: Ingrese un nombre y formato de instantánea personalizados. Por ejemplo, <i>customtext_resourcegroup_policy_hostname</i> o <i>resourcegroup_hostname</i>. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Recursos, realice los siguientes pasos:

- a. Seleccione el tipo de recurso y el grupo de disponibilidad de base de datos de las listas desplegables para filtrar la lista de recursos disponibles.



Si ha agregado recursos recientemente, aparecerán en la lista de Recursos disponibles solo después de actualizar su lista de recursos.

En las secciones Recursos disponibles y Recursos seleccionados, se muestra el nombre de la base de datos con el FQDN del host. Este FQDN solo indica que la base de datos está activa en ese host específico y es posible que no realice copias de seguridad en este host. Debe seleccionar uno o más servidores de respaldo en la opción Selección de servidor, donde desea realizar el respaldo en caso de que haya seleccionado la opción **Realizar copias de respaldo en servidores que se seleccionarán en el momento de creación del trabajo de respaldo** en la política.

- b. Escriba el nombre del recurso en el cuadro de texto de búsqueda o desplácese para localizar un recurso.
- c. Para mover recursos de la sección Recursos disponibles a la sección Recursos seleccionados, realice uno de los siguientes pasos:
- Seleccione **Seleccionar automáticamente todos los recursos en el mismo volumen de almacenamiento** para mover todos los recursos del mismo volumen a la sección Recursos seleccionados.
 - Seleccione los recursos de la sección Recursos disponibles y luego haga clic en la flecha derecha para moverlos a la sección Recursos seleccionados.

Los grupos de recursos de SnapCenter para Microsoft Exchange Server no pueden tener más de 30 bases de datos por instantánea. Si hay más de 30 bases de datos en un grupo de recursos, se crea una segunda instantánea para las bases de datos adicionales. Por lo tanto, se crean 2 subtrabajos bajo el trabajo de respaldo principal. Para las copias de seguridad que tienen replicación secundaria, mientras la actualización de SnapMirror o SnapVault está en progreso, podría haber escenarios en los que la actualización de ambos subtrabajos se superponga. La tarea de respaldo principal continúa ejecutándose indefinidamente incluso si los registros indican que la tarea se completó.

6. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.



Si una política contiene la opción **Realizar copias de seguridad en servidores que se seleccionarán en el momento de creación del trabajo de copia de seguridad**, se muestra una opción de selección de servidor para seleccionar uno o más servidores. La opción de selección de servidor mostrará solo el servidor donde se encuentra la base de datos seleccionada en el almacenamiento de NetApp .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. En la sección Configurar programaciones para políticas seleccionadas, haga clic en  * en la columna ***Configurar programaciones** de la política para la que desea configurar la programación.

- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación especificando la fecha de inicio, la fecha de vencimiento y la frecuencia, y luego haga clic en **Aceptar**.

Debe hacer esto para cada frecuencia indicada en la póliza. Los horarios configurados se enumeran en la columna **Horarios aplicados** en la sección Configurar horarios para políticas seleccionadas.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell. `Set-SmSmtServer` .

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

8. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para Exchange Server

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar copias de seguridad y restaurar.

Antes de empezar

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de datos única.

Pasos

1. Inicie una sesión de conexión de PowerShell mediante el `Open-SmConnection` cmdlet.

Este ejemplo abre una sesión de PowerShell:

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

2. Cree una nueva conexión al sistema de almacenamiento mediante el uso del `Add-SmStorageConnection` cmdlet.

Este ejemplo crea una nueva conexión al sistema de almacenamiento:

```
PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una nueva cuenta Ejecutar como mediante el uso de `Add-Credential` cmdlet.

Este ejemplo crea una nueva cuenta Ejecutar como denominada `ExchangeAdmin` con credenciales de Windows:

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows  
-Credential sddev\administrator
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de las bases de datos de Exchange

Si una base de datos no es parte de ningún grupo de recursos, puede realizar una copia de seguridad de la base de datos o del grupo de disponibilidad de base de datos desde la página Recursos.

Antes de empezar

- Debes haber creado una política de respaldo.
- Debe haber asignado el agregado que está utilizando la operación de respaldo al SVM utilizado por la base de datos.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".
- Si desea realizar una copia de seguridad de una base de datos o de un grupo de disponibilidad de base de datos que tiene una copia de base de datos activa/pasiva en un almacenamiento NetApp y no NetApp, y ha seleccionado la opción **Hacer copia de seguridad de copias activas o Hacer copia de seguridad de copias en servidores que se seleccionarán durante el momento de creación del trabajo de copia de seguridad** en la política, entonces los trabajos de copia de seguridad pasarán al estado de advertencia. La copia de seguridad será exitosa para la copia de base de datos activa/pasiva en el almacenamiento NetApp y la copia de seguridad fallará para la copia de base de datos activa/pasiva en el almacenamiento que no sea NetApp.

Mejor práctica: No ejecute copias de seguridad de bases de datos activas y pasivas al mismo tiempo. Puede ocurrir una condición de carrera y una de las copias de seguridad podría fallar.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el **complemento de Microsoft Exchange Server** de la lista.
2. En la página Recursos, seleccione **Base de datos** o **Grupo de disponibilidad de base de datos** en la lista **Ver**.

En la página de Recursos, la  El icono indica que la base de datos está en un almacenamiento que no es de NetApp .



En un DAG, si una copia de base de datos activa está en un almacenamiento que no es de NetApp y al menos una copia de base de datos pasiva reside en un almacenamiento de NetApp , entonces puede proteger la base de datos.

Haga clic en  y luego seleccione el nombre del host y el tipo de base de datos para filtrar los recursos. Luego puedes hacer clic en  para cerrar el panel de filtro.

- Si desea hacer una copia de seguridad de una base de datos, haga clic en el nombre de la base de datos.
 - i. Si se muestra la vista Topología, haga clic en **Proteger**.
 - ii. Si se muestra el asistente Base de datos - Proteger recurso, continúe con el Paso 3.
 - Si desea realizar una copia de seguridad de un grupo de disponibilidad de base de datos, haga clic en el nombre del grupo de disponibilidad de base de datos.
3. Si desea especificar un nombre de instantánea personalizado, en la página Recursos, seleccione la casilla de verificación **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

4. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en  .



Si una política contiene la opción **Realizar copias de seguridad en servidores que se seleccionarán en el momento de creación del trabajo de copia de seguridad**, se muestra una opción de selección de servidor para seleccionar uno o más servidores. La opción de selección de servidor mostrará solo el servidor donde se encuentra la base de datos seleccionada en un almacenamiento NetApp .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

b.

Haga clic en  en la columna Configurar programaciones de la política para la que desea

configurar una programación.

- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

5. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de respaldo realizada en el recurso, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell `Set-SmSmtplibServer`.

6. Revise el resumen y luego haga clic en **Finalizar**.

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

7. Haga clic en **Hacer copia de seguridad ahora**.

8. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

- b. Haga clic en **Copia de seguridad**.

9. Supervise el progreso de la copia de seguridad haciendo doble clic en el trabajo en el panel Actividad en la parte inferior de la página para mostrar la página Detalles del trabajo.

- En configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

Para obtener información, consulte: ["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar.

Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese script, el comando `do_start method` inicia el servicio del complemento VMware de SnapCenter. Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

Se muestra la solicitud de nombre de usuario y contraseña.

2. Cree una política de respaldo mediante el cmdlet `Add-SmPolicy`.

Este ejemplo crea una nueva política de respaldo con un tipo de respaldo de Exchange de respaldo completo y respaldo de registro:

```
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 respaldo con una copia de seguridad completa cada hora y un tipo de copia de seguridad de registro 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 respaldo para realizar copias de seguridad únicamente de los registros de Exchange:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup  
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Descubra los recursos del host mediante el cmdlet `Get-SmResources`.

Este ejemplo descubre los recursos para el complemento de Microsoft Exchange Server en el host especificado:

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCE
```

4. Agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet `Add-SmResourceGroup`.

Este ejemplo crea un nuevo grupo de recursos de copia de seguridad de la base de datos de Exchange Server con la política y los recursos especificados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

Este ejemplo crea un nuevo grupo de recursos de respaldo del grupo de disponibilidad de base de datos (DAG) de Exchange con la política y los recursos especificados:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

5. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

Este ejemplo crea una nueva copia de seguridad en un almacenamiento secundario:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Vea el estado del trabajo de respaldo mediante el cmdlet Get-SmBackupReport.

Este ejemplo muestra un informe de resumen de trabajos de todos los trabajos que se ejecutaron en la fecha especificada:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Este ejemplo muestra un informe de resumen de trabajo para un ID de trabajo específico:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, véase ["Guía de referencia de cmdlets"](#)

Realizar copias de seguridad de grupos de recursos de Exchange

Un grupo de recursos es una colección de recursos en un host o DAG de Exchange, y el grupo de recursos puede incluir un DAG completo o bases de datos individuales. Puede realizar una copia de seguridad de los grupos de recursos desde la página Recursos.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.
- Debe haber asignado el agregado que utiliza la operación de respaldo a la máquina virtual de almacenamiento (SVM) utilizada por la base de datos.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".
- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, la operación de respaldo en algunos de los hosts podría comenzar tarde debido a problemas de red. Debes configurar el valor de `MaxRetryForUninitializedHosts` en `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 que tiene una copia de base de datos activa/pasiva en un almacenamiento NetApp y no NetApp, y ha seleccionado la opción **Hacer copia de seguridad de copias activas o Hacer copia de seguridad de copias en servidores que se seleccionarán durante el momento de creación del trabajo de copia de seguridad** en la política, entonces los trabajos de copia de seguridad pasarán al estado de advertencia.

La copia de seguridad será exitosa para la copia de base de datos activa/pasiva en el almacenamiento NetApp y la copia de seguridad fallará para la copia de base de datos activa/pasiva en el almacenamiento que no sea NetApp.

Acerca de esta tarea

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el **complemento de Microsoft Exchange Server** de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o haciendo clic en  y luego seleccionando la etiqueta. Luego puedes hacer clic en  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y haga clic en **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si ha asociado varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

b. Haga clic en **Copia de seguridad**.

5. Supervise el progreso de la copia de seguridad haciendo doble clic en el trabajo en el panel Actividad en la parte inferior de la página para mostrar la página Detalles del trabajo.

Supervisar las operaciones de copia de seguridad

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desee verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar operaciones en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 operaciones de copia de seguridad de la base de datos de Exchange

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de copia de seguridad.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	a. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. b. Seleccione la operación y luego haga clic en Cancelar trabajo.

Desde...	Acción
Panel de actividades	a. Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Ver copias de seguridad de Exchange en la página Topología

Cuando se prepara para realizar una copia de seguridad de un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad en los almacenamientos primario y secundario.

Acerca de esta tarea

En la página Topología, puede ver todas las copias de seguridad disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y luego seleccionarlas para realizar operaciones de protección de datos.

Puede revisar el siguiente ícono en la vista Administrar copias para determinar si las copias de seguridad están disponibles en el almacenamiento principal o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad reflejadas en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad que se replican en el almacenamiento secundario mediante la tecnología SnapVault .
 - La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario.

Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.

Mejor práctica: para garantizar que se muestre la cantidad correcta de copias de seguridad replicadas, recomendamos actualizar la topología.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), puede ver los siguientes íconos adicionales:

-  El sitio de réplica está activo.
-  El sitio de réplica está inactivo.
-  No se ha restablecido la relación de espejo secundario o bóveda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione la base de datos, el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione 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 Topología del recurso seleccionado.

4. Revise la sección de la tarjeta Resumen para ver un resumen de la cantidad de copias de seguridad disponibles en el almacenamiento primario y secundario.

La sección Tarjeta de resumen muestra el número total de copias de seguridad y el número total de copias de seguridad 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración 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 respaldo de SnapCenter consultando a ONTAP los sitios principales y de réplica. Una programación semanal también realiza esta actividad para 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 Async Mirror o Async MirrorVault con el nuevo destino principal se deben configurar manualmente después de la conmutación por error. Desde ONTAP 9.15.1 en adelante, Async Mirror o Async MirrorVault se configura automáticamente en el nuevo destino principal después de la conmutación por error.
 - Después de la conmutación por error, se debe crear una copia de seguridad para que SnapCenter esté al tanto de la conmutación por error. Puede hacer clic en **Actualizar** sólo después de haber creado una copia de seguridad.
5. En la vista Administrar copias, haga clic en **Copias de seguridad** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad.

Los detalles de las copias de seguridad se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, cambio de nombre y eliminación.



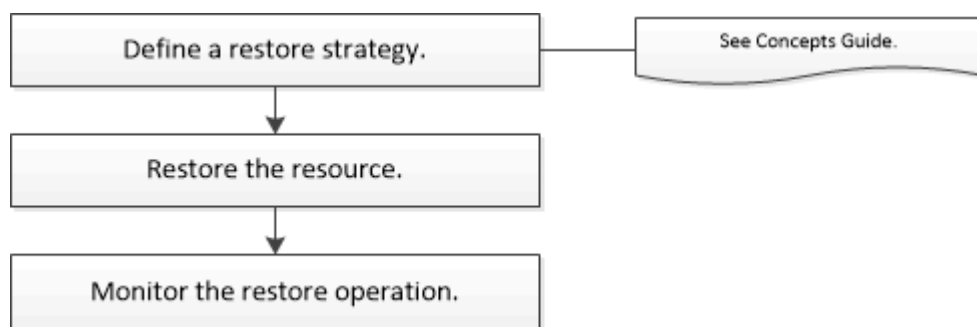
No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario. La eliminación de instantáneas se gestiona mediante la configuración de retención de ONTAP .

Restaurar recursos de Exchange

Restaurar flujo de trabajo

Puede utilizar SnapCenter para restaurar bases de datos de Exchange restaurando una o más copias de seguridad en su sistema de archivos activo.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar las operaciones de restauración de la base de datos de Exchange:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad y restauración. Para obtener información detallada sobre los cmdlets de PowerShell, utilice la ayuda de cmdlets de SnapCenter o consulte ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Requisitos para restaurar una base de datos de Exchange

Antes de restaurar una base de datos de Exchange Server desde una copia de seguridad del complemento de SnapCenter para Microsoft Exchange Server, debe asegurarse de que se cumplan varios requisitos.



Para utilizar la funcionalidad de restauración por completo, debe actualizar tanto SnapCenter Server como la base de datos del complemento SnapCenter para Exchange a 4.6.

- El servidor Exchange debe estar en línea y en ejecución antes de poder restaurar una base de datos.
- Las bases de datos deben existir en el servidor Exchange.



No se admite la restauración de bases de datos eliminadas.

- Las programaciones de SnapCenter para la base de datos deben suspenderse.
- El servidor SnapCenter y el complemento SnapCenter para el host de Microsoft Exchange Server deben estar conectados al almacenamiento principal y secundario que contiene las copias de seguridad que desea restaurar.

Restaurar bases de datos de Exchange

Puede utilizar SnapCenter para restaurar bases de datos de Exchange respaldadas.

Antes de empezar

- Debe haber realizado una copia de seguridad de los grupos de recursos, la base de datos o los grupos de disponibilidad de bases de datos (DAG).
- Cuando se migra una base de datos de Exchange a otra ubicación, la operación de restauración no funciona para copias de seguridad antiguas.
- Si está replicando instantáneas a un espejo o bóveda, el administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y de destino.
- En un DAG, si una copia de base de datos activa está en un almacenamiento que no es NetApp y desea restaurarla desde la copia de seguridad de la copia de base de datos pasiva que está en un almacenamiento NetApp , haga la copia pasiva (almacenamiento NetApp) como copia activa, actualice los recursos y realice la operación de restauración.

Ejecutar el `Move-ActiveMailboxDatabase` Comando para hacer que la copia de la base de datos pasiva sea una copia de la base de datos activa.

El "[Documentación de Microsoft](#)" Contiene información sobre este comando.

Acerca de esta tarea

- Cuando se realiza una operación de restauración en una base de datos, la base de datos se vuelve a montar en el mismo host y no se crea ningún volumen nuevo.
- Las copias de seguridad a nivel DAG deben restaurarse desde bases de datos individuales.
- No se admite la restauración completa del disco cuando existen archivos distintos del archivo de base de datos de Exchange (.edb).

El complemento 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 complemento para Exchange realiza una única operación de restauración de archivo.

- El complemento para Exchange no puede restaurar unidades cifradas con BitLocker.
- `SCRIPTS_PATH` se define utilizando la clave `PredefinedWindowsScriptsDirectory` ubicada en el archivo `SMCoreServiceHost.exe.Config` del host del complemento.

Si es necesario, puede cambiar esta ruta y reiniciar el servicio `SMcore`. Se recomienda que utilice la ruta predeterminada por seguridad.

El valor de la clave se puede mostrar desde swagger a través de la API: `API /4.7/configsettings`

Puede utilizar la API `GET` para mostrar el valor de la clave. La API `SET` no es compatible.

- 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 .
- Para la operación de restauración de sincronización activa de SnapMirror , debe seleccionar la copia de seguridad de la ubicación principal.

Interfaz de usuario 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 complemento de Exchange Server de la lista desplegable.
3. En la página Recursos, seleccione **Base de datos** de la lista Ver.
4. Seleccione la base de datos de la lista.
5. Desde la vista Administrar copias, seleccione **Copias de seguridad**, en la tabla Copias de seguridad principales, y luego haga clic en *  *.
6. En la página Opciones, seleccione una de las siguientes opciones de copia de seguridad de registros:

Opción	Descripción
Todas las copias de seguridad de registros	Seleccione Todas las copias de seguridad de registros para realizar una operación de restauración de copia de seguridad actualizada para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa.
Mediante copias de seguridad de registros hasta	Seleccione Por copias de seguridad de registros hasta para realizar una operación de restauración en un punto en el tiempo, que restaura la base de datos basándose en las copias de seguridad de registros hasta el registro seleccionado.  La cantidad de registros que se muestran en la lista desplegable se basa en UTM. Por ejemplo, si la retención de copia de seguridad completa es 5 y la retención de UTM es 3, la cantidad de copias de seguridad de registros disponibles es 5, pero en el menú desplegable solo se enumerarán 3 registros para realizar la operación de restauración.

Opción	Descripción
Por fecha específica hasta	Seleccione Por fecha específica hasta para especificar la fecha y la hora hasta la cual se aplicarán los registros de transacciones a la base de datos restaurada. Esta operación de restauración en un punto determinado del tiempo restaura las entradas del registro de transacciones que se registraron hasta la última copia de seguridad en la fecha y hora especificadas.
Ninguno	Elija Ninguno cuando necesite restaurar solo la copia de seguridad completa sin ninguna copia de seguridad de registros.

Puede realizar una de las siguientes acciones:

- **Recuperar y montar la base de datos después de la restauración:** esta opción está seleccionada de forma predeterminada.
- **No verificar la integridad de los registros de transacciones en la copia de seguridad antes de restaurar:** 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.

- En la página Script, ingrese la ruta y los argumentos del prescript o postscript que deben ejecutarse antes o después de la operación de restauración, respectivamente.

Los argumentos de restauración del script incluyen \$Database y \$ServerInstance.

Los argumentos de restauración de postscript incluyen \$Database, \$ServerInstance, \$BackupName, \$LogDirectory y \$TargetServerInstance.

Puede ejecutar un script para actualizar trampas SNMP, automatizar alertas, enviar registros, etc.



La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

- En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

- Revise el resumen y luego haga clic en **Finalizar**.

- Puede ver el estado del trabajo de restauración expandiendo el panel Actividad en la parte inferior de la página.

Debes supervisar el proceso de restauración utilizando la página **Monitor > Trabajos**.

Al restaurar una base de datos activa desde una copia de seguridad, la base de datos pasiva puede entrar en estado suspendido o fallido si hay un retraso entre la réplica y la base de datos activa.

El cambio de estado puede ocurrir cuando la cadena de registro de la base de datos activa se bifurca y comienza una nueva rama que interrumpe la replicación. Exchange Server intenta reparar la réplica, pero si no puede hacerlo, después de la restauración debe crear una nueva copia de seguridad y luego volver a iniciar la réplica.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el uso del `Open-SmConnection` cmdlet.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. Recupere la información sobre una o más copias de seguridad que desea restaurar mediante el uso de `Get-SmBackup` cmdlet.

Este ejemplo muestra información sobre todas las copias de seguridad 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. Restaurar datos desde la copia de seguridad mediante el uso de `Restore-SmBackup` cmdlet.

Este ejemplo restaura una copia de seguridad actualizada al 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 una copia de seguridad de un punto en el tiempo:

```
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 una copia de seguridad del almacenamiento secundario en la historia principal:

```
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
```

El `-archive` Este parámetro le permite especificar los volúmenes primarios y secundarios que desea utilizar para la restauración.

El `-IsRecoverMount:$true` El parámetro le permite montar la base de datos después de la restauración.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Recuperación granular de correos y buzones

El software Single Mailbox Recovery (SMBR) le permite restaurar y recuperar correos o buzones en lugar de la base de datos de Exchange completa.

Restaurar una base de datos completa sólo para recuperar un solo correo consumirá mucho tiempo y recursos. SMBR ayuda a recuperar rápidamente los correos creando una copia clonada de la instantánea y luego utilizando las API de Microsoft para montar el buzón en SMBR. Para obtener información sobre cómo utilizar SMBR, consulte ["Guía de administración de SMBR"](#).

Para obtener información adicional sobre SMBR, consulte lo siguiente:

- ["Cómo restaurar manualmente un solo elemento con SMBR \(también aplicable para restauraciones de Ontrack Power Control\)"](#)
- ["Cómo restaurar desde el almacenamiento secundario en SMBR con SnapCenter"](#)
- ["Recuperación de correo de Microsoft Exchange desde SnapVault mediante SMBR"](#)

Restaurar una base de datos de Exchange Server desde un almacenamiento secundario

Puede restaurar una base de datos de Exchange Server respaldada desde un almacenamiento secundario (espejo o bóveda).

Debes haber replicado las instantáneas del almacenamiento principal a un almacenamiento secundario.

Acerca de esta tarea

- 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 .
- Para la operación de restauración de sincronización activa de SnapMirror , debe seleccionar la copia de seguridad de la ubicación principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **Complemento de Microsoft Exchange Server** de la lista.
2. En la página Recursos, seleccione **Base de datos** o **Grupo de recursos** en la lista desplegable **Ver**.
3. Seleccione la base de datos o el grupo de recursos.

Se muestra la página de topología de la base de datos o del grupo de recursos.

4. En la sección Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento secundario (espejo o bóveda).
5. Seleccione la copia de seguridad de la lista y luego haga clic en  .
6. En la página Ubicación, elija el volumen de destino para restaurar el recurso seleccionado.
7. Complete el asistente de restauración, revise el resumen y luego haga clic en **Finalizar**.

Resembrar una réplica de nodo de Exchange pasivo

Si necesita volver a sembrar una copia de réplica, por ejemplo cuando una copia está dañada, puede volver a sembrar la última copia de seguridad usando la función de resembrado en SnapCenter.

Antes de empezar

Debes haber creado una copia de seguridad de la base de datos que desees volver a sembrar.

+ Para evitar retrasos entre nodos, puede crear una nueva copia de seguridad antes de realizar una operación de resiembra 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 **Complemento de Microsoft Exchange Server** de la lista.
2. En la página Recursos, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para volver a sembrar una sola base de datos	Seleccione Base de datos de la lista Ver.
Para volver a sembrar bases de datos en un DAG	Seleccione Grupo de disponibilidad de base de datos de la lista Ver.

3. Seleccione el recurso que desea resembrar.

4. En la página Administrar copias, haga clic en **Resembrar**.
5. De la lista de copias de bases de datos no saludables en el asistente de resembrado, seleccione la que desea resembrar y luego haga clic en **Siguiente**.
6. En la ventana Host, seleccione el host con la copia de seguridad desde la que desea volver a sembrar y luego haga clic en **Siguiente**.
7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

8. Revise el resumen y luego haga clic en **Finalizar**.
9. Puede ver el estado del trabajo expandiendo el panel Actividad en la parte inferior de la página.



La operación de resembrado no se admite si la copia de la base de datos pasiva reside en un almacenamiento que no es de NetApp .

Resembrar una réplica mediante cmdlets de PowerShell para la base de datos de Exchange

Puede usar cmdlets de PowerShell para restaurar una réplica en mal estado utilizando la copia más reciente en el mismo host o la copia más reciente de un host alternativo.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el uso del `Open-SmConnection` cmdlet.

```
Open-smconnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Vuelva a sembrar la base de datos mediante el uso de `reseed-SmDagReplicaCopy` cmdlet.

Este ejemplo vuelve a sembrar la copia fallida de la base de datos llamada `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
```

Este ejemplo vuelve a sembrar la copia fallida de la base de datos llamada `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 las operaciones de restauración

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Cancelar operaciones de restauración de la base de datos de Exchange

Puede cancelar trabajos de restauración que estén en cola.

Debe iniciar 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.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones de restauración que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de restauración en cola de otros miembros mientras usan ese rol.

Paso

Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	1. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. 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 Actividad 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

Descripción general del complemento SnapCenter para IBM Db2

El complemento SnapCenter para la base de datos IBM Db2 es un componente del lado del host del SnapCenter software de NetApp que permite la gestión de protección de datos teniendo en cuenta las aplicaciones de las bases de datos IBM Db2. El complemento para IBM Db2 Database automatiza la copia de seguridad, la restauración y la clonación de bases de datos IBM Db2 en su entorno 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. Además, a partir de SnapCenter 6.0.1, se admite IBM Db2 en AIX.

SnapCenter admite configuraciones de Db2 de instancia única y de instancias múltiples. Puede utilizar el complemento para IBM Db2 Database en entornos Linux y Windows. En entornos Windows, Db2 se admitirá como recurso manual.



El entorno Db2 pureScale y los sistemas Db2 multinodo (DPF) no son compatibles.

Cuando se instala el complemento para IBM Db2 Database, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen. También puede utilizar el complemento con la tecnología NetApp SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de los estándares.

El complemento SnapCenter para Db2 admite NFS y SAN en diseños de almacenamiento de archivos ONTAP y Azure NetApp .

Se admite el diseño de almacenamiento virtual VMDK, vVol y RDM.

Qué puede hacer utilizando el complemento SnapCenter para IBM Db2

Cuando instala el complemento para IBM Db2 Database en su entorno, puede utilizar SnapCenter para realizar copias de seguridad, restaurar y clonar bases de datos IBM Db2 y sus recursos. También puede realizar tareas de apoyo a dichas operaciones.

- Agregar bases de datos.
- Crear copias de seguridad.
- Restaurar desde copias de seguridad.
- Copias de seguridad clonadas.
- Programar operaciones de respaldo.
- Supervisar operaciones de copia de seguridad, restauración y clonación.
- Ver informes de operaciones de copia de seguridad, restauración y clonación.

Funciones del complemento SnapCenter para IBM Db2

SnapCenter se integra con la aplicación complementaria y con las tecnologías NetApp en el sistema de almacenamiento. Para trabajar con el complemento para IBM Db2 Database, utilice la interfaz gráfica de usuario de SnapCenter .

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite realizar operaciones consistentes de copia de seguridad, restauración y clonación en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y supervisar trabajos en todos los complementos.

- **Administración central automatizada**

Puede programar operaciones de respaldo, configurar la retención de respaldo basada en políticas y realizar operaciones de restauración. También puede supervisar su entorno de forma proactiva configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología de copia de instantáneas de NetApp sin interrupciones**

SnapCenter utiliza la tecnología de instantáneas de NetApp con el complemento para IBM Db2 Database para realizar copias de seguridad de los recursos.

El uso del complemento para IBM Db2 también ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de copia de seguridad, restauración y clonación
- Seguridad respaldada por RBAC y delegación de roles centralizada

También puede configurar las credenciales para que los usuarios autorizados de SnapCenter tengan permisos a nivel de aplicación.

- Creación de copias puntuales y con uso eficiente del espacio de recursos para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

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

- Compatibilidad con la función de instantánea del grupo de consistencia (CG) de ONTAP como parte de la creación de copias de seguridad.
- Capacidad de ejecutar múltiples copias de seguridad simultáneamente en múltiples hosts de recursos

En una sola operación, las instantáneas se consolidan cuando los recursos de un solo host comparten el mismo volumen.

- Capacidad de crear instantáneas mediante comandos externos.
- Soporte para Linux LVM en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el complemento SnapCenter para IBM Db2

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas físicas como en máquinas virtuales (VM). Debe verificar el soporte para su tipo de

almacenamiento antes de instalar el complemento SnapCenter para IBM Db2.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • Volúmenes conectados a NFS
VMware ESXi	• El escaneo de los adaptadores de bus de host (HBA) puede demorar mucho tiempo en completarse porque SnapCenter escanea todos los adaptadores de bus de host presentes en el host. Puede editar el archivo LinuxConfig.pm ubicado en <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> para establecer el valor del parámetro SCSI_HOSTS_OPTIMIZED_RESCAN en 1 para volver a escanear solo los HBA que figuran en HBA_DRIVER_NAMES. • LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creados • Volúmenes NFS conectados directamente al sistema invitado • Almacenes de datos vVol tanto en NFS como en SAN El almacén de datos vVol solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP necesarios para el complemento IBM Db2

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo
 - lun crear

- lun crear
- lun crear
- eliminar lun
- agregar igroup lun
- crear igroup lun
- eliminar igroup lun
- Cambiar nombre de igroup lun
- Cambiar nombre de igroup lun
- Programa de igroup de Lun
- Asignación de LUN a nodos de informes adicionales
- creación de mapeo LUN
- eliminar mapeo lun
- Mapeo de LUN: eliminar nodos de informes
- espectáculo de mapeo de lun
- modificar lun
- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- lun reserva persistente clara
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada

- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- tiempo de caducidad de modificación de instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFS de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIFS de vserver
- Mostrar copia de sombra de CIFS de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi
- Mostrar conexión iscsi de vserver
- espectáculo vserver

- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red
 - Mostrar interfaz de red
 - vservers

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para IBM Db2

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Estrategia de respaldo para IBM Db2

Definir una estrategia de respaldo para IBM Db2

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a tener los respaldos que necesita para restaurar o clonar sus recursos con éxito. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Acerca de esta tarea

Un SLA define el nivel de servicio que se espera y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. RPO define la estrategia para la edad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA, RTO y RPO contribuyen a la estrategia de protección de datos.

Pasos

1. Determina cuándo debes realizar copias de seguridad de tus recursos.
2. Decide cuántos trabajos de respaldo necesitas.
3. Decide cómo nombrar tus copias de seguridad.
4. Decida si desea crear una política basada en copias de instantáneas para realizar copias de seguridad de instantáneas de la base de datos consistentes con la aplicación.
5. Decida si desea utilizar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
6. Determine el período de retención de las instantáneas en el sistema de almacenamiento de origen y el destino SnapMirror .
7. Determine si desea ejecutar algún comando antes o después de la operación de copia de seguridad y proporcione un script previo o posterior.

Descubrimiento automático de recursos en el host Linux

Los recursos son bases de datos e instancias de IBM Db2 en el host Linux que son administradas por SnapCenter. Después de instalar el complemento SnapCenter Plug-in para IBM Db2, las bases de datos IBM Db2 de todas las instancias en ese host Linux se detectan automáticamente y se muestran en la página Recursos.

Tipo de backups admitido

El tipo de copia de seguridad especifica el tipo de copia de seguridad que desea crear. SnapCenter admite el tipo de copia de seguridad basado en instantáneas para bases de datos IBM Db2.

Copia de seguridad basada en instantáneas

Las copias de seguridad basadas en instantáneas aprovechan la tecnología de instantáneas de NetApp para crear copias en línea, de solo lectura, de los volúmenes en los que residen las bases de datos de IBM Db2.

Cómo el complemento SnapCenter para IBM Db2 utiliza instantáneas de grupos de consistencia

Puede utilizar el complemento para crear instantáneas de grupos de consistencia para grupos de recursos. Un grupo de consistencia es un contenedor que puede albergar múltiples volúmenes para que puedas administrarlos como una sola entidad. Un grupo de consistencia son instantáneas simultáneas de múltiples volúmenes que proporcionan copias consistentes de un grupo de volúmenes.

También puede especificar el tiempo de espera para que el controlador de almacenamiento agrupe las instantáneas de manera consistente. Las opciones de tiempo de espera disponibles son **Urgente**, **Medio** y **Relajado**. También puede habilitar o deshabilitar la sincronización del diseño de archivo Write Anywhere (WAFL) durante la operación de instantánea de grupo consistente. La sincronización de WAFL mejora el rendimiento de una instantánea de grupo de consistencia.

Cómo gestiona SnapCenter el mantenimiento de las copias de seguridad de datos

SnapCenter administra el mantenimiento de las copias de seguridad de datos en los

niveles del sistema de almacenamiento y del sistema de archivos.

Las instantáneas del almacenamiento primario o secundario y sus entradas correspondientes en el catálogo de IBM Db2 se eliminan según la configuración de retención.

Consideraciones para determinar las programaciones de copias de seguridad para IBM Db2

El factor más crítico para determinar un cronograma de respaldo es la tasa de cambio del recurso. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su acuerdo de nivel de servicio (SLA) y su objetivo de punto de recuperación (RPO).

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de copia de seguridad (con qué frecuencia se deben realizar las copias de seguridad)

La frecuencia de copia de seguridad, también llamada tipo de programación para algunos complementos, es parte de una configuración de política. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual.

- Programaciones de copias de seguridad (cuándo exactamente se realizarán las copias de seguridad)

Las programaciones de copias de seguridad son parte de la configuración de un recurso o de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m.

Número de trabajos de respaldo necesarios para IBM Db2

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño del recurso, la cantidad de volúmenes utilizados, la tasa de cambio del recurso y su Acuerdo de Nivel de Servicio (SLA).

Convenciones de nombres de copia de seguridad para bases de datos de complementos IBM Db2

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

`resourcegroupname_hostname_timestamp`

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, `customtext_resourcegroup_policy_hostname` o `resourcegroup_hostname`. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Estrategia de restauración y recuperación para IBM Db2

Definir una estrategia de restauración y recuperación para los recursos de IBM Db2

Debe definir una estrategia antes de restaurar y recuperar su base de datos para poder realizar operaciones de restauración y recuperación con éxito.



Sólo se admite la recuperación manual de la base de datos.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos de IBM Db2 agregados manualmente
2. Determinar las estrategias de restauración compatibles con las bases de datos IBM Db2 detectadas automáticamente

Tipos de estrategias de restauración compatibles con recursos de IBM Db2 agregados manualmente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter. Hay dos tipos de estrategias de restauración para recursos de IBM Db2 agregados manualmente.



No es posible recuperar recursos de IBM Db2 agregados manualmente.

Restauración completa de recursos

- Restaura todos los volúmenes, qtrees y LUN de un recurso



Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Tipo de estrategia de restauración compatible con IBM Db2 detectado automáticamente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter.

La restauración completa de recursos es la estrategia de restauración compatible con las bases de datos IBM

Db2 descubiertas automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para IBM Db2 detectado automáticamente

El complemento SnapCenter para IBM Db2 admite SnapRestore de archivo único y tipos de restauración de conexión y copia para bases de datos IBM Db2 detectadas automáticamente.

SnapRestore de archivo único se realiza en entornos NFS para los siguientes escenarios:

- Si solo se selecciona la opción **Recurso completo**
- Cuando la copia de seguridad seleccionada es de una ubicación secundaria de SnapMirror o SnapVault y está seleccionada la opción **Recurso completo**

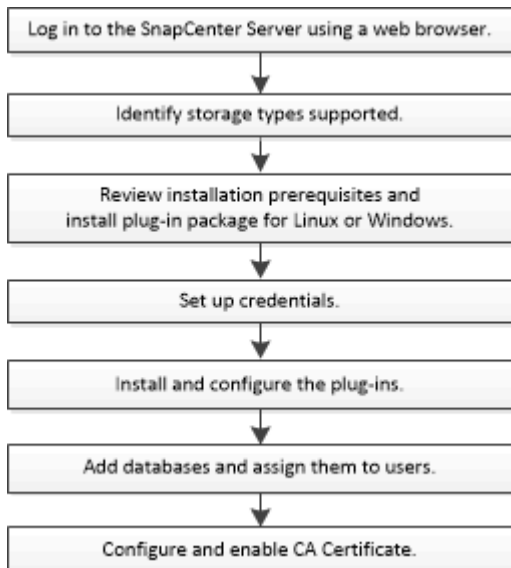
SnapRestore de archivo único se realiza en entornos SAN para los siguientes escenarios:

- Si solo se selecciona la opción **Recurso completo**
- Cuando se selecciona la copia de seguridad desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Recurso completo**

Prepárese para instalar el complemento SnapCenter para IBM Db2

Flujo de trabajo de instalación del complemento SnapCenter para IBM Db2

Debe instalar y configurar el complemento SnapCenter para IBM Db2 si desea proteger las bases de datos de IBM Db2.



Requisitos previos para agregar hosts e instalar paquetes de complementos para Windows, Linux o AIX

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos. Complemento SnapCenter para IBM Db2 compatible con entornos

Windows, Linux y AIX.

- Debes tener instalado Java 11 en tu host.



IBM Java no es compatible con hosts Windows y Linux.

- Para Windows, el servicio de creación de complementos debe ejecutarse utilizando el usuario de Windows "LocalSystem", que es el comportamiento predeterminado cuando el complemento para IBM Db2 se instala como administrador de dominio.
- Al instalar un complemento 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 complemento SnapCenter para Microsoft Windows se implementará de forma predeterminada con el complemento IBM Db2 en los hosts de Windows.
- El servidor SnapCenter debe tener acceso al puerto 8145 o personalizado del complemento para el host IBM Db2.

Hosts de Windows

- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Al instalar el complemento para IBM Db2 en un host Windows, el complemento de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Windows.

["Descargar JAVA para Windows"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Hosts Linux y AIX

- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Linux.

["Descargar JAVA para Linux"](#)

["Descargar JAVA para AIX"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Para las bases de datos IBM Db2 que se ejecutan en un host Linux, al instalar el complemento para IBM Db2, el complemento SnapCenter para UNIX se instala automáticamente.
- Debe tener **bash** como el shell predeterminado para la instalación del complemento.

Comandos suplementarios

Para ejecutar un comando complementario en el complemento 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 complementarios en el host del complemento, abra el archivo `allowed_commands.config` en un editor. Ingrese cada comando en una línea separada y los comandos no distinguen entre mayúsculas y minúsculas. Asegúrese de especificar la ruta de acceso completa y de encerrarla entre comillas (") si contiene espacios.

Por ejemplo:

comando: montar

comando: desmontar

Comando: "C:\Archivos de programa\NetApp\SnapCreator commands\sdcli.exe"

comando: myscript.bat

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.



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

Configurar privilegios de sudo para usuarios no root para el host Linux

SnapCenter permite que un usuario no root instale el paquete de complementos de SnapCenter para Linux e inicie el proceso de instalación del complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el permiso 555. De lo contrario, la instalación del complemento podría fallar.
- Para el usuario no root, asegúrese de que el nombre del usuario no root y el grupo del usuario sean los mismos.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- /inicio/*USUARIO_LINUX*/sc_netapp/snapcenter_linux_host_plugin.bin
- /ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar
- /ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl

Pasos

1. Inicie sesión en el host Linux en el que desea instalar el paquete de complementos de SnapCenter para Linux.
2. Agregue las siguientes líneas al archivo /etc/sudoers utilizando la utilidad visudo para 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_Precchecks.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 SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, 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 RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Configurar privilegios de sudo para usuarios no root para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no root instale el paquete de complementos de SnapCenter para AIX e inicie el proceso de complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el

permiso 555. De lo contrario, la instalación del complemento podría fallar.

- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- `/inicio/USUARIO_AIX/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl`

Pasos

1. Inicie sesión en el host AIX en el que desea instalar el paquete de complementos de SnapCenter para AIX.
2. Agregue las siguientes líneas al archivo `/etc/sudoers` utilizando la utilidad `visudo` para 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/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si tiene una configuración RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux

Antes de instalar el paquete de complementos de SnapCenter para Linux, debe familiarizarse con algunos requisitos básicos de tamaño y espacio del sistema host.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Servidor empresarial SUSE Linux (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .
RAM mínima para el complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 Oracle Java y OpenJDK Si ha actualizado JAVA a la última versión, 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 correcta. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Configurar credenciales para el complemento SnapCenter para IBM Db2

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en bases de datos o sistemas de archivos de Windows.

Acerca de esta tarea

- Hosts Linux

Debe configurar credenciales para instalar complementos en hosts Linux.

Debe configurar las credenciales para el usuario root o para un usuario no root que tenga privilegios de

sudo para instalar e iniciar el proceso del complemento.

Mejor práctica: Si bien se le permite crear credenciales para Linux después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

- Hosts de Windows

Debe configurar las credenciales de Windows antes de instalar complementos.

Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.

Si configura 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 de respaldo al nombre de usuario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, especifique la información necesaria para configurar las credenciales:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. - Administrador del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: <i>NetBIOS\Nombre de usuario</i> <i>Dominio FQDN\Nombre de usuario</i> - 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>NombreDeUsuario</i> No utilice comillas dobles (") ni tildes invertidas (') en las contraseñas. No debe utilizar los símbolos menor que (<) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que<!10, menos que10<!, acento grave`12.
Password	Introduzca la contraseña utilizada para la autenticación.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar.
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no sea root.  Aplicable únicamente a usuarios de Linux.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Configurar gMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -Effectivelmmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Añade objetos de computadora 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,...>  
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de  
servicio.
```

4. Configure el gMSA en sus hosts:
 - a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
 - b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
 - c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Instalar el complemento SnapCenter para IBM Db2

Agregar hosts e instalar paquetes de complementos en hosts remotos

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar los paquetes de complementos. Los complementos se instalan automáticamente en los hosts remotos. Puede agregar un host e instalar paquetes de complementos 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 complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
 - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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 esté ejecutándose.
- La documentación de administración contiene información sobre la gestión de hosts.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar la cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para IBM Db2"](#)

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host: • Ventanas • Linux  El complemento para IBM Db2 se instala en el host del cliente IBM Db2, y este host puede estar en un sistema Windows o en un sistema Linux.
Host name	Introduzca el nombre del host de comunicación. Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN.

Para este campo...	Haz esto...
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que proporcionó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección Seleccionar complementos para instalar, seleccione los complementos que desea instalar.

Al utilizar la API REST para instalar el complemento para Db2, debe pasar la versión como 3.0. Por ejemplo, Db2:3.0

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.

Para este campo...	Haz esto...
Ruta de instalación	El complemento para IBM Db2 se instala en el host del cliente IBM Db2, y este host puede estar en un sistema Windows o en un sistema Linux. • Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\ NetApp\ SnapCenter. Opcionalmente, puedes personalizar la ruta. • Para el paquete de complementos de SnapCenter para Linux, la ruta predeterminada es /opt/ NetApp/snapcenter. Opcionalmente, puedes personalizar la ruta.
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Para el host de Windows, seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento.  Proporcione el nombre gMSA en el siguiente formato: domainName\accountName\$.  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla "Omitir comprobaciones previas", se valida el host para verificar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell, la versión de .NET, la ubicación (para complementos de Windows) y Java 11 (para complementos de Windows y Linux) se validan según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Si el tipo de host es Linux, verifique la huella digital y luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

- Para el complemento de Windows, los registros de instalación y actualización se encuentran en: `C:\Windows\ SnapCenter plugin\Install<JOBID>\`
- Para el complemento 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 complemento basado en PERL existente para Db2 se desinstalará del servidor de complementos remoto.

Instalar paquetes de complementos de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de complementos de SnapCenter para Linux o Windows en varios hosts simultáneamente mediante el cmdlet de PowerShell `Install-SmHostPackage`.

Antes de empezar

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar el paquete de complemento.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet `Open-SmConnection` y luego ingrese sus credenciales.
3. Instale el complemento en varios hosts utilizando el cmdlet `Install-SmHostPackage` y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Puede utilizar la opción `-skipprecheck` cuando haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.

4. Introduzca sus credenciales para la instalación remota.

Instale el complemento SnapCenter para IBM Db2 en hosts Linux mediante la interfaz de línea de comandos

Debe instalar el complemento SnapCenter para IBM Db2 Database mediante la interfaz de usuario (UI) de SnapCenter . Si su entorno no permite la instalación remota del complemento desde la interfaz de usuario de SnapCenter , puede instalar el

complemento para IBM Db2 Database en modo de consola o en modo silencioso mediante la interfaz de línea de comandos (CLI).

Antes de empezar

- Debe instalar el complemento para la base de datos IBM Db2 en cada uno de los hosts Linux donde reside el cliente IBM Db2.
- El host Linux en el que está instalando el complemento SnapCenter para IBM Db2 Database debe cumplir con los requisitos de software, base de datos y sistema operativo dependientes.

La herramienta Matriz de Interoperabilidad (IMT) contiene la información más reciente sobre las configuraciones admitidas.

"Herramienta de matriz de interoperabilidad de NetApp"

- El complemento SnapCenter para IBM Db2 Database es parte del paquete de complementos SnapCenter para Linux. Antes de instalar el paquete de complementos de SnapCenter para Linux, ya debe haber instalado SnapCenter en un host 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 complementos de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\ NetApp\ SnapCenter\Package Repository al host donde desea instalar el complemento para IBM Db2.

Puede acceder a esta ruta desde el host donde está instalado SnapCenter Server.

2. Desde el símbolo del sistema, navegue hasta el directorio donde copió el archivo de instalación.
3. Instalar el complemento:

```
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 especifica el puerto de comunicación HTTPS de SMCore.
- -DSERVER_IP especifica la dirección IP del servidor SnapCenter .
- -DSERVER_HTTPS_PORT especifica el puerto HTTPS del servidor SnapCenter .
- -DUSER_INSTALL_DIR especifica el directorio donde desea instalar el paquete de complementos de SnapCenter para Linux.
- DINSTALL_LOG_NAME especifica 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 /<directorio de instalación>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y luego agregue el parámetro PLUGINS_ENABLED = DB2:3.0.

5. Agregue el host al servidor SnapCenter mediante el cmdlet Add-Smhost y los parámetros necesarios.

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 cmdlets del software SnapCenter"](#).

Supervisar el estado de la instalación del complemento para IBM Db2

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:

- a. Haga doble clic en el certificado.
- b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
- c. Desplácese por la lista de campos y haga clic en **Huella digital**.
- d. Copia los caracteres hexadecimales del cuadro.
- e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:

- a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado recientemente instalado por el nombre del sujeto.

```
Get-ChildItem -Path Certificado:\LocalMachine\Mi
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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 CA para el servicio de complementos IBM Db2 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 por 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. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave
privada en el almacén de claves a la misma contraseña utilizada para el
almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar 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 agregar 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 /opt/NetApp/snapcenter/scc/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 de alias en el certificado de CA es largo y contiene espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a un nombre simple:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure el nombre de 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 en el archivo `agent.properties` contra la clave `CRL_PATH`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Configurar el certificado CA para el servicio de complementos IBM Db2 de SnapCenter 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 por 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 correspondiente a la clave `KEYSTORE_PASS`.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool con su ruta completa.

```
C:\Archivos de programa\Java\<versión_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves:

```
keytool -keypasswd -alias "nombre_alias_en_certificado" -keystore keystore.jks
```

Actualice lo mismo para la clave `KEYSTORE_PASS` en el archivo `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:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe agregar 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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo *keystore.jks*.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 "nombre_de_alias_en_certificado_de_CA" -keystore keystore.jks
```

8. Configure el nombre de 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 para el certificado CA relacionado, consulte ["Cómo actualizar el archivo de lista de revocación de certificados en SnapCenter CA Certificate"](#) .
- 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 en el archivo *agent.properties* contra la clave `CRL_PATH`.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Prepárese para la protección de datos

Requisitos previos para utilizar el complemento SnapCenter para IBM Db2

Antes de utilizar el complemento SnapCenter para IBM Db2, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter Server.

- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento y creando credenciales, si corresponde.
- Instale Java 11 en su host Linux o Windows.

Debe configurar la ruta de Java en la variable de ruta ambiental de la máquina host.

- Configure SnapMirror y SnapVault si desea replicación de respaldo.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger IBM Db2

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de copia de seguridad, clonación y restauración que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser bases de datos IBM Db2 que usted respalda o clona con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

- Las políticas especifican la frecuencia de las copias de seguridad, la replicación, los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede seleccionar una política cuando realiza una copia de seguridad a pedido para un solo recurso.

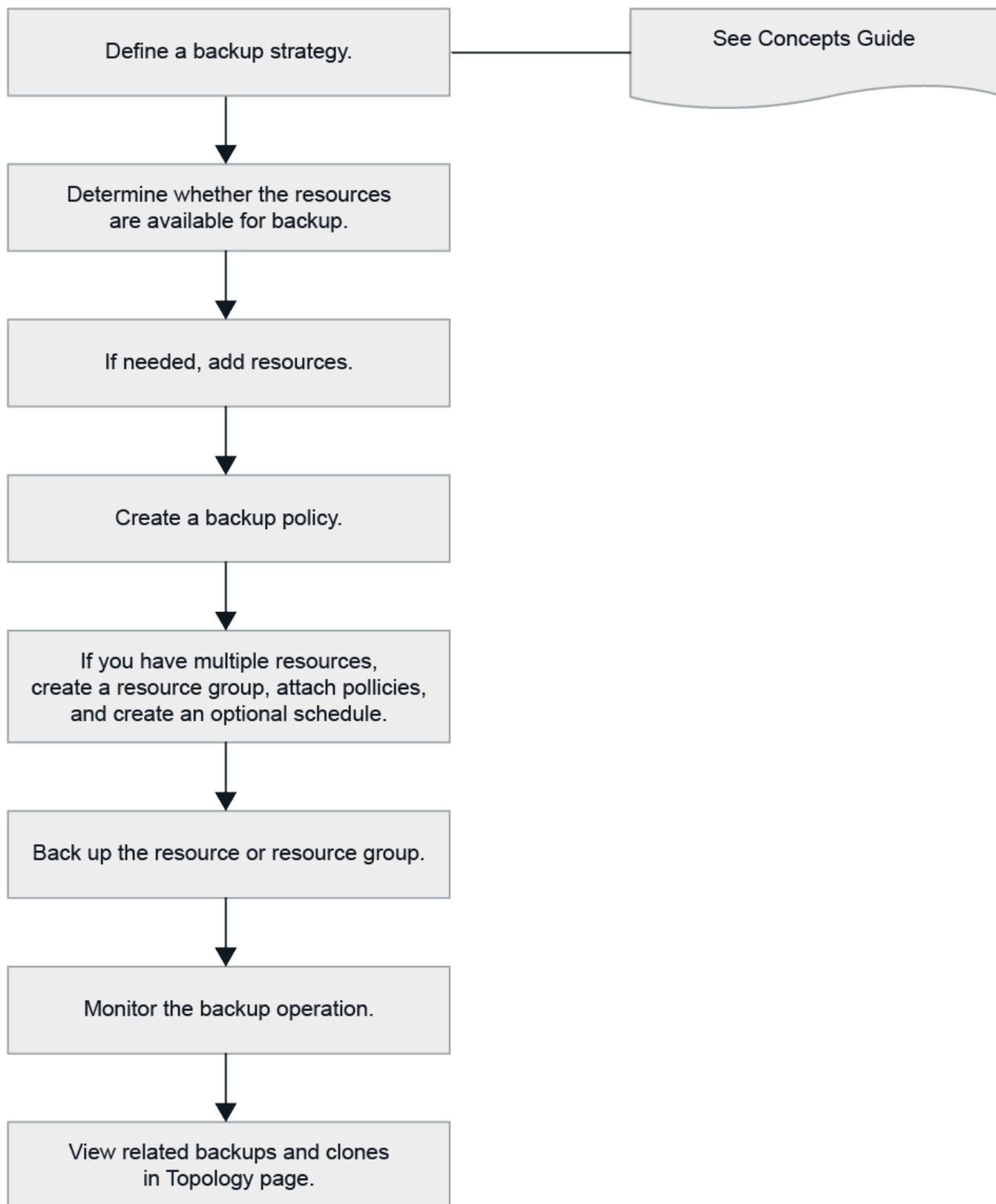
Piense en un grupo de recursos como si definiera lo que desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera cómo desea protegerla. Si está realizando una copia de seguridad de todas las bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos del host. Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Al crear el grupo de recursos y adjuntar las políticas, puede configurar el grupo de recursos para que realice una copia de seguridad completa diariamente.

Realizar copias de seguridad de los recursos de IBM Db2

Realizar copias de seguridad de los recursos de IBM Db2

Puede crear una copia de seguridad de un recurso (base de datos) o de un grupo de recursos. El flujo de trabajo de respaldo incluye la planificación, la identificación de las bases de datos para el respaldo, la administración de políticas de respaldo, la creación de grupos de recursos y la asociación de políticas, la creación de respaldos y el monitoreo de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen más información sobre los cmdlets de PowerShell. ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Descubra las bases de datos automáticamente

Los recursos son bases de datos IBM Db2 en el host Linux que son administradas por SnapCenter. Puede agregar recursos a grupos de recursos para realizar operaciones de protección de datos después de descubrir las bases de datos de IBM Db2 que están disponibles.

Antes de empezar

- Ya debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y configurar las conexiones del sistema de almacenamiento.
- El complemento SnapCenter para IBM Db2 no admite el descubrimiento automático de los recursos que residen en entornos virtuales RDM/VMDK. Debe proporcionar la información de almacenamiento para los entornos virtuales al agregar las bases de datos manualmente.

Acerca de esta tarea

- Después de instalar el complemento, todas las bases de datos de ese host Linux se descubren automáticamente y se muestran en la página Recursos.
- Sólo las bases de datos se descubren automáticamente.

Los recursos descubiertos automáticamente no se pueden modificar ni eliminar.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione el complemento para IBM Db2 de la lista.
2. En la página Recursos, seleccione el tipo de recurso de la lista Ver.
3. (Opcional) Haga clic en  * y luego seleccione el nombre del host.

Luego puedes hacer clic en  * para cerrar el panel de filtro.

4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

Los recursos se muestran junto con información como el tipo de recurso, el nombre del host, los grupos de recursos asociados, el tipo de copia de seguridad, las políticas y el estado general.

- Si la base de datos está en un almacenamiento NetApp y no está protegida, se muestra No protegido en la columna Estado general.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, y no se realiza ninguna operación de respaldo, se muestra Copia de seguridad no ejecutada en la columna Estado general. De lo contrario, el estado cambiará a Copia de seguridad fallida o Copia de seguridad exitosa según el último estado de la copia de seguridad.



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

Agregar recursos manualmente al host del complemento

El descubrimiento automático no es compatible con el host Windows. Debe agregar instancias de Db2 y recursos de base de datos manualmente.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y configurar conexiones del sistema de almacenamiento.

Acerca de esta tarea

El descubrimiento manual no es compatible con las siguientes configuraciones:

- Diseños RDM y VMDK

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el complemento SnapCenter para IBM Db2 en la lista desplegable.
2. En la página Recursos, haga clic en **Agregar recurso IBM DB2**.
3. En la página Proporcionar detalles de recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Especifique el nombre de la base de datos.
Nombre del host	Introduzca el nombre del host.
Tipo	Seleccione base de datos o instancia.
Instancia	Especifique el nombre de la instancia, que es la principal de la base de datos.
Cartas credenciales	Seleccione las credenciales o agregue información para las credenciales. Esto es opcional.

4. En la página Proporcionar espacio de almacenamiento, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees, y luego haga clic en **Guardar**.

Opcional: Puede hacer clic en el *  * Icono para agregar más volúmenes, LUN y qtrees de otros sistemas de almacenamiento.

5. Opcional: En la página Configuración de recursos, para los recursos en el host de Windows, ingrese pares clave-valor personalizados para el complemento de IBM Db2
6. Revise el resumen y luego haga clic en **Finalizar**.

Las bases de datos se muestran junto con información como el nombre del host, los grupos de recursos y políticas asociados y el estado general.

Si desea proporcionar a los usuarios acceso a los recursos, debe asignar los recursos a los usuarios. Esto permite a los usuarios realizar las acciones para las que tienen permiso en los activos que les están asignados.

["Agregar un usuario o grupo y asignarle roles y activos"](#)

Después de agregar las bases de datos, puede modificar los detalles de la base de datos de IBM Db2.

Crear políticas de copia de seguridad para IBM Db2

Antes de utilizar SnapCenter para realizar copias de seguridad de recursos de IBM Db2, debe crear una política de copia de seguridad para el recurso o grupo de recursos que desea respaldar. Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad.

Antes de empezar

- Debes haber definido tu estrategia de backup.

Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para bases de datos de IBM Db2.

- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, configurar conexiones del sistema de almacenamiento y agregar recursos.
- El administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino si está replicando instantáneas a un espejo o bóveda.

Además, puede especificar configuraciones de replicación, scripts y aplicaciones en la política. Estas opciones ahorran tiempo cuando desea reutilizar la política para otro grupo de recursos.

Acerca de esta tarea

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.
 - Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad de instantáneas mayor que la cantidad especificada 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.
5. En la página Tipo de política, 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 deba pasarse al complemento en formato clave-valor.

Puede proporcionar varios valores clave para pasarlos al complemento.

6. En la página Instantánea y replicación, realice las siguientes acciones.

- a. Especifique la frecuencia de programación seleccionando **A pedido**, **Cada hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero también le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

- a. En la sección Configuración de instantáneas, realice las siguientes acciones:

Si quieres...	Entonces...
Conservar una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 del Snaplock debe ser inferior a 100 años.



Para las copias de seguridad basadas en copias instantáneas, debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva 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 Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Esta opción debe estar habilitada para la sincronización activa de SnapMirror .
Actualizar SnapVault después de crear una copia de instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault).
Recuento de reintentos de error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

8. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados a una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.  El nombre del grupo de recursos no debe exceder los 250 caracteres.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desee utilizar para el nombre de la instantánea. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

Esto ayuda a filtrar la información en la pantalla.

- Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
- En la página Configuración de la aplicación, haga lo siguiente:

- Haga clic en la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación de instantánea del grupo de consistencia	Seleccione Urgente, Medio o Relajado para especificar el tiempo de espera para que se complete la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

+

1

2

3

4

5

6

Name

Resources

Application Settings

Policies

Notification

Summary

Backups

☒ Enable consistency group backup

Afford time to wait for Consistency Group Snapshot operation to complete

Urgent

Medium

Relaxed

☐ Disable WAFL Sync

Scripts

Custom Configurations

Snapshot Copy Tool

- Haga clic en la flecha **Scripts** e ingrese los comandos pre y post para las operaciones de inactividad, instantánea y activación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
- Haga clic en la flecha **Configuraciones personalizadas** e ingrese los pares clave-valor personalizados necesarios para todas las operaciones de protección de datos que utilicen este recurso.

Parámetro	Valor	Descripción
HABILITAR REGISTRO DE ARCHIVO	(T/N)	Permite que la gestión del registro de archivo elimine los registros de archivo.
RETENCIÓN DE REGISTRO DE ARCHIVO	número_de_días	Especifica el número de días que se conservan los registros de archivo. Esta configuración debe ser igual o mayor que NTAP_SNAPSHOT_RETENTIONS.
DIRECCIÓN DE REGISTRO DE ARCHIVO	directorio_de_información_de_cambio/registros	Especifica la ruta al directorio que contiene los registros de archivo.

Parámetro	Valor	Descripción
EXTRACCIÓN DEL REGISTRO DE ARCHIVO	extensión_de_archivo	Especifica la longitud de la extensión del archivo de registro de archivo. Por ejemplo, si el registro de archivo es log_backup_0_0_0_0.161518551942 9 y el valor de file_extension es 5, entonces la extensión del registro retendrá 5 dígitos, que es 16151.
ARCHIVO_REGISTRO_BÚSQUEDA_RECURSIVA ARCH	(T/N)	Permite la gestión de registros de archivo dentro de 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 complemento IBM Db2 Linux y no son compatibles con las bases de datos IBM Db2 registradas como un complemento centralizado de Windows.

- c. Haga clic en la flecha **Herramienta de copia de instantáneas** para seleccionar la herramienta para crear instantáneas:

Si quieres...	Entonces...
SnapCenter para utilizar el complemento para Windows y poner el sistema de archivos en un estado consistente antes de crear una instantánea. Para los recursos de Linux, esta opción no es aplicable.	Seleccione * SnapCenter con consistencia del sistema de archivos*.
SnapCenter para crear una instantánea de nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
Ingresa el comando que se ejecutará en el host para crear copias instantáneas.	Seleccione Otro y luego ingrese el comando que se ejecutará en el host para crear una instantánea.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

Las políticas se enumeran en la sección Configurar programaciones para políticas seleccionadas.

- b. En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna **Horarios aplicados**.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El servidor SMTP debe configurarse en **Configuración > Configuración global**.

9. Revise el resumen y luego haga clic en **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos de IBM Db2 en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más

adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:
 - a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:
 - a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
 - b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
 - c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para IBM Db2

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar copias de seguridad, restaurar o clonar bases de datos de IBM Db2.

Antes de empezar

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de datos única.

Pasos

1. Haga clic en **SnapCenterPS** para iniciar PowerShell Core.
2. Cree una nueva conexión al 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 nueva credencial mediante el cmdlet `Add-SmCredential`.

Este ejemplo muestra cómo crear una nueva credencial llamada FinanceAdmin con credenciales de Windows:

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux  
-AuthenticationType PasswordBased -Credential db2hostuser  
-EnableSudoPrivileges:$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 complemento 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. Establezca la ruta a SQLLIB.

Para Windows, el complemento Db2 utilizará la ruta predeterminada para la carpeta SQLLIB: "C:\Program Files\IBM\SQLLIB\BIN"

Si desea anular la ruta predeterminada, utilice el siguiente comando.

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<<custom_path>\IBM\SQLLIB\BIN"}
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de bases de datos Db2

Realizar una copia de seguridad de una base de datos incluye establecer una conexión con el servidor SnapCenter, agregar recursos, agregar una política, crear un grupo de recursos de copia de seguridad y realizar una copia de seguridad.

Antes de empezar

- Debes haber creado una política de respaldo.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".

- Para la operación de copia de seguridad basada en instantáneas, asegúrese de que todas las bases de datos de los inquilinos sean válidas y activas.
- Para los comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Seleccionar  y luego seleccione el nombre del host y el tipo de recurso para filtrar los recursos. Luego puedes seleccionar  para cerrar el panel de filtro.

3. Seleccione el recurso que desea respaldar.
4. En la página Recursos, seleccione **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Configuración de la aplicación, haga lo siguiente:
 - Seleccione la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia, si es necesario, y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación "Instantánea del grupo de consistencia"	Seleccione Urgente , Medio o Relajado para especificar el tiempo de espera para que finalice la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

- Seleccione la flecha **Scripts** para ejecutar comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo.

También puede ejecutar comandos previos antes de salir de la operación de copia de seguridad. Los prescriptos y posscripts se ejecutan en el servidor SnapCenter .

- Seleccione la flecha **Configuraciones personalizadas** y luego ingrese los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.
- Seleccione la flecha **Herramienta Copiar Instantánea** para seleccionar la herramienta para crear Instantáneas:

Si quieres...	Entonces...
SnapCenter para crear una instantánea a nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
SnapCenter para usar el complemento para Windows para poner el sistema de archivos en un estado consistente y luego crear una instantánea	Seleccione * SnapCenter con consistencia del sistema de archivos*.
Para ingresar el comando para crear una instantánea	Seleccione Otro y luego ingrese el comando para crear una instantánea.

6. En la página Políticas, realice los siguientes pasos:

- Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- Seleccionar *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.

policy_name es el nombre de la política que usted seleccionó.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en **Configuración > Configuración global**.

8. Revise el resumen y luego seleccione **Finalizar**.

Se muestra la página de topología de recursos.

9. Seleccione **Hacer copia de seguridad ahora**.

10. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

- En configuraciones de MetroCluster , es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

Para obtener información, consulte: ["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

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

Se muestra la solicitud de nombre de usuario y contraseña.

2. Agregue 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";"StorageSystem"="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";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Cree una política de respaldo mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
5. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

Este ejemplo muestra cómo realizar una copia de seguridad de un grupo de recursos:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

Este ejemplo realiza una copia de seguridad 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 una copia de seguridad de una base de datos Db2:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCD";"PluginName"="DB2"
} -Policy db2_policy
```

6. Supervise el estado del trabajo (en ejecución, completado o fallido) 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 respaldo, como la identificación y el nombre del respaldo, para realizar una operación de restauración o clonación 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de grupos de recursos

Un grupo de recursos es una colección de recursos en un host. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.

- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.

Acerca de esta tarea

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o seleccionando  , y luego seleccionando la etiqueta. Luego puedes seleccionar  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en bases de datos IBM Db2 en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 operaciones de copia de seguridad de IBM Db2

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las

operaciones de copia de seguridad.

- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	a. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. b. Seleccione la operación y luego haga clic en Cancelar trabajo.
Panel de actividades	a. Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Ver copias de seguridad y clones de IBM Db2 en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario.

Acerca de esta tarea

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento

secundario mediante la tecnología SnapVault .



La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página de topología del recurso seleccionado.

4. Revise la **tarjeta de resumen** para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario y secundario.

La sección **Tarjeta de resumen** muestra el número total de copias de seguridad basadas en instantáneas 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración de SnapLock más largo se recupera de ONTAP.

Después de realizar una copia de seguridad a pedido, al hacer clic en el botón **Actualizar** se actualizan los detalles de la copia de seguridad o la clonación.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

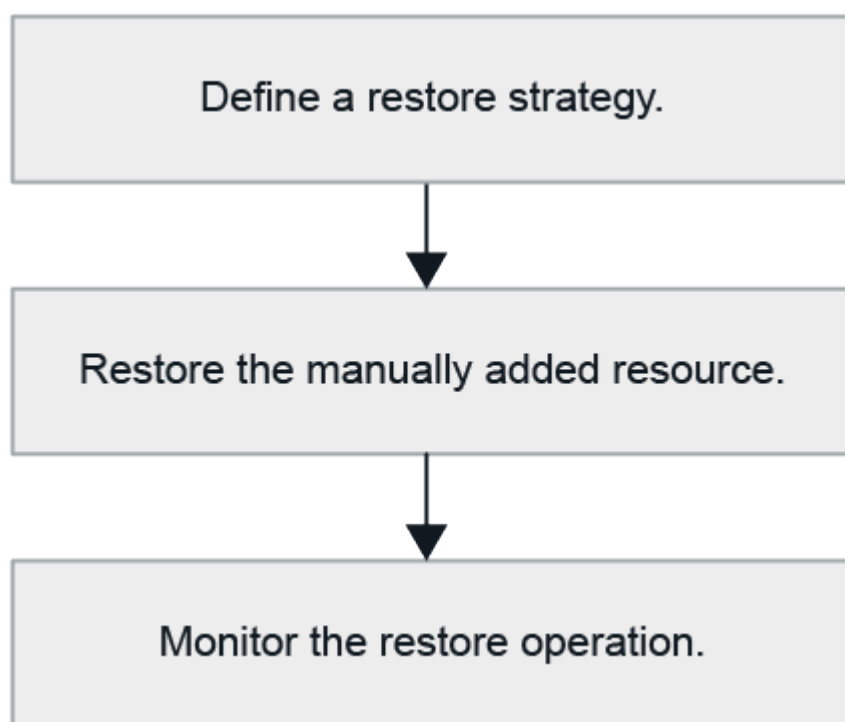
7. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en .
8. Si desea dividir un clon, seleccione el clon de la tabla y luego haga clic en .

Restaurar IBM Db2

Restaurar flujo de trabajo

El flujo de trabajo de restauración y recuperación incluye la planificación, la ejecución de las operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de restauración:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar una copia de seguridad de un recurso agregado manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.

- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



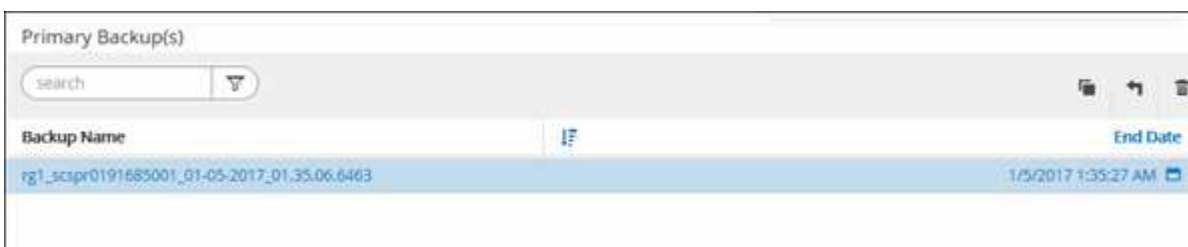
Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.



Primary Backup(s)	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01:35:06.6463	1/5/2017 1:35:27 AM

6. En la página Restaurar alcance, seleccione **Recurso completo**.
 - 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 instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Puede seleccionar varios LUN.



Si selecciona **Todos**, se restaurarán todos los archivos en los volúmenes, qtrees o LUN.

7. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.
8. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior

para ejecutarlos después de realizar un trabajo de restauración.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Después de terminar

La recuperación solo es posible si el estado de Rollforward está en estado "DB pendiente". Este estado es aplicable a bases de datos Db2 con registro de archivo habilitado.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

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

2. Identifique la copia de seguridad que desea restaurar mediante los cmdlets Get-SmBackup y Get-SmBackupReport.

Este ejemplo muestra que hay dos copias de seguridad disponibles para la restauración:

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.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
```

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.



AppObjectId es "Host\Plugin\UID", donde UID = <instance_name> es para el recurso de instancia DB2 descubierto manualmente y UID = <instance_name>\<database_name> es para el recurso de base de datos IBM Db2. Puede obtener el ResourceID desde el cmdlet Get-smResources.

```
Get-smResources -HostName cn24.sscore.test.com -PluginCode DB2
```

Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento principal:

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.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.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>"; "Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"})
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar y recuperar una copia de seguridad de una base de datos descubierta automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Para los recursos descubiertos automáticamente, la restauración es compatible 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 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. En la página Restaurar ámbito, seleccione **Recurso completo** para restaurar los volúmenes de datos configurados de la base de datos IBM Db2.
7. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no son necesarios para los recursos descubiertos automáticamente.

8. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no son necesarios para los recursos descubiertos automáticamente.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Después de terminar

La recuperación solo es posible si el estado de Rollforward está en estado "DB pendiente". Este estado es aplicable a bases de datos Db2 con registro de archivo habilitado.

Supervisar las operaciones de restauración de IBM Db2

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Clonar copias de seguridad de recursos de IBM Db2

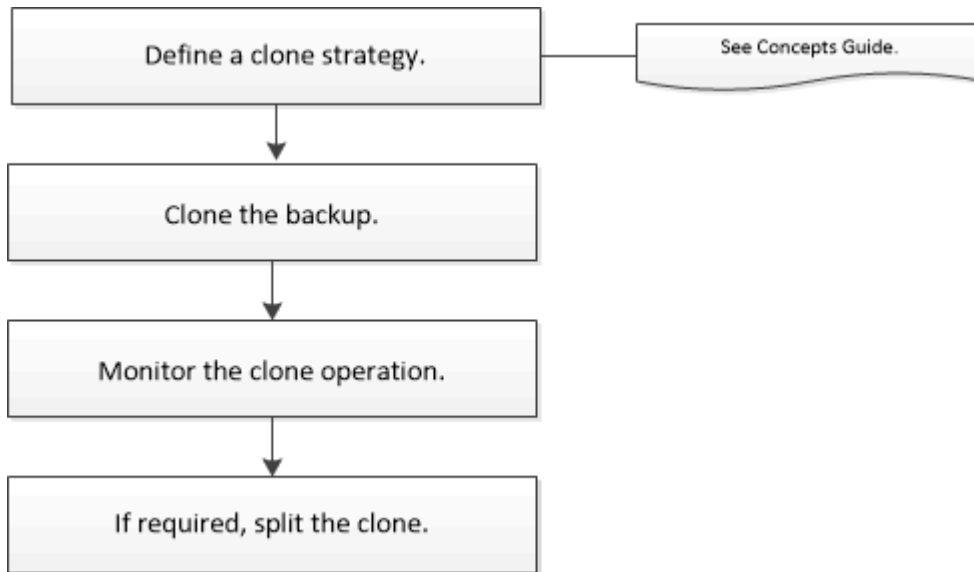
Flujo de trabajo de clonación

El flujo de trabajo de clonación incluye la realización de la operación de clonación y la supervisión de la operación.

Acerca de esta tarea

- Puede clonar en el servidor IBM Db2 de origen.
- Puede clonar copias de seguridad de recursos por los siguientes motivos:
 - Para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de recursos actuales durante los ciclos de desarrollo de aplicaciones
 - Para herramientas de extracción y manipulación de datos al rellenar almacenes de datos
 - Para recuperar datos que fueron borrados o modificados por error

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de clonación:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

Después de terminar

Después de clonar los recursos de Db2 descubiertos automáticamente, el recurso clonado se marca como recurso manual. Haga clic en **Actualizar recursos** para recuperar el recurso Db2 clonado. Cuando eliminas el clon, el almacenamiento y el host también se limpian.

Si no actualiza los recursos después de la operación de clonación e intenta eliminar el clon, el almacenamiento y el host no se limpiarán. Debes eliminar las entradas manualmente en fstab.

Clonar una copia de seguridad de IBM Db2

Puede utilizar SnapCenter para clonar una copia de seguridad. Puede clonar desde una copia de seguridad primaria o secundaria.

Antes de empezar

- Deberías haber realizado una copia de seguridad de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados que alojan los volúmenes estén 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 que sea la misma que la ruta de montaje original en el otro host. La ruta de montaje

debe tener permiso de ejecución 755.

- Para los comandos previos o posteriores a la clonación, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["Dividir un volumen FlexClone de su volumen principal"] .
- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con información como el tipo, el host, los grupos de recursos y políticas asociados y el estado.

3. Seleccione el recurso o grupo de recursos.

Debe seleccionar un recurso si selecciona un grupo de recursos.

Se muestra la página de topología de recursos o grupos de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).

5. Seleccione la copia de seguridad de datos de la tabla y luego haga clic en  .

6. En la página Ubicación, realice las siguientes acciones:

Para este campo...	Haz esto...
Servidor clonado	Seleccione un host en el que se debe crear el clon.
Instancia de clonación de destino	Introduzca el ID de la instancia de clonación de Db2 de destino para clonar desde las copias de seguridad existentes. Esto solo se aplica a recursos de tipo de almacenamiento ANF.
Nombre del clon de destino	Introduzca el nombre del clon. Esto solo se aplica al recurso de base de datos Db2.
Dirección IP de exportación de NFS	Introduzca las direcciones IP o los nombres de host a los que se exportarán los volúmenes clonados. Esto solo se aplica a recursos de tipo de almacenamiento NFS.
Capacidad de almacenamiento máxima (MiB/s)	Introduzca el rendimiento máximo de un grupo de capacidad.

7. En la página Scripts, realice los siguientes pasos:



Los scripts se ejecutan en el host del complemento.

- a. Introduzca los comandos para pre-clonar o post-clonar que deben ejecutarse antes o después de la operación de clonación, respectivamente.
 - Comando de preclonación: eliminar bases de datos existentes con el mismo nombre
 - Comando posterior a la clonación: verificar una base de datos o iniciar una base de datos.
- b. Introduzca el comando de montaje para montar un sistema de archivos en un host.

Comando de montaje para un volumen o qtree en una máquina Linux:

Ejemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

9. Revise el resumen y luego haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Después de terminar

Después de clonar los recursos de Db2 descubiertos automáticamente, el recurso clonado se marca como recurso manual. Haga clic en **Actualizar recursos** para recuperar el recurso Db2 clonado. Cuando eliminas el clon, el almacenamiento y el host también se limpian.

Si no actualiza los recursos después de la operación de clonación e intenta eliminar el clon, el almacenamiento y el host no se limpiarán. Debes eliminar las entradas manualmente en fstab.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Enumere las copias de seguridad que se pueden clonar mediante el cmdlet `Get-SmBackup` o `Get-SmResourceGroup`.

Este ejemplo muestra información sobre todas las copias de seguridad 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	

Este ejemplo muestra información sobre un grupo de recursos específico, sus recursos y 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
SchedulersSQLInstance :
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 clonación desde una copia de seguridad existente utilizando el cmdlet New-SmClone.

Este ejemplo crea un clon a partir de una copia de seguridad especificada 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

```

Este ejemplo crea un clon de una instancia específica 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. Vea el estado del trabajo de clonación mediante el cmdlet Get-SmCloneReport.

Este ejemplo muestra un informe clonado para el ID de trabajo especificado:

```
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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar las operaciones de clones de IBM Db2

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte ["Dividir un volumen FlexClone de su volumen principal"](#) .
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCORE. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCORE sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Eliminar o dividir clones de bases de datos de IBM Db2 después de actualizar SnapCenter

Después de actualizar a SnapCenter 4.3, ya no verá los clones. Puede eliminar el clon o dividir los clones desde la página Topología del recurso desde el cual se crearon los clones.

Acerca de esta tarea

Si desea localizar la huella de almacenamiento de los clones ocultos, ejecute el siguiente comando: `Get-SmClone -ListStorageFootprint`

Pasos

1. Elimine las copias de seguridad de los recursos clonados mediante el cmdlet `remove-smbbackup`.
2. Elimine el grupo de recursos de los recursos clonados mediante el cmdlet `remove-smresourcegroup`.
3. Elimine la protección del recurso clonado mediante el cmdlet `remove-smprotectresource`.
4. Seleccione el recurso principal en la página Recursos.

Se muestra la página de topología de recursos.

5. Desde la vista Administrar copias, seleccione los clones de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).
6. Seleccione los clones y luego haga clic  Para eliminar clones o hacer clic  Para dividir los clones.

7. Haga clic en **Aceptar**.

Proteger PostgreSQL

Complemento de SnapCenter para PostgreSQL

Descripción general del complemento de SnapCenter para PostgreSQL

El complemento SnapCenter para el clúster PostgreSQL es un componente del lado del host del SnapCenter software de NetApp que permite la gestión de protección de datos consciente de la aplicación de los clústeres PostgreSQL. El complemento para el clúster PostgreSQL automatiza la copia de seguridad, la restauración y la clonación de clústeres PostgreSQL en su entorno de SnapCenter .

SnapCenter admite configuraciones de PostgreSQL de un solo clúster y de varios clústeres. Puede utilizar el complemento para clústeres PostgreSQL en entornos Linux y Windows. En entornos Windows, PostgreSQL se admitirá como recurso manual.

Cuando se instala el complemento para el clúster PostgreSQL, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen. También puede utilizar el complemento con la tecnología NetApp SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de los estándares.

El complemento SnapCenter para PostgreSQL admite diseños de almacenamiento de archivos NFS y SAN en ONTAP y Azure NetApp .

Se admite el diseño de almacenamiento virtual VMDK, vVol y RDM.

Qué puede hacer utilizando el complemento SnapCenter para PostgreSQL

Cuando instala el complemento para el clúster PostgreSQL en su entorno, puede usar SnapCenter para realizar copias de seguridad, restaurar y clonar clústeres PostgreSQL y sus recursos. También puede realizar tareas de apoyo a dichas operaciones.

- Añadir clústeres.
- Crear copias de seguridad.
- Restaurar desde copias de seguridad.
- Copias de seguridad clonadas.
- Programar operaciones de respaldo.
- Supervisar operaciones de copia de seguridad, restauración y clonación.
- Ver informes de operaciones de copia de seguridad, restauración y clonación.

Funciones del complemento SnapCenter para PostgreSQL

SnapCenter se integra con la aplicación complementaria y con las tecnologías NetApp en el sistema de almacenamiento. Para trabajar con el complemento para el clúster PostgreSQL, utilice la interfaz gráfica de usuario de SnapCenter .

- Interfaz gráfica de usuario unificada

La interfaz de SnapCenter proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite realizar operaciones consistentes de copia de seguridad, restauración y clonación en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y supervisar trabajos en todos los complementos.

- **Administración central automatizada**

Puede programar operaciones de respaldo, configurar la retención de respaldo basada en políticas y realizar operaciones de restauración. También puede supervisar su entorno de forma proactiva configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología de copia de instantáneas de NetApp sin interrupciones**

SnapCenter utiliza la tecnología de instantáneas de NetApp con el complemento para clúster PostgreSQL para realizar copias de seguridad de los recursos.

El uso del complemento para PostgreSQL también ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de copia de seguridad, restauración y clonación
- Seguridad respaldada por RBAC y delegación de roles centralizada

También puede configurar las credenciales para que los usuarios autorizados de SnapCenter tengan permisos a nivel de aplicación.

- Creación de copias puntuales y con uso eficiente del espacio de recursos para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

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

- Compatibilidad con la función de instantánea del grupo de consistencia (CG) de ONTAP como parte de la creación de copias de seguridad.
- Capacidad de ejecutar múltiples copias de seguridad simultáneamente en múltiples hosts de recursos

En una sola operación, las instantáneas se consolidan cuando los recursos de un solo host comparten el mismo volumen.

- Capacidad de crear instantáneas mediante comandos externos.
- Soporte para Linux LVM en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el complemento SnapCenter para PostgreSQL

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas físicas como en máquinas virtuales (VM). Debe verificar la compatibilidad con su tipo de almacenamiento antes de instalar el complemento SnapCenter para PostgreSQL.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • Volúmenes conectados a NFS
VMware ESXi	• El escaneo de los adaptadores de bus de host (HBA) puede demorar mucho tiempo en completarse porque SnapCenter escanea todos los adaptadores de bus de host presentes en el host. Puede editar el archivo LinuxConfig.pm ubicado en <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> para establecer el valor del parámetro SCSI_HOSTS_OPTIMIZED_RESCAN en 1 para volver a escanear solo los HBA que figuran en HBA_DRIVER_NAMES. • LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS • Volúmenes NFS conectados directamente al sistema invitado • Almacenes de datos vVol tanto en NFS como en SAN El almacén de datos vVol solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP necesarios para el complemento PostgreSQL

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo
 - lun crear
 - lun crear
 - lun crear

- eliminar lun
- agregar igroup lun
- crear igroup lun
- eliminar igroup lun
- Cambiar nombre de igroup lun
- Cambiar nombre de igroup lun
- Programa de igroup de Lun
- Asignación de LUN a nodos de informes adicionales
- creación de mapeo LUN
- eliminar mapeo lun
- Mapeo de LUN: eliminar nodos de informes
- espectáculo de mapeo de lun
- modificar lun
- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- lun reserva persistente clara
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen

- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- tiempo de caducidad de modificación de instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFs de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIF de vserver
- Mostrar copia de sombra de CIF de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi
- Mostrar conexión iscsi de vserver
- espectáculo vserver
- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red

- Mostrar interfaz de red
- vserver

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para PostgreSQL

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Estrategia de respaldo para PostgreSQL

Definir una estrategia de respaldo para PostgreSQL

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a tener los respaldos que necesita para restaurar o clonar sus recursos con éxito. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Acerca de esta tarea

Un SLA define el nivel de servicio que se espera y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. RPO define la estrategia para la edad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA, RTO y RPO contribuyen a la estrategia de protección de datos.

Pasos

1. Determina cuándo debes realizar copias de seguridad de tus recursos.
2. Decide cuántos trabajos de respaldo necesitas.
3. Decide cómo nombrar tus copias de seguridad.
4. Decida si desea crear una política basada en copias de instantáneas para realizar copias de seguridad de instantáneas consistentes con la aplicación del clúster.
5. Decida si desea utilizar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
6. Determine el período de retención de las instantáneas en el sistema de almacenamiento de origen y el destino SnapMirror .
7. Determine si desea ejecutar algún comando antes o después de la operación de copia de seguridad y proporcione un script previo o posterior.

Descubrimiento automático 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 complemento SnapCenter Plug-in para PostgreSQL, los clústeres PostgreSQL de todas las instancias en ese host Linux se detectan automáticamente y se muestran en la página Recursos.

Tipo de backups admitido

El tipo de copia de seguridad especifica el tipo de copia de seguridad que desea crear. SnapCenter admite el tipo de copia de seguridad basada en instantáneas para clústeres PostgreSQL.

Copia de seguridad basada en instantáneas

Las copias de seguridad basadas en instantáneas aprovechan la tecnología de instantáneas de NetApp para crear copias en línea, de solo lectura, de los volúmenes en los que residen los clústeres PostgreSQL.

Cómo el complemento SnapCenter para PostgreSQL utiliza instantáneas de grupos de consistencia

Puede utilizar el complemento para crear instantáneas de grupos de consistencia para grupos de recursos. Un grupo de consistencia es un contenedor que puede albergar múltiples volúmenes para que puedas administrarlos como una sola entidad. Un grupo de consistencia son instantáneas simultáneas de múltiples volúmenes que proporcionan copias consistentes de un grupo de volúmenes.

También puede especificar el tiempo de espera para que el controlador de almacenamiento agrupe las instantáneas de manera consistente. Las opciones de tiempo de espera disponibles son **Urgente**, **Medio** y **Relajado**. También puede habilitar o deshabilitar la sincronización del diseño de archivo Write Anywhere (WAFL) durante la operación de instantánea de grupo consistente. La sincronización de WAFL mejora el rendimiento de una instantánea de grupo de consistencia.

Cómo gestiona SnapCenter el mantenimiento de las copias de seguridad de datos

SnapCenter administra el mantenimiento de las copias de seguridad de datos en los niveles del sistema de almacenamiento y del sistema de archivos.

Las instantáneas del almacenamiento primario o secundario y sus entradas correspondientes en el catálogo de PostgreSQL se eliminan según la configuración de retención.

Consideraciones para determinar los cronogramas de copias de seguridad para PostgreSQL

El factor más crítico para determinar un cronograma de respaldo es la tasa de cambio del recurso. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su acuerdo de nivel de servicio (SLA) y su objetivo de punto de recuperación (RPO).

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de copia de seguridad (con qué frecuencia se deben realizar las copias de seguridad)

La frecuencia de copia de seguridad, también llamada tipo de programación para algunos complementos, es parte de una configuración de política. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual.

- Programaciones de copias de seguridad (cuándo exactamente se realizarán las copias de seguridad)

Las programaciones de copias de seguridad son parte de la configuración de un recurso o de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m.

Número de trabajos de respaldo necesarios para PostgreSQL

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño del recurso, la cantidad de volúmenes utilizados, la tasa de cambio del recurso y su Acuerdo de Nivel de Servicio (SLA).

Convenciones de nomenclatura de copias de seguridad para complementos de clústeres de PostgreSQL

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

```
resourcegroupname_hostname_timestamp
```

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.
- *03-12-2015_23.17.26* es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, *customtext_resourcegroup_policy_hostname* o *resourcegroup_hostname*. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Estrategia de restauración y recuperación para PostgreSQL

Definir una estrategia de restauración y recuperación para los recursos de PostgreSQL

Debe definir una estrategia antes de restaurar y recuperar su clúster para poder realizar operaciones de restauración y recuperación con éxito.



Sólo se admite la recuperación manual del clúster.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos de PostgreSQL agregados manualmente
2. Determinar las estrategias de restauración compatibles con los clústeres de PostgreSQL detectados automáticamente
3. Decide el tipo de operaciones de recuperación que deseas realizar.

Tipos de estrategias de restauración compatibles con recursos de PostgreSQL agregados manualmente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter.



No es posible recuperar recursos de PostgreSQL agregados manualmente.

Restauración completa de recursos

- Restaura todos los volúmenes, qtrees y LUN de un recurso



Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

NOTA: El complemento para PostgreSQL crea una etiqueta de respaldo y un mapa de espacio de tabla en la carpeta `</OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/` para ayudar a realizar la recuperación manual.

Tipo de estrategia de restauración compatible con PostgreSQL detectado automáticamente

Debe definir una estrategia antes de poder realizar con éxito operaciones de

restauración mediante SnapCenter.

La restauración completa de recursos es la estrategia de restauración compatible con los clústeres PostgreSQL descubiertos automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para PostgreSQL detectado automáticamente

El complemento SnapCenter para PostgreSQL admite SnapRestore de archivo único y tipos de restauración de conexión y copia para clústeres PostgreSQL detectados automáticamente.

SnapRestore de archivo único se realiza en entornos NFS para los siguientes escenarios:

- Si solo se selecciona la opción **Recurso completo**
- Cuando la copia de seguridad seleccionada es de una ubicación secundaria de SnapMirror o SnapVault y está seleccionada la opción **Recurso completo**

SnapRestore de archivo único se realiza en entornos SAN para los siguientes escenarios:

- Si solo se selecciona la opción **Recurso completo**
- Cuando se selecciona la copia de seguridad desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Recurso completo**

Tipos de operaciones de recuperación compatibles con clústeres de PostgreSQL

SnapCenter le permite realizar diferentes tipos de operaciones de recuperación para clústeres PostgreSQL.

- Recuperar el clúster hasta el estado más reciente
- Recuperar el clúster hasta un punto específico en el tiempo

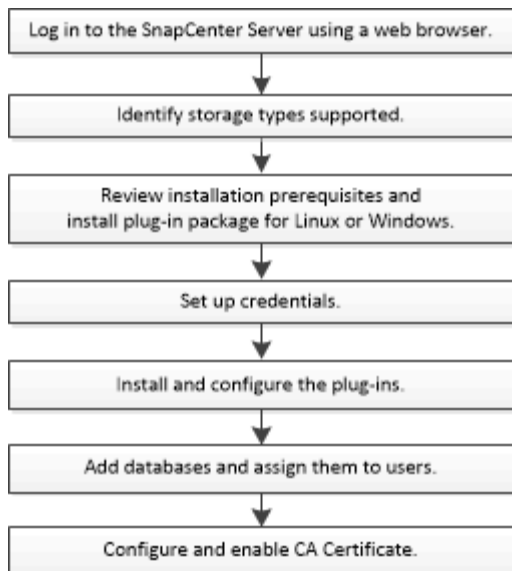
Debe especificar la fecha y hora para la recuperación.

SnapCenter también proporciona la opción Sin recuperación para clústeres PostgreSQL.

Prepárese para instalar el complemento SnapCenter para PostgreSQL

Flujo de trabajo de instalación del complemento SnapCenter para PostgreSQL

Debe instalar y configurar el complemento SnapCenter para PostgreSQL si desea proteger los clústeres de PostgreSQL.



Requisitos previos para agregar hosts e instalar el complemento SnapCenter para PostgreSQL

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos. El complemento SnapCenter para PostgreSQL está disponible en entornos Windows y Linux.

- Debes tener instalado Java 11 en tu host.



IBM Java no es compatible con hosts Windows y Linux.

- Para Windows, el servicio de creación de complementos debe ejecutarse utilizando el usuario de Windows "LocalSystem", que es el comportamiento predeterminado cuando el complemento para PostgreSQL se instala como administrador de dominio.
- Al instalar un complemento 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 complemento SnapCenter para Microsoft Windows se implementará de forma predeterminada con el complemento PostgreSQL en los hosts de Windows.
- El servidor SnapCenter debe tener acceso al puerto 8145 o personalizado del host del complemento para PostgreSQL.

Hosts de Windows

- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Al instalar el complemento para PostgreSQL en un host Windows, el complemento de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Windows.

["Descargar JAVA para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Hosts Linux

- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Linux.

["Descargar JAVA para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Para los clústeres PostgreSQL que se ejecutan en un host Linux, al instalar el complemento para PostgreSQL, el complemento de SnapCenter para UNIX se instala automáticamente.
- Debe tener **bash** como el shell predeterminado para la instalación del complemento.

Comandos suplementarios

Para ejecutar un comando complementario en el complemento 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 complementarios en el host del complemento, abra el archivo *allowed_commands.config* en un editor. Ingrese cada comando en una línea separada y los comandos no distinguen entre mayúsculas y minúsculas. Asegúrese de especificar la ruta de acceso completa y de encerrarla entre comillas (") si contiene espacios.

Por ejemplo:

comando: mount comando: umount comando: "C:\Archivos de programa\ NetApp\ SnapCreator commands\ sdccli.exe" comando: myscript.bat

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.



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

Configurar privilegios de sudo para usuarios no root para el host Linux

SnapCenter permite que un usuario no root instale el paquete de complementos de SnapCenter para Linux e inicie el proceso de instalación del complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el permiso 555. De lo contrario, la instalación del complemento podría fallar.
- Para el usuario no root, asegúrese de que el nombre del usuario no root y el grupo del usuario sean los mismos.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- `/inicio/USUARIO_LINUX/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl`

Pasos

1. Inicie sesión en el host Linux en el que desea instalar el paquete de complementos de SnapCenter para Linux.
2. Agregue las siguientes líneas al archivo `/etc/sudoers` utilizando la utilidad visudo para 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/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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` _ si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	Requisitos
Sistemas operativos	Microsoft Windows Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp".

Artículo	Requisitos
RAM mínima para el complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux

Antes de instalar el paquete de complementos de SnapCenter para Linux, debe familiarizarse con algunos requisitos básicos de tamaño y espacio del sistema host.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Servidor empresarial SUSE Linux (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .
RAM mínima para el complemento SnapCenter en el host	1 GB

Artículo	Requisitos
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 Oracle Java y OpenJDK Si ha actualizado JAVA a la última versión, 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 correcta. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Configurar credenciales para el complemento SnapCenter para PostgreSQL

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en clústeres o sistemas de archivos de Windows.

Acerca de esta tarea

- Hosts Linux

Debe configurar credenciales para instalar complementos en hosts Linux.

Debe configurar las credenciales para el usuario root o para un usuario no root que tenga privilegios de sudo para instalar e iniciar el proceso del complemento.

Mejor práctica: Si bien se le permite crear credenciales para Linux después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

- Hosts de Windows

Debe configurar las credenciales de Windows antes de instalar complementos.

Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador en

el host remoto.

Si configura 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 de respaldo al nombre de usuario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, especifique la información necesaria para configurar las credenciales:

Para este campo...	Haz esto...
Nombre de la 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 del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: ◦ <i>NetBIOS\Nombre de usuario</i> ◦ <i>Dominio FQDN\Nombre de usuario</i> • 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>NombreDeUsuario</i> No utilice comillas dobles (") ni tildes invertidas (') en las contraseñas. No debe utilizar los símbolos menor que (<) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que<!10, menos que10<!, acento grave`12.

Para este campo...	Haz esto...
Password	Introduzca la contraseña utilizada para la autenticación.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar.
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no sea root.  Aplicable únicamente a usuarios de Linux.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Configurar gMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -Effectivelmmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```

domainName\accountName$
.. Añade objetos de computadora 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,...>
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de
servicio.
```

4. Configure el gMSA en sus hosts:

- a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
 - b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
 - c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Instalar el complemento SnapCenter para PostgreSQL

Agregar hosts e instalar paquetes de complementos en hosts remotos

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar los paquetes de complementos. Los complementos se instalan automáticamente en los hosts remotos. Puede agregar el host e instalar paquetes de complementos 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 complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
 - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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 esté ejecutándose.
- La documentación de administración contiene información sobre la gestión de hosts.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar una cuenta de servicio administrada grupal en Windows Server 2016 o posterior para PostgreSQL"](#)

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host: Ventanas Linux El complemento para PostgreSQL se instala en el host del cliente PostgreSQL, y este host puede estar en un sistema Windows o en un sistema Linux.

Para este campo...	Haz esto...
Host name	Introduzca el nombre del host de comunicación. Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN.
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que proporcionó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea instalar.

Al utilizar la API REST para instalar el complemento para PostgreSQL, debe pasar la versión como 3.0. Por ejemplo, PostgreSQL:3.0

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.

Para este campo...	Haz esto...
Ruta de instalación	El complemento para PostgreSQL se instala en el host del cliente PostgreSQL, y este host puede estar en un sistema Windows o en un sistema Linux. • Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\ NetApp\ SnapCenter. Opcionalmente, puedes personalizar la ruta. • Para el paquete de complementos de SnapCenter para Linux, la ruta predeterminada es /opt/ NetApp/snapcenter. Opcionalmente, puedes personalizar la ruta.
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Agregar todos los hosts en el clúster	Seleccione esta casilla de verificación para agregar todos los nodos del clúster.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Para el host de Windows, seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento.  Proporcione el nombre gMSA en el siguiente formato: domainName\accountName\$.  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla "Omitir comprobaciones previas", se valida el host para verificar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell, la versión de .NET, la ubicación (para complementos de Windows) y la versión de Java (para complementos de Linux) se validan según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Si el tipo de host es Linux, verifique la huella digital y luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

- Para el complemento de Windows, los registros de instalación y actualización se encuentran en:
`C:\Windows\ SnapCenter plugin\Install<JOBID>\_`
- Para el complemento 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_`

Instalar paquetes de complementos de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de complementos de SnapCenter para Linux o Windows en varios hosts simultáneamente mediante el cmdlet de PowerShell `Install-SmHostPackage`.

Antes de empezar

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar el paquete de complemento.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet `Open-SmConnection` y luego ingrese sus credenciales.
3. Instale el complemento en varios hosts utilizando el cmdlet `Install-SmHostPackage` y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Puede utilizar la opción `-skipprecheck` cuando haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.

4. Introduzca sus credenciales para la instalación remota.

Instale el complemento SnapCenter para PostgreSQL en hosts Linux mediante la interfaz de línea de comandos

Debe instalar el complemento SnapCenter para el clúster PostgreSQL mediante la interfaz de usuario (UI) de SnapCenter . Si su entorno no permite la instalación remota del complemento desde la interfaz de usuario de SnapCenter , puede instalar el

complemento para el clúster PostgreSQL en modo consola o en modo silencioso mediante la interfaz de línea de comandos (CLI).

Antes de empezar

- Debe instalar el complemento para el clúster PostgreSQL en cada uno de los hosts Linux donde reside el cliente PostgreSQL.
- El host Linux en el que está instalando el complemento SnapCenter para el clúster PostgreSQL debe cumplir con los requisitos de software, clúster y sistema operativo dependientes.

La herramienta Matriz de Interoperabilidad (IMT) contiene la información más reciente sobre las configuraciones admitidas.

"Herramienta de matriz de interoperabilidad de NetApp"

- El complemento SnapCenter para el clúster PostgreSQL es parte del paquete de complementos SnapCenter para Linux. Antes de instalar el paquete de complementos de SnapCenter para Linux, ya debe haber instalado SnapCenter en un host Windows.

Pasos

1. Copie el archivo de instalación del paquete de complementos de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\ SnapCenter\Package Repository al host donde desea instalar el complemento para PostgreSQL.

Puede acceder a esta ruta desde el host donde está instalado SnapCenter Server.

2. Desde el símbolo del sistema, navegue hasta el directorio donde copió el archivo de instalación.

3. Instalar el complemento:

```
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 especifica el puerto de comunicación HTTPS de SMCore.
- -DSERVER_IP especifica la dirección IP del servidor SnapCenter .
- -DSERVER_HTTPS_PORT especifica el puerto HTTPS del servidor SnapCenter .
- -DUSER_INSTALL_DIR especifica el directorio donde desea instalar el paquete de complementos de SnapCenter para Linux.
- DINSTALL_LOG_NAME especifica 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 /<directorio de instalación>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y luego agregue el parámetro PLUGINS_ENABLED = PostgreSQL:3.0.
5. Agregue el host al servidor SnapCenter mediante el cmdlet Add-Smhost y los parámetros necesarios.

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 cmdlets del software SnapCenter"](#).

Supervisar el estado de instalación del complemento para PostgreSQL

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Huella digital**.
 - d. Copia los caracteres hexadecimales del cuadro.
 - e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

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

Get-ChildItem -Path Certificado:\LocalMachine\Mi

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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 CA para el servicio de complementos 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 por 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. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave
privada en el almacén de claves a la misma contraseña utilizada para el
almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar 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 agregar 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 /opt/NetApp/snapcenter/scc/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se

agregó al almacén de claves.

7. Cambie la contraseña de clave privada agregada 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 de alias en el certificado de CA es largo y contiene espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a un nombre simple:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure el nombre de 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 en el archivo `agent.properties` contra la clave `CRL_PATH`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Configurar el certificado de CA para el servicio de complementos de SnapCenter PostgreSQL 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 por 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 correspondiente a la clave *KEYSTORE_PASS*.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool con su ruta completa.

```
C:\Archivos de programa\Java\<versión_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves:

```
keytool -keypasswd -alias "nombre_alias_en_certificado" -keystore keystore.jks
```

Actualice lo mismo para la clave *KEYSTORE_PASS* en el archivo *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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe agregar 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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo *keystore.jks*.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 "nombre_de_alias_en_certificado_de_CA" -keystore keystore.jks
```

8. Configure el nombre de 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 para el certificado CA relacionado, consulte ["Cómo actualizar el archivo de lista de revocación de certificados en SnapCenter CA Certificate"](#) .
- 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 en el archivo *agent.properties* contra la clave `CRL_PATH`.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Prepárese para la protección de datos

Requisitos previos para utilizar el complemento SnapCenter para PostgreSQL

Antes de utilizar el complemento SnapCenter para PostgreSQL, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter Server.

- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento y creando credenciales, si corresponde.
- Instale Java 11 en su host Linux o Windows.

Debe configurar la ruta de Java en la variable de ruta ambiental de la máquina host.

- Configure SnapMirror y SnapVault si desea replicación de respaldo.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger PostgreSQL

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de copia de seguridad, clonación y restauración que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser clústeres PostgreSQL que usted respalda o clona con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

- Las políticas especifican la frecuencia de las copias de seguridad, la replicación, los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede seleccionar una política cuando realiza una copia de seguridad a pedido para un solo recurso.

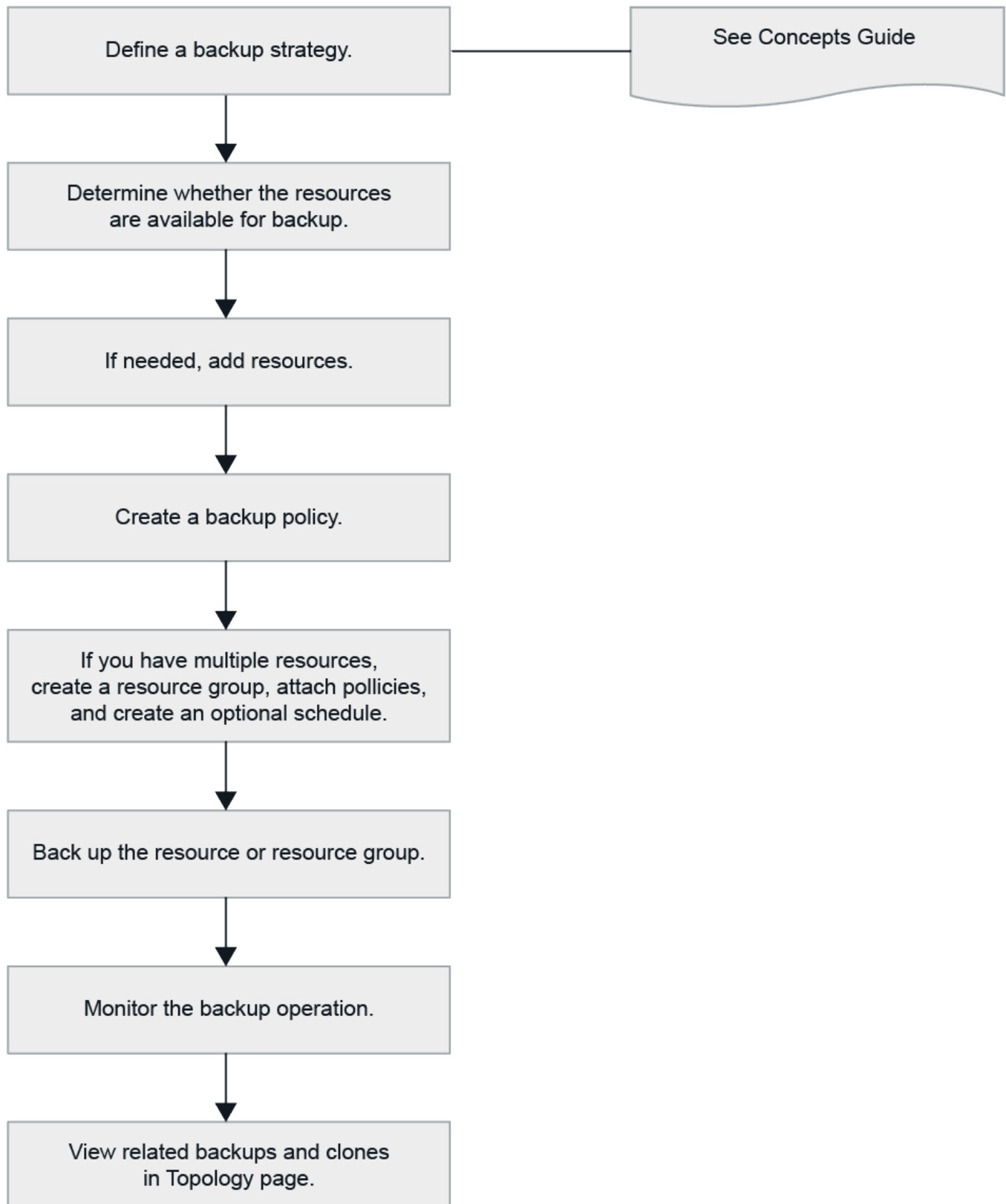
Piense en un grupo de recursos como si definiera lo que desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera cómo desea protegerla. Si está realizando una copia de seguridad de todos los clústeres, por ejemplo, puede crear un grupo de recursos que incluya todos los clústeres del host. Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Al crear el grupo de recursos y adjuntar las políticas, puede configurar el grupo de recursos para que realice una copia de seguridad completa diariamente.

Realizar copias de seguridad de los recursos de PostgreSQL

Realizar copias de seguridad de los recursos de PostgreSQL

Puede crear una copia de seguridad de un recurso (clúster) o de un grupo de recursos. El flujo de trabajo de respaldo incluye la planificación, la identificación de los clústeres para el respaldo, la administración de políticas de respaldo, la creación de grupos de recursos y la asociación de políticas, la creación de respaldos y el monitoreo de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen más información sobre los cmdlets de PowerShell. ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Descubra los clústeres automáticamente

Los recursos son clústeres PostgreSQL en el host Linux que son administrados por SnapCenter. Puede agregar recursos a grupos de recursos para realizar operaciones de protección de datos después de descubrir los clústeres de PostgreSQL que están disponibles.

Antes de empezar

- Ya debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y configurar las conexiones del sistema de almacenamiento.
- El complemento SnapCenter para PostgreSQL no admite el descubrimiento automático de los recursos que residen en entornos virtuales RDM/VMDK.

Acerca de esta tarea

- Después de instalar el complemento, todos los clústeres en ese host Linux se detectan automáticamente y se muestran en la página Recursos.
- Sólo los clústeres se descubren automáticamente.

Los recursos descubiertos automáticamente no se pueden modificar ni eliminar.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento para PostgreSQL de la lista.
2. En la página Recursos, seleccione el tipo de recurso de la lista Ver.
3. (Opcional) Haga clic en  y luego seleccione el nombre del host.

Luego puedes hacer clic en  para cerrar el panel de filtro.

4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

Los recursos se muestran junto con información como el tipo de recurso, el nombre del host, los grupos de recursos asociados, el tipo de copia de seguridad, las políticas y el estado general.

- Si el clúster está en un almacenamiento NetApp y no está protegido, se muestra No protegido en la columna Estado general.
- Si el clúster está en un sistema de almacenamiento NetApp y está protegido, y no se realiza ninguna operación de respaldo, se muestra Copia de seguridad no ejecutada en la columna Estado general. De lo contrario, el estado cambiará a Copia de seguridad fallida o Copia de seguridad exitosa según el último estado de la copia de seguridad.



Debe actualizar los recursos si se cambia el nombre de los clústeres fuera de SnapCenter.

Agregar recursos manualmente al host del complemento

El descubrimiento automático no es compatible con el host Windows. Debe agregar recursos del clúster Postgresql manualmente.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y configurar conexiones del sistema de almacenamiento.

Acerca de esta tarea

El descubrimiento automático no es compatible con las siguientes configuraciones:

- Diseños RDM y VMDK

Pasos

1. En el panel de navegación izquierdo, seleccione el complemento SnapCenter para Postgresql de la lista desplegable y luego haga clic en **Recursos**.
2. En la página Recursos, haga clic en **Agregar recursos de Postgresql**.
3. En la página Proporcionar detalles de recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Especifique el nombre del clúster.
Nombre del host	Introduzca el nombre del host.
Tipo	Seleccionar cluster.
Instancia	Especifique el nombre de la instancia, que es la principal del clúster.
Cartas credenciales	Seleccione las credenciales o agregue información para las credenciales. Esto es opcional.

4. En la página Proporcionar espacio de almacenamiento, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees, y luego haga clic en **Guardar**.

Opcional: Puede hacer clic en el *  * Icono para agregar más volúmenes, LUN y qtrees de otros sistemas de almacenamiento.

5. Opcional: En la página Configuración de recursos, para los recursos en el host de Windows, ingrese pares clave-valor personalizados para el complemento PostgreSQL
6. Revise el resumen y luego haga clic en **Finalizar**.

Los clústeres se muestran junto con información como el nombre del host, los grupos de recursos y políticas asociados, y el estado general.

Si desea proporcionar a los usuarios acceso a los recursos, debe asignar los recursos a los usuarios. Esto permite a los usuarios realizar las acciones para las que tienen permiso en los activos que les están asignados.

["Agregar un usuario o grupo y asignarle roles y activos"](#)

Después de terminar

- Después de agregar los clústeres, puede modificar los detalles del clúster PostgreSQL.

- Los recursos migrados (espacios de tabla y clústeres) de SnapCenter 5.0 se etiquetarán como tipo de clúster PostgreSQL en SnapCenter 6.0.
- Cuando modifique los recursos agregados manualmente que se migran desde SnapCenter 5.0 o versiones anteriores, haga lo siguiente en la página **Configuración de recursos** para pares de valores clave personalizados:
 - Especifique el término "PUERTO" en el campo **Nombre**.
 - Especifique el número de puerto en el campo **Valor**.

Crear políticas de respaldo para PostgreSQL

Antes de usar SnapCenter para realizar copias de seguridad de recursos de PostgreSQL, debe crear una política de copia de seguridad para el recurso o grupo de recursos que desea respaldar. Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad.

Antes de empezar

- Debes haber definido tu estrategia de backup.

Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para clústeres PostgreSQL.

- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, configurar conexiones del sistema de almacenamiento y agregar recursos.
- El administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino si está replicando instantáneas a un espejo o bóveda.

Además, puede especificar configuraciones de replicación, scripts y aplicaciones en la política. Estas opciones ahorran tiempo cuando desea reutilizar la política para otro grupo de recursos.

Acerca de esta tarea

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.
 - Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad de instantáneas mayor que la cantidad especificada 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.

5. En la página Tipo de política, 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 deba pasarse al complemento en formato clave-valor.

Puede proporcionar varios valores clave para pasarlos al complemento.

6. En la página Copia de seguridad y replicación, realice las siguientes acciones:

- a. Especifique la frecuencia de programación seleccionando **A pedido**, **Cada hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero también le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

- a. En la sección Configuración de instantáneas, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página **Tipo de copia de seguridad**:

Si quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.  Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva 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 .
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Si la relación de protección en ONTAP es de tipo Mirror and Vault y selecciona solo esta opción, las instantáneas creadas en el servidor principal no se transferirán al destino, pero aparecerán en él. Si se selecciona esta instantánea desde el destino para realizar una operación de restauración, se muestra el siguiente mensaje de error: La ubicación secundaria no está disponible para la copia de seguridad almacenada/duplicada seleccionada. Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Ver "Ver copias de seguridad y clones relacionados con los recursos de PostgreSQL en la página Topología".
Actualizar SnapVault después de crear una copia de instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault). Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón Actualizar en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre SnapLock Vault, consulte Confirmar instantáneas en WORM en un destino de bóveda Ver "Ver copias de seguridad y clones relacionados con los recursos de PostgreSQL en la página Topología".

Para este campo...	Haz esto...
Recuento de reintentos por error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

9. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados a una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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 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

- En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
- En la página Recursos, haga clic en **Nuevo grupo de recursos**.
- En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.  El nombre del grupo de recursos no debe exceder los 250 caracteres.
Etiquetas	Ingresa una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

Para este campo...	Haz esto...
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desee utilizar para el nombre de la instantánea. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

4. En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

Esto ayuda a filtrar la información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. En la página Configuración de la aplicación, haga lo siguiente:
- Haga clic en la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación de instantánea del grupo de consistencia	Seleccione Urgente, Medio o Relajado para especificar el tiempo de espera para que se complete la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

+

- Haga clic en la flecha **Scripts** e ingrese los comandos pre y post para las operaciones de inactividad, instantánea y activación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
- Haga clic en la flecha **Configuraciones personalizadas** e ingrese los pares clave-valor personalizados necesarios para todas las operaciones de protección de datos que utilicen este recurso.

Parámetro	Valor	Descripción
HABILITAR REGISTRO DE ARCHIVO	(T/N)	Permite que la gestión del registro de archivo elimine los registros de archivo.
RETENCIÓN DE REGISTRO DE ARCHIVO	número_de_días	Especifica el número de días que se conservan los registros de archivo. Esta configuración debe ser igual o mayor que NTAP_SNAPSHOT_RETENTIONS.
DIRECCIÓN DE REGISTRO DE ARCHIVO	directorio_de_información_de_cambio/registros	Especifica la ruta al directorio que contiene los registros de archivo.

Parámetro	Valor	Descripción
EXTRACCIÓN DEL REGISTRO DE ARCHIVO	extensión_de_archivo	Especifica la longitud de la extensión del archivo de registro de archivo. Por ejemplo, si el registro de archivo es log_backup_0_0_0_0.161518551942 9 y el valor de file_extension es 5, entonces la extensión del registro retendrá 5 dígitos, que es 16151.
ARCHIVO_REGISTRO_BÚSQUEDA_RECURSIVA ARCH	(T/N)	Permite la gestión de registros de archivo dentro de 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 complementos PostgreSQL para Linux y no son compatibles con el clúster PostgreSQL registrado como un complemento centralizado de Windows.

- c. Haga clic en la flecha **Herramienta de copia de instantáneas** para seleccionar la herramienta para crear instantáneas:

Si quieres...	Entonces...
SnapCenter para utilizar el complemento para Windows y poner el sistema de archivos en un estado consistente antes de crear una instantánea. Para los recursos de Linux, esta opción no es aplicable.	Seleccione * SnapCenter con consistencia del sistema de archivos*.
SnapCenter para crear una instantánea de nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
Ingresa el comando que se ejecutará en el host para crear copias instantáneas.	Seleccione Otro y luego ingrese el comando que se ejecutará en el host para crear una instantánea.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

Las políticas se enumeran en la sección Configurar programaciones para políticas seleccionadas.

- b. En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna **Horarios aplicados**.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El servidor SMTP debe configurarse en **Configuración > Configuración global**.

9. Revise el resumen y luego haga clic en **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos de PostgreSQL en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más

adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:
 - a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:
 - a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
 - b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
 - c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para PostgreSQL

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar copias de seguridad, restaurar o clonar clústeres de PostgreSQL.

Antes de empezar

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de los clústeres puede mostrarse en la GUI de SnapCenter como “No disponible para respaldo” o “No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP 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 al sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una nueva credencial mediante el cmdlet Add-SmCredential.

Este ejemplo muestra cómo crear una nueva credencial llamada FinanceAdmin con 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 complemento 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. Establezca la ruta a SQLLIB.

Para Windows, el complemento PostgreSQL utilizará la ruta predeterminada para la carpeta SQLLIB: "C:\Program Files\IBM\SQLLIB\BIN"

Si desea anular la ruta predeterminada, utilice el siguiente comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode PostgreSQL -configSettings @{ "PostgreSQL_SQLLIB_CMD" = "<custom_path>\IBM\SQLLIB\BIN" }
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar una copia de seguridad de PostgreSQL

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Antes de empezar

- Debes haber creado una política de respaldo.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".
- Para la operación de copia de seguridad basada en instantáneas, asegúrese de que todos los clústeres de inquilinos sean válidos y activos.
- Para los comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del

modo inactivo, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:

- 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 los comandos no existen en la lista de comandos, la operación fallará.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Seleccionar ** y, a continuación, seleccione el nombre del host y el tipo de recurso para filtrar los recursos. Luego puedes seleccionar  para cerrar el panel de filtro.

3. Seleccione el recurso que desea respaldar.
4. En la página Recursos, seleccione **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Configuración de la aplicación, haga lo siguiente:
 - Seleccione la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia, si es necesario, y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación "Instantánea del grupo de consistencia"	Seleccione Urgente , Medio o Relajado para especificar el tiempo de espera para que finalice la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

- Seleccione la flecha **Scripts** para ejecutar comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo.

También puede ejecutar comandos previos antes de salir de la operación de copia de seguridad. Los prescriptos y posscripts se ejecutan en el servidor SnapCenter .

- Seleccione la flecha **Configuraciones personalizadas** y luego ingrese los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.
- Seleccione la flecha **Herramienta Copiar Instantánea** para seleccionar la herramienta para crear Instantáneas:

Si quieres...	Entonces...
SnapCenter para crear una instantánea a nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
SnapCenter para usar el complemento para Windows para poner el sistema de archivos en un estado consistente y luego crear una instantánea	Seleccione * SnapCenter con consistencia del sistema de archivos*.
Para ingresar el comando para crear una instantánea	Seleccione Otro y luego ingrese el comando para crear una instantánea.

6. En la página Políticas, realice los siguientes pasos:

- Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- Seleccionar *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.

policy_name es el nombre de la política que usted seleccionó.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en **Configuración > Configuración global**.

8. Revise el resumen y luego seleccione **Finalizar**.

Se muestra la página de topología de recursos.

9. Seleccione **Hacer copia de seguridad ahora**.

10. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

- En configuraciones de MetroCluster , es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

Para obtener información, consulte: ["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar.

Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese script, el comando `do_start method` inicia el servicio del complemento VMware de SnapCenter . Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

Se muestra la solicitud de nombre de usuario y contraseña.

2. Agregue recursos manuales mediante el cmdlet `Add-SmResources`.

Este ejemplo muestra cómo agregar una instancia de 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 respaldo mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
5. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

Este ejemplo muestra cómo realizar una copia de seguridad 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 una copia de seguridad 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 del trabajo (en ejecución, completado o fallido) mediante el cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Supervise los detalles del trabajo de respaldo, como la identificación y el nombre del respaldo, para realizar una operación de restauración o clonación 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de grupos de recursos

Un grupo de recursos es una colección de recursos en un host. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".

Acerca de esta tarea

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o seleccionando , y luego seleccionando la etiqueta. Luego puedes seleccionar  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 PostgreSQL

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:

- a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en clústeres de PostgreSQL en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 operaciones de copia de seguridad para PostgreSQL

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de copia de seguridad.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	a. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. b. Seleccione la operación y luego haga clic en Cancelar trabajo.
Panel de actividades	a. Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Ver copias de seguridad y clones de PostgreSQL en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario.

Acerca de esta tarea

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .



La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página de topología del recurso seleccionado.

4. Revise la **tarjeta de resumen** para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario y secundario.

La sección **Tarjeta de resumen** muestra el número total de copias de seguridad basadas en instantáneas 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración de SnapLock más largo se recupera de ONTAP.

Después de realizar una copia de seguridad a pedido, al hacer clic en el botón **Actualizar** se actualizan los detalles de la copia de seguridad o la clonación.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

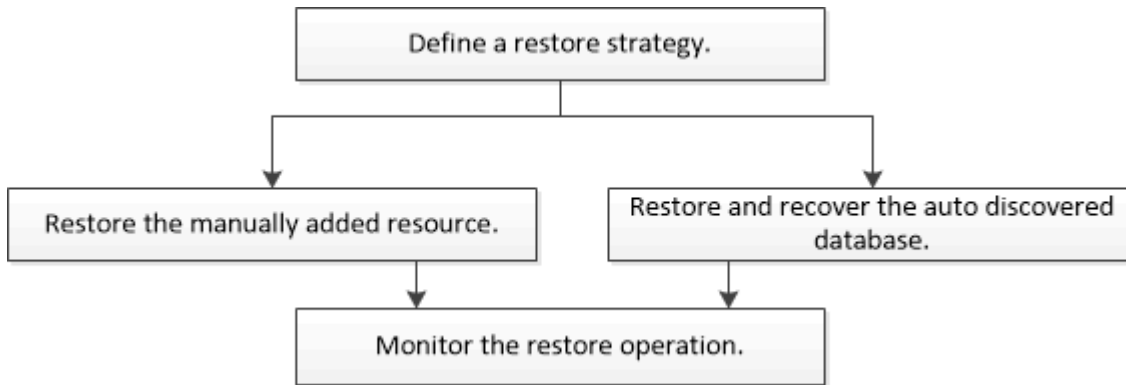
7. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en .
8. Si desea dividir un clon, seleccione el clon de la tabla y luego haga clic en .

Restaurar PostgreSQL

Restaurar flujo de trabajo

El flujo de trabajo de restauración y recuperación incluye la planificación, la ejecución de las operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de restauración:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

["Guía de referencia de cmdlets del software SnapCenter"](#) .

Restaurar y recuperar una copia de seguridad de un recurso agregado manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



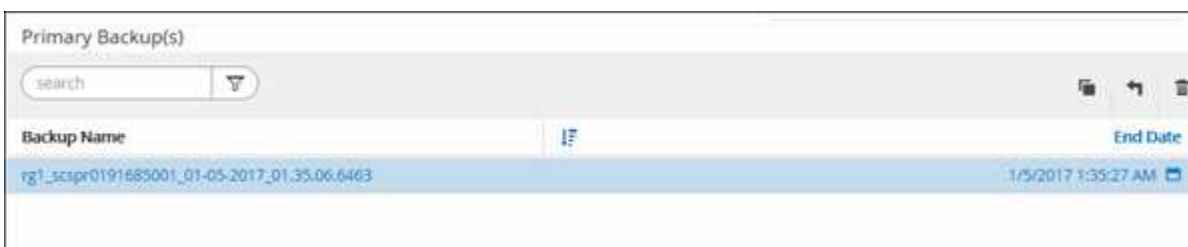
Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.



Primary Backup(s)	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01:35:06.6463	1/5/2017 1:35:27 AM

6. En la página Restaurar alcance, seleccione **Recurso completo**.

- a. Si selecciona **Recurso completo**, se restauran todos los volúmenes de datos configurados del clúster PostgreSQL.

Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Puede seleccionar varios LUN.



Si selecciona **Todos**, se restaurarán todos los archivos en los volúmenes, qtrees o LUN.

7. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no están disponibles para los recursos descubiertos automáticamente.

8. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no están disponibles para los recursos descubiertos automáticamente.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets Get-SmBackup y Get-SmBackupReport.

Este ejemplo muestra información sobre todas las copias de seguridad 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	

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:


```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet `Restore-SmBackup`.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar y recuperar una copia de seguridad de un clúster detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los

comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:

- 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Las copias de seguridad basadas en archivos no se pueden restaurar desde SnapCenter.
- Para los recursos descubiertos automáticamente, la restauración es compatible 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 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

- En la página Restaurar alcance, seleccione **Recurso completo** para restaurar los volúmenes de datos configurados del clúster PostgreSQL.
- En la página Ámbito de recuperación, seleccione una de las siguientes opciones:

Si usted...	Haz esto...
Quiere recuperarse lo más cerca posible de la hora actual	Seleccione Recuperar al estado más reciente . Para recursos de contenedor único, especifique una o más ubicaciones de respaldo de registros y catálogos.
¿Quieres recuperar el punto especificado en el tiempo?	Seleccione Recuperar a punto en el tiempo. a. Introduzca fecha y hora. Introduzca fecha y hora. Por ejemplo, el host de PostgreSQL Linux está ubicado en Sunnyvale, CA y el usuario en Raleigh, NC está recuperando los registros en SnapCenter. Si el usuario desea realizar una recuperación a las 5 a. m. de Sunnyvale, CA, entonces el usuario debe configurar la zona horaria del navegador a la zona horaria del host de PostgreSQL Linux, que es GMT-07:00 y especificar la fecha y hora como 5:00 a. m.
No quiero recuperarme	Seleccione Sin recuperación .



No es posible recuperar recursos de PostgreSQL agregados manualmente.



El complemento SnapCenter para PostgreSQL crea una etiqueta de respaldo y un mapa de espacio de tabla en la carpeta `/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/` para ayudar a realizar la recuperación manual.

- En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no están disponibles para los recursos descubiertos automáticamente.

- En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no están disponibles para los recursos descubiertos automáticamente.

- En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

4. Revise el resumen y luego haga clic en **Finalizar**.
5. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Restaurar recursos mediante cmdlets de PowerShell

Restaurar una copia de seguridad de un recurso incluye iniciar una sesión de conexión con el servidor SnapCenter , enumerar las copias de seguridad y recuperar información de las copias de seguridad, y restaurar una copia de seguridad.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```

PS C:\> Get-SmBackupReport -FromDate "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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar operaciones de restauración de PostgreSQL

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso

-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Clonar copias de seguridad de recursos de PostgreSQL

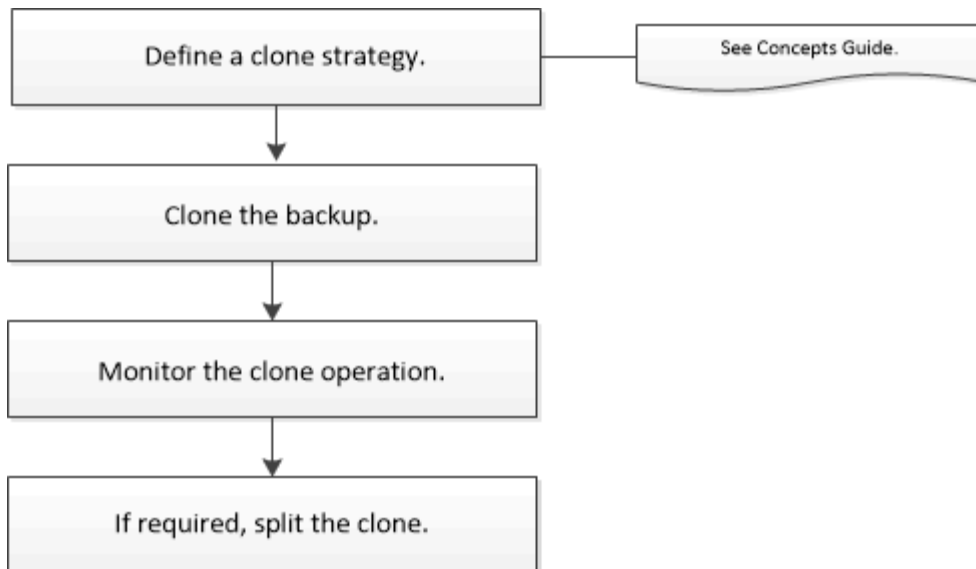
Flujo de trabajo de clonación

El flujo de trabajo de clonación incluye la realización de la operación de clonación y la supervisión de la operación.

Acerca de esta tarea

- Puede clonar en el servidor PostgreSQL de origen.
- Puede clonar copias de seguridad de recursos por los siguientes motivos:
 - Para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de recursos actuales durante los ciclos de desarrollo de aplicaciones
 - Para herramientas de extracción y manipulación de datos al rellenar almacenes de datos
 - Para recuperar datos que fueron borrados o modificados por error

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de clonación:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

Clonar una copia de seguridad de PostgreSQL

Puede utilizar SnapCenter para clonar una copia de seguridad. Puede clonar desde una copia de seguridad primaria o secundaria.

Antes de empezar

- Deberías haber realizado una copia de seguridad de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados que alojan los volúmenes estén en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Para los comandos previos o posteriores a la clonación, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["Dividir un volumen FlexClone de su volumen principal"] .
- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con información como el tipo, el host, los grupos de recursos y políticas asociados y el estado.

3. Seleccione el recurso o grupo de recursos.

Debe seleccionar un recurso si selecciona un grupo de recursos.

Se muestra la página de topología de recursos o grupos de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).

5. Seleccione la copia de seguridad de datos de la tabla y luego haga clic en  .

6. En la página Ubicación, realice las siguientes acciones:

Para este campo...	Haz esto...
Servidor clonado	Seleccione un host en el que se debe crear el clon.
Puerto de destino	Ingrese el puerto de destino de PostgreSQL para clonar desde las copias de seguridad existentes.
Dirección IP de exportación de NFS	Introduzca las direcciones IP o los nombres de host a los que se exportarán los volúmenes clonados. Esto solo se aplica a recursos de tipo de almacenamiento NFS.
Capacidad de almacenamiento máxima (MiB/s)	Introduzca el rendimiento máximo de un grupo de capacidad. Esto solo se aplica a recursos de tipo de almacenamiento ANF.

7. En la página Scripts, realice los siguientes pasos:



Los scripts se ejecutan en el host del complemento.

- a. Introduzca los comandos para pre-clonar o post-clonar que deben ejecutarse antes o después de la operación de clonación, respectivamente.
 - Comando de preclonación: eliminar clústeres existentes con el mismo nombre

- Comando posterior a la clonación: verificar un clúster o iniciar un clúster.

b. Introduzca el comando de montaje para montar un sistema de archivos en un host.

Comando de montaje para un volumen o qtree en una máquina Linux:

Ejemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

9. Revise el resumen y luego haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere las copias de seguridad para realizar la operación de clonación mediante el cmdlet `Get-SmBackup`.

Este ejemplo muestra que hay dos copias de seguridad 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 clonación desde una copia de seguridad existente y especifique las direcciones IP de exportación NFS en las que se exportan los volúmenes clonados.

Este ejemplo muestra que la copia de seguridad que se va a clonar tiene una dirección `NFSExportIPs` de 10.32.212.14:

Para el 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 especifica NFSExportIPs, el valor predeterminado se exporta al host de destino clonado.

4. Verifique que las copias de seguridad se hayan clonado correctamente utilizando el cmdlet Get-SmCloneReport para ver los detalles del trabajo de clonación.

Puede ver detalles como el ID del clon, la fecha y hora de inicio, 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           :
```

Supervisar operaciones de clonación de PostgreSQL

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone, consulte ["Dividir un volumen FlexClone de su volumen principal"](#).
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento

apropiado de la lista.

2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Eliminar o dividir clones del clúster PostgreSQL después de actualizar SnapCenter

Después de actualizar a SnapCenter 4.3, ya no verá los clones. Puede eliminar el clon o dividir los clones desde la página Topología del recurso desde el cual se crearon los clones.

Acerca de esta tarea

Si desea localizar la huella de almacenamiento de los clones ocultos, ejecute el siguiente comando: `Get-SmClone -ListStorageFootprint`

Pasos

1. Elimine las copias de seguridad de los recursos clonados mediante el cmdlet remove-smbbackup.
2. Elimine el grupo de recursos de los recursos clonados mediante el cmdlet remove-smresourcegroup.
3. Elimine la protección del recurso clonado mediante el cmdlet remove-smprotectresource.
4. Seleccione el recurso principal en la página Recursos.

Se muestra la página de topología de recursos.

5. Desde la vista Administrar copias, seleccione los clones de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).
6. Seleccione los clones y luego haga clic  Para eliminar clones o hacer clic  Para dividir los clones.
7. Haga clic en **Aceptar**.

Proteger MySQL

Complemento de SnapCenter para MySQL

Descripción general del complemento SnapCenter para MySQL

El complemento SnapCenter para bases de datos MySQL es un componente del lado del host del SnapCenter software de NetApp que permite la gestión de protección de datos consciente de la aplicación de bases de datos MySQL. El complemento para la base de datos MySQL automatiza la copia de seguridad, la restauración y la clonación de bases de datos MySQL en su entorno de SnapCenter .

SnapCenter admite configuraciones de MySQL de instancia única. Puede utilizar el complemento para la base de datos MySQL en entornos Linux y Windows. En entornos Windows, MySQL se soportará como recurso manual.

Cuando se instala el complemento para la base de datos MySQL, puede utilizar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen. También puede utilizar el complemento con la tecnología NetApp SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de los estándares.

El complemento SnapCenter para MySQL admite NFS y SAN en diseños de almacenamiento de archivos ONTAP y Azure NetApp .

Se admite el diseño de almacenamiento virtual VMDK, vVol y RDM.

No se admiten enlaces simbólicos.

Qué puede hacer utilizando el complemento SnapCenter para MySQL

Cuando instala el complemento para la base de datos MySQL en su entorno, puede usar SnapCenter para realizar copias de seguridad, restaurar y clonar instancias de MySQL. También puede realizar tareas de apoyo a dichas operaciones.

- Agregar instancias.
- Crear copias de seguridad.
- Restaurar desde copias de seguridad.
- Copias de seguridad clonadas.
- Programar operaciones de respaldo.
- Supervisar operaciones de copia de seguridad, restauración y clonación.
- Ver informes de operaciones de copia de seguridad, restauración y clonación.

Funciones del complemento SnapCenter para MySQL

SnapCenter se integra con la aplicación complementaria y con las tecnologías NetApp en el sistema de almacenamiento. Para trabajar con el complemento para la base de datos MySQL, utilice la interfaz gráfica de usuario de SnapCenter .

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite realizar operaciones consistentes de copia de seguridad, restauración y clonación en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y supervisar trabajos en todos los complementos.

- **Administración central automatizada**

Puede programar operaciones de respaldo, configurar la retención de respaldo basada en políticas y realizar operaciones de restauración. También puede supervisar su entorno de forma proactiva configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología de copia de instantáneas de NetApp sin interrupciones**

SnapCenter utiliza la tecnología de instantáneas de NetApp con el complemento para base de datos MySQL para realizar copias de seguridad de los recursos.

El uso del complemento para MySQL también ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de copia de seguridad, restauración y clonación
- Seguridad respaldada por RBAC y delegación de roles centralizada

También puede configurar las credenciales para que los usuarios autorizados de SnapCenter tengan permisos a nivel de aplicación.

- Creación de copias puntuales y con uso eficiente del espacio de recursos para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

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

- Compatibilidad con la función de instantánea del grupo de consistencia (CG) de ONTAP como parte de la creación de copias de seguridad.
- Capacidad de ejecutar múltiples copias de seguridad simultáneamente en múltiples hosts de recursos

En una sola operación, las instantáneas se consolidan cuando los recursos de un solo host comparten el mismo volumen.

- Capacidad de crear instantáneas mediante comandos externos.
- Soporte para Linux LVM en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el complemento SnapCenter para MySQL

SnapCenter admite una amplia gama de tipos de almacenamiento tanto en máquinas físicas como en máquinas virtuales (VM). Debe verificar la compatibilidad con su tipo de almacenamiento antes de instalar el complemento SnapCenter para MySQL.

Máquina	Tipo de almacenamiento
Servidor físico	• LUN conectados a FC • LUN conectados a iSCSI • Volúmenes conectados a NFS
VMware ESXi	• El escaneo de los adaptadores de bus de host (HBA) puede demorar mucho tiempo en completarse porque SnapCenter escanea todos los adaptadores de bus de host presentes en el host. Puede editar el archivo LinuxConfig.pm ubicado en <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> para establecer el valor del parámetro SCSI_HOSTS_OPTIMIZED_RESCAN en 1 para volver a escanear solo los HBA que figuran en HBA_DRIVER_NAMES. • LUN iSCSI conectados directamente al sistema invitado por el iniciador iSCSI • VMDK en almacenes de datos NFS • VMDK en VMFS creados • Volúmenes NFS conectados directamente al sistema invitado • Almacenes de datos vVol tanto en NFS como en SAN El almacén de datos vVol solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP necesarios para el complemento MySQL

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - almuerzo
 - lun crear
 - lun crear
 - lun crear

- eliminar lun
- agregar igroup lun
- crear igroup lun
- eliminar igroup lun
- Cambiar nombre de igroup lun
- Cambiar nombre de igroup lun
- Programa de igroup de Lun
- Asignación de LUN a nodos de informes adicionales
- creación de mapeo LUN
- eliminar mapeo lun
- Mapeo de LUN: eliminar nodos de informes
- espectáculo de mapeo de lun
- modificar lun
- volumen de movimiento de LUN
- lun sin conexión
- lun en línea
- lun reserva persistente clara
- cambio de tamaño de lun
- serie lun
- espectáculo de almuerzo
- regla de adición de política de SnapMirror
- regla de modificación de política de SnapMirror
- regla de eliminación de política de SnapMirror
- Mostrar política de Snapmirror
- restauración de SnapMirror
- espectáculo de Snapmirror
- historial de programas de Snapmirror
- actualización de SnapMirror
- actualización-ls-set de snapmirror
- Lista de destinos de Snapmirror
- versión
- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen

- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- tiempo de caducidad de modificación de instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFs de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIF de vserver
- Mostrar copia de sombra de CIF de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- política de exportación de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- vserver iscsi
- Mostrar conexión iscsi de vserver
- espectáculo vserver
- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red

- Mostrar interfaz de red
- vsServer

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para MySQL

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Estrategia de respaldo para MySQL

Definir una estrategia de respaldo para MySQL

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le ayudará a tener los respaldos que necesita para restaurar o clonar sus recursos con éxito. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Acerca de esta tarea

Un SLA define el nivel de servicio que se espera y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. RPO define la estrategia para la edad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA, RTO y RPO contribuyen a la estrategia de protección de datos.

Pasos

1. Determina cuándo debes realizar copias de seguridad de tus recursos.
2. Decide cuántos trabajos de respaldo necesitas.
3. Decide cómo nombrar tus copias de seguridad.
4. Decida si desea crear una política basada en copias de instantáneas para realizar copias de seguridad de instantáneas de la base de datos consistentes con la aplicación.
5. Decida si desea utilizar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
6. Determine el período de retención de las instantáneas en el sistema de almacenamiento de origen y el destino SnapMirror .
7. Determine si desea ejecutar algún comando antes o después de la operación de copia de seguridad y proporcione un script previo o posterior.

Descubrimiento automático de recursos en el host Linux

Los recursos son instancias de MySQL en el host Linux que son administradas por SnapCenter. Después de instalar el complemento SnapCenter Plug-in para MySQL, las instancias de MySQL en ese host Linux se detectan automáticamente y se muestran en la página Recursos.

Tipo de backups admitido

El tipo de copia de seguridad especifica el tipo de copia de seguridad que desea crear. SnapCenter admite el tipo de copia de seguridad basada en instantáneas para bases de datos MySQL.

Copia de seguridad basada en instantáneas

Las copias de seguridad basadas en instantáneas aprovechan la tecnología de instantáneas de NetApp para crear copias en línea, de solo lectura, de los volúmenes en los que residen las bases de datos MySQL.

Cómo el complemento SnapCenter para MySQL utiliza instantáneas de grupos de consistencia

Puede utilizar el complemento para crear instantáneas de grupos de consistencia para grupos de recursos. Un grupo de consistencia es un contenedor que puede albergar múltiples volúmenes para que puedas administrarlos como una sola entidad. Un grupo de consistencia son instantáneas simultáneas de múltiples volúmenes que proporcionan copias consistentes de un grupo de volúmenes.

También puede especificar el tiempo de espera para que el controlador de almacenamiento agrupe las instantáneas de manera consistente. Las opciones de tiempo de espera disponibles son **Urgente**, **Medio** y **Relajado**. También puede habilitar o deshabilitar la sincronización del diseño de archivo Write Anywhere (WAFL) durante la operación de instantánea de grupo consistente. La sincronización de WAFL mejora el rendimiento de una instantánea de grupo de consistencia.

Cómo gestiona SnapCenter el mantenimiento de las copias de seguridad de registros

SnapCenter administra el mantenimiento de las copias de seguridad de datos en los niveles del sistema de almacenamiento y del sistema de archivos.

Consideraciones para determinar los cronogramas de copias de seguridad para MySQL

El factor más crítico para determinar un cronograma de respaldo es la tasa de cambio del recurso. Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su acuerdo de nivel de servicio (SLA) y su objetivo de punto de recuperación (RPO).

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de copia de seguridad (con qué frecuencia se deben realizar las copias de seguridad)

La frecuencia de copia de seguridad, también llamada tipo de programación para algunos complementos, es parte de una configuración de política. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual.

- Programaciones de copias de seguridad (cuándo exactamente se realizarán las copias de seguridad)

Las programaciones de copias de seguridad son parte de la configuración de un recurso o de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m.

Número de trabajos de respaldo necesarios para MySQL

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño del recurso, la cantidad de volúmenes utilizados, la tasa de cambio del recurso y su Acuerdo de Nivel de Servicio (SLA).

Convenciones de nombres de copias de seguridad para complementos de bases de datos MySQL

Puede utilizar la convención de nombres de instantáneas predeterminada o utilizar una convención de nombres personalizada. La convención de nombres de copia de seguridad predeterminada agrega una marca de tiempo a los nombres de las instantáneas que le ayuda a identificar cuándo se crearon las copias.

La instantánea utiliza la siguiente convención de nombres predeterminada:

```
resourcegroupname_hostname_timestamp
```

Debes nombrar tus grupos de recursos de respaldo de forma lógica, como en el siguiente ejemplo:

```
dts1_mach1x88_03-12-2015_23.17.26
```

En este ejemplo, los elementos de sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre del host.

- 03-12-2015_23.17.26 es la fecha y la marca de tiempo.

Como alternativa, puede especificar el formato del nombre de la instantánea mientras protege recursos o grupos de recursos seleccionando **Usar formato de nombre personalizado para copia de instantánea**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, el sufijo de marca de tiempo se agrega al nombre de la instantánea.

Estrategia de restauración y recuperación para MySQL

Definir una estrategia de restauración y recuperación para los recursos de MySQL

Debe definir una estrategia antes de restaurar y recuperar su base de datos para poder realizar operaciones de restauración y recuperación con éxito.



Sólo se admite la recuperación manual de la base de datos.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos MySQL agregados manualmente
2. Determinar las estrategias de restauración compatibles con las bases de datos MySQL detectadas automáticamente
3. Decide el tipo de operaciones de recuperación que deseas realizar.

Tipos de estrategias de restauración compatibles con recursos MySQL agregados manualmente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter. Hay dos tipos de estrategias de restauración para recursos MySQL agregados manualmente.



No es posible recuperar recursos MySQL agregados manualmente.

Restauración completa de recursos

- Restaura todos los volúmenes, qtrees y LUN de un recurso



Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Tipo de estrategia de restauración compatible con MySQL detectado automáticamente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter.

La restauración completa de recursos es la estrategia de restauración compatible con las bases de datos MySQL descubiertas automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para MySQL detectado automáticamente

El complemento SnapCenter para MySQL admite SnapRestore de archivo único y tipos de restauración de conexión y copia para bases de datos MySQL descubiertas automáticamente.

SnapRestore de archivo único se realiza en entornos NFS para los siguientes escenarios:

- Si solo se selecciona la opción **Recurso completo**
- Cuando la copia de seguridad seleccionada es de una ubicación secundaria de SnapMirror o SnapVault y está seleccionada la opción **Recurso completo**

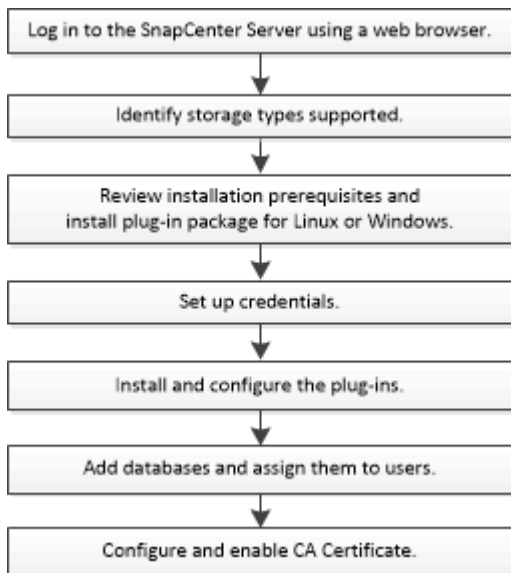
SnapRestore de archivo único se realiza en entornos SAN para los siguientes escenarios:

- Si solo se selecciona la opción **Recurso completo**
- Cuando se selecciona la copia de seguridad desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Recurso completo**

Prepárese para instalar el complemento SnapCenter para MySQL

Flujo de trabajo de instalación del complemento SnapCenter para MySQL

Debe instalar y configurar el complemento SnapCenter para MySQL si desea proteger las bases de datos MySQL.



Requisitos previos para agregar hosts e instalar el complemento SnapCenter para MySQL

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos. El complemento SnapCenter para MySQL está disponible en entornos Windows y Linux.

- Debes tener instalado Java 11 en tu host.



IBM Java no es compatible con hosts Windows y Linux.

- Para Windows, el servicio de creación de complementos debe ejecutarse utilizando el usuario de Windows "LocalSystem", que es el comportamiento predeterminado cuando el complemento para MySQL se instala como administrador de dominio.
- Al instalar un complemento 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 complemento SnapCenter para Microsoft Windows se implementará de forma predeterminada con el complemento MySQL en los hosts de Windows.
- El servidor SnapCenter debe tener acceso al puerto 8145 o personalizado del host del complemento para MySQL.
- Para MySQL 5.7, binlog debe especificarse en el archivo de configuración de MySQL (my.cnf o mysql-server.cnf).

Hosts de Windows

- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Al instalar el complemento para MySQL en un host Windows, el complemento de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Windows.

["Descargar JAVA para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Hosts Linux

- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Linux.

["Descargar JAVA para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Para las bases de datos MySQL que se ejecutan en un host Linux, al instalar el complemento para MySQL, el complemento de SnapCenter para UNIX se instala automáticamente.
- Debe tener **bash** como el shell predeterminado para la instalación del complemento.

Comandos suplementarios

Para ejecutar un comando complementario en el complemento 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 complementarios en el host del complemento, abra el archivo `allowed_commands.config` en un editor. Ingrese cada comando en una línea separada y los comandos no distinguen entre mayúsculas y minúsculas. Asegúrese de especificar la ruta de acceso completa y de encerrarla entre comillas (") si contiene espacios.

Por ejemplo:

comando: mount comando: umount comando: "C:\Archivos de programa\NetApp\SnapCreator commands\sdcli.exe" comando: myscript.bat

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.

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

"No se permite la ejecución de [/mnt/mount -a]. Autorice agregando el comando en el archivo %s en el host del complemento.



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

Configurar privilegios de sudo para usuarios no root para el host Linux

SnapCenter permite que un usuario no root instale el paquete de complementos de SnapCenter para Linux e inicie el proceso de instalación del complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Si la umask es 0027, asegúrese de que la carpeta java y todos los archivos dentro de ella tengan el permiso 555. De lo contrario, la instalación del complemento podría fallar.
- Para el usuario no root, asegúrese de que el nombre del usuario no root y el grupo del usuario sean los mismos.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- /inicio/*USUARIO_LINUX*/sc_netapp/snapcenter_linux_host_plugin.bin
- /ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar
- /ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl

Pasos

1. Inicie sesión en el host Linux en el que desea instalar el paquete de complementos de SnapCenter para Linux.
2. Agregue las siguientes líneas al archivo /etc/sudoers utilizando la utilidad visudo para 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_Precchecks.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 SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, 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 RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` _ si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux

Antes de instalar el paquete de complementos de SnapCenter para Linux, debe familiarizarse con algunos requisitos básicos de tamaño y espacio del sistema host.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Servidor empresarial SUSE Linux (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .
RAM mínima para el complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 Oracle Java y OpenJDK Si ha actualizado JAVA a la última versión, 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 correcta. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Configurar credenciales para el complemento SnapCenter para MySQL

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en bases de datos o sistemas de archivos de Windows.

Acerca de esta tarea

- Hosts Linux

Debe configurar credenciales para instalar complementos en hosts Linux.

Debe configurar las credenciales para el usuario root o para un usuario no root que tenga privilegios de

sudo para instalar e iniciar el proceso del complemento.

Mejor práctica: Si bien se le permite crear credenciales para Linux después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

- Hosts de Windows

Debe configurar las credenciales de Windows antes de instalar complementos.

Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.

Si configura 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 de respaldo al nombre de usuario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, especifique la información necesaria para configurar las credenciales:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. - Administrador del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: <i>NetBIOS\Nombre de usuario</i> <i>Dominio FQDN\Nombre de usuario</i> - 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>NombreDeUsuario</i> No utilice comillas dobles (") ni tildes invertidas (´) en las contraseñas. No debe utilizar los símbolos menor que (<) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que<!10, menos que10<!, acento grave`12.
Password	Introduzca la contraseña utilizada para la autenticación.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar.
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no sea root.  Aplicable únicamente a usuarios de Linux.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Instalar el complemento SnapCenter para MySQL

Agregar hosts e instalar paquetes de complementos en hosts remotos

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar los paquetes de complementos. Los complementos se instalan automáticamente en los hosts remotos. Puede agregar el host e instalar paquetes de complementos 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 complemento es Windows 2022, debe realizar lo siguiente:
 - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
 - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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 esté ejecutándose.
- La documentación de administración contiene información sobre la gestión de hosts.

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host: • Ventanas • Linux  El complemento para MySQL debe instalarse en el servidor de base de datos MySQL.

Para este campo...	Haz esto...
Host name	Introduzca el nombre del host de comunicación. Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN.
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que proporcionó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea instalar.

Al utilizar la API REST para instalar el complemento para MySQL, debe pasar la versión como 3.0. Por ejemplo, MySQL:3.0

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.

Para este campo...	Haz esto...
Ruta de instalación	El complemento para MySQL se instala en el host del cliente MySQL, y este host puede estar en un sistema Windows o en un sistema Linux. • Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\ NetApp\ SnapCenter. Opcionalmente, puedes personalizar la ruta. • Para el paquete de complementos de SnapCenter para Linux, la ruta predeterminada es /opt/ NetApp/snapcenter. Opcionalmente, puedes personalizar la ruta.
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Agregar todos los hosts en el clúster	No aplicable.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	No aplicable.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla "Omitir comprobaciones previas", se valida el host para verificar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell, la versión de .NET, la ubicación (para complementos de Windows) y la versión de Java (para complementos de Linux) se validan según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Si el tipo de host es Linux, verifique la huella digital y luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

- Para el complemento de Windows, los registros de instalación y actualización se encuentran en:
C:\Windows\ SnapCenter plugin\Install<JOBID>_

- Para el complemento 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 6.0 de SnapCenter , el complemento basado en PERL existente para MySQL se desinstalará del servidor de complementos remoto.

Instalar paquetes de complementos de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de complementos de SnapCenter para Linux o Windows en varios hosts simultáneamente mediante el cmdlet de PowerShell `Install-SmHostPackage`.

Antes de empezar

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar el paquete de complemento.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet `Open-SmConnection` y luego ingrese sus credenciales.
3. Instale el complemento en varios hosts utilizando el cmdlet `Install-SmHostPackage` y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Puede utilizar la opción `-skipprecheck` cuando haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.

4. Introduzca sus credenciales para la instalación remota.

Instale el complemento SnapCenter para MySQL en hosts Linux mediante la interfaz de línea de comandos

Debe instalar el complemento SnapCenter para la base de datos MySQL mediante la interfaz de usuario (UI) de SnapCenter . Si su entorno no permite la instalación remota del complemento desde la interfaz de usuario de SnapCenter , puede instalar el complemento para la base de datos MySQL en modo consola o en modo silencioso mediante la interfaz de línea de comandos (CLI).

Antes de empezar

- Debe instalar el complemento para la base de datos MySQL en cada uno de los hosts Linux donde se debe proteger la instancia MySQL.
- El host Linux en el que está instalando el complemento de SnapCenter para la base de datos MySQL debe cumplir con los requisitos de software, base de datos y sistema operativo dependientes.

La herramienta Matriz de Interoperabilidad (IMT) contiene la información más reciente sobre las

configuraciones admitidas.

"Herramienta de matriz de interoperabilidad de NetApp"

- El complemento de SnapCenter para la base de datos MySQL es parte del paquete de complementos de SnapCenter para Linux. Antes de instalar el paquete de complementos de SnapCenter para Linux, ya debe haber instalado SnapCenter en un host Windows.

Pasos

1. Copie el archivo de instalación del paquete de complementos de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\ SnapCenter\Package Repository al host donde desea instalar el complemento para MySQL.

Puede acceder a esta ruta desde el host donde está instalado SnapCenter Server.

2. Desde el símbolo del sistema, navegue hasta el directorio donde copió el archivo de instalación.
3. Instalar el complemento:

```
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 especifica el puerto de comunicación HTTPS de SMCore.
- -DSERVER_IP especifica la dirección IP del servidor SnapCenter .
- -DSERVER_HTTPS_PORT especifica el puerto HTTPS del servidor SnapCenter .
- -DUSER_INSTALL_DIR especifica el directorio donde desea instalar el paquete de complementos de SnapCenter para Linux.
- DINSTALL_LOG_NAME especifica 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 /<directorio de instalación>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y luego agregue el parámetro PLUGINS_ENABLED = MySQL:3.0.
5. Agregue el host al servidor SnapCenter mediante el cmdlet Add-Smhost y los parámetros necesarios.

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 cmdlets del software SnapCenter"](#) .

Supervisar el estado de la instalación del complemento para MySQL

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado CA"](#).



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.

- c. Desplácese por la lista de campos y haga clic en **Huella digital**.
- d. Copia los caracteres hexadecimales del cuadro.
- e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:

- a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado recientemente instalado por el nombre del sujeto.

```
Get-ChildItem -Path Certificado:\LocalMachine\Mi
```

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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 CA para el servicio de complementos 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 por 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. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks  
. Cambie la contraseña de todos los alias de las entradas de clave  
privada en el almacén de claves a la misma contraseña utilizada para el  
almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar 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 agregar 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 /opt/NetApp/snapcenter/scc/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 de alias en el certificado de CA es largo y contiene
espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a
un nombre simple:
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configure el nombre de 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 en el archivo agent.properties contra la clave CRL_PATH.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Configurar el certificado CA para el servicio de complementos MySQL de SnapCenter 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 por 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 correspondiente a la clave *KEYSTORE_PASS*.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool con su ruta completa.

```
C:\Archivos de programa\Java\<versión_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves:

```
keytool -keypasswd -alias "nombre_alias_en_certificado" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe agregar 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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo *keystore.jks*.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 "nombre_de_alias_en_certificado_de_CA" -keystore keystore.jks
```

8. Configure el nombre de 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 para el certificado CA relacionado, consulte ["Cómo actualizar el archivo de lista de revocación de certificados en SnapCenter CA Certificate"](#).
- 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 en el archivo *agent.properties* contra la clave CRL_PATH.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede

obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Prepárese para la protección de datos

Requisitos previos para utilizar el complemento SnapCenter para MySQL

Antes de utilizar el complemento SnapCenter para MySQL, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter Server.
- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento y creando credenciales, si corresponde.
- Instale Java 11 en su host Linux o Windows.

Debe configurar la ruta de Java en la variable de ruta ambiental de la máquina host.

- Configure SnapMirror y SnapVault si desea replicación de respaldo.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger MySQL

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de copia de seguridad, clonación y restauración que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser instancias de MySQL que usted respalda o clona con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

- Las políticas especifican la frecuencia de las copias de seguridad, la replicación, los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede seleccionar una política cuando realiza una copia de seguridad a pedido para un solo recurso.

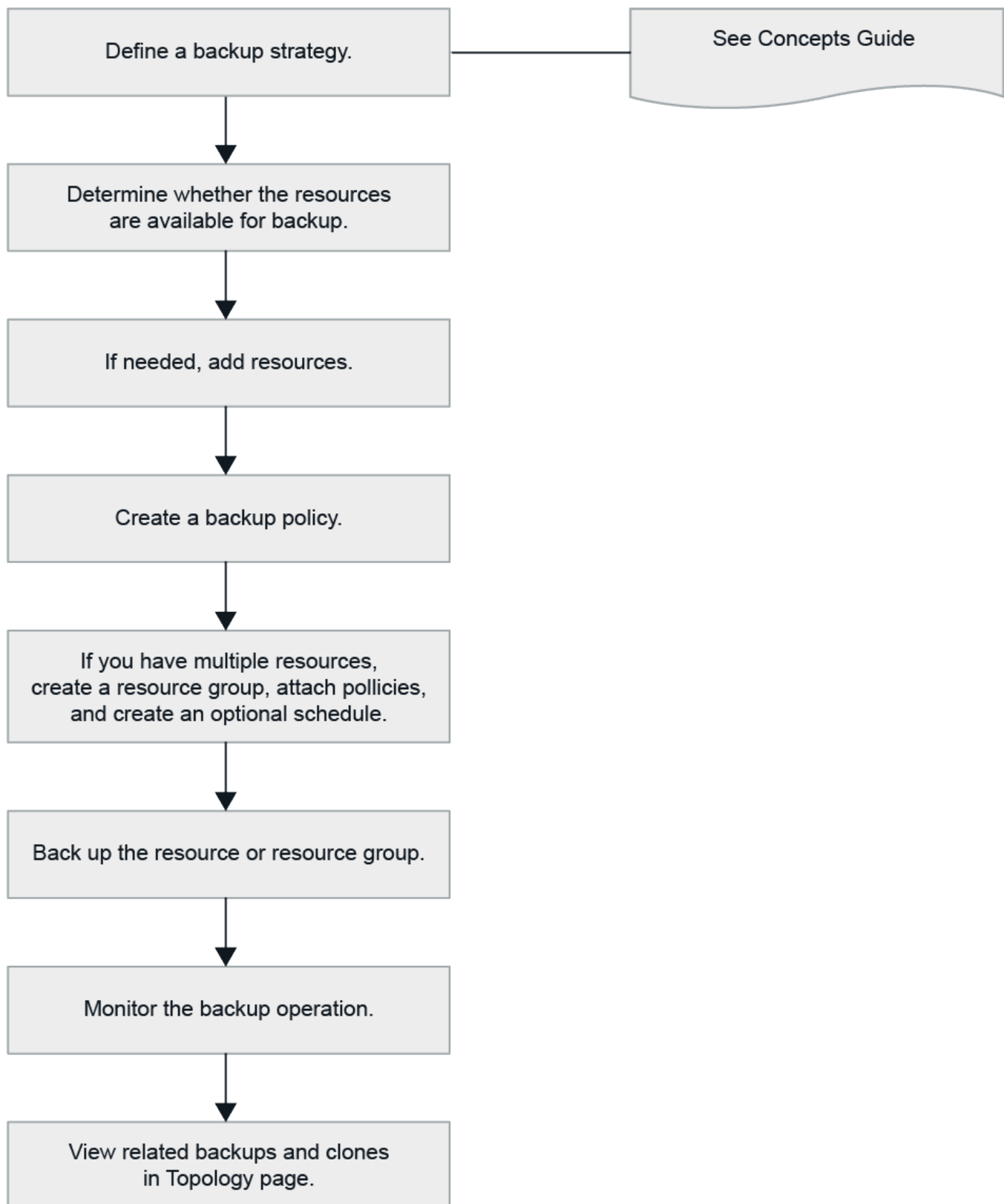
Piense en un grupo de recursos como si definiera lo que desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera cómo desea protegerla. Si está realizando una copia de seguridad de todas las bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos del host. Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Al crear el grupo de recursos y adjuntar las políticas, puede configurar el grupo de recursos para que realice una copia de seguridad completa diariamente.

Realizar copias de seguridad de los recursos de MySQL

Realizar copias de seguridad de los recursos de MySQL

Puede crear una copia de seguridad de un recurso (base de datos) o de un grupo de recursos. El flujo de trabajo de respaldo incluye la planificación, la identificación de las bases de datos para el respaldo, la administración de políticas de respaldo, la creación de grupos de recursos y la asociación de políticas, la creación de respaldos y el monitoreo de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen más información sobre los cmdlets de PowerShell. ["Guía de referencia de cmdlets del software SnapCenter"](#).

Descubra las bases de datos automáticamente

Los recursos son bases de datos MySQL en el host Linux que son administradas por SnapCenter. Puede agregar los recursos a los grupos de recursos para realizar operaciones de protección de datos después de descubrir las bases de datos MySQL que están disponibles.

Antes de empezar

- Ya debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y configurar las conexiones del sistema de almacenamiento.
- El complemento SnapCenter para MySQL no admite el descubrimiento automático de los recursos que residen en entornos virtuales RDM/VMDK. Debe proporcionar la información de almacenamiento para los entornos virtuales al agregar las bases de datos manualmente.

Acerca de esta tarea

- Después de instalar el complemento, todas las bases de datos de ese host Linux se descubren automáticamente y se muestran en la página Recursos.
- Sólo las bases de datos se descubren automáticamente.

Los recursos descubiertos automáticamente no se pueden modificar ni eliminar.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento para MySQL de la lista.
2. En la página Recursos, seleccione el tipo de recurso de la lista Ver.
3. (Opcional) Haga clic en  * y luego seleccione el nombre del host.

Luego puedes hacer clic en  * para cerrar el panel de filtro.

4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

Los recursos se muestran junto con información como el tipo de recurso, el nombre del host, los grupos de recursos asociados, el tipo de copia de seguridad, las políticas y el estado general.

- Si la base de datos está en un almacenamiento NetApp y no está protegida, se muestra No protegido en la columna Estado general.
- Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, y no se realiza ninguna operación de respaldo, se muestra Copia de seguridad no ejecutada en la columna Estado general. De lo contrario, el estado cambiará a Copia de seguridad fallida o Copia de seguridad exitosa según el último estado de la copia de seguridad.



Debe actualizar los recursos si las instancias cambian de nombre fuera de SnapCenter.

Agregar recursos manualmente al host del complemento

El descubrimiento automático no es compatible con el host Windows. Debe agregar instancias de MySQL y recursos de base de datos manualmente.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y configurar conexiones del sistema de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, seleccione el complemento SnapCenter para MySQL de la lista desplegable y luego haga clic en **Recursos**.
2. En la página Recursos, haga clic en **Agregar recursos MySQL**.
3. En la página Proporcionar detalles de recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Especifique el nombre de la base de datos.
Nombre del host	Introduzca el nombre del host.
Tipo	Seleccionar instancia.
Instancia	No aplicable.
Cartas credenciales	Seleccione las credenciales o agregue información para las credenciales. Esto es opcional.

4. En la página Proporcionar espacio de almacenamiento, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees, y luego haga clic en **Guardar**.

Opcional: Puede hacer clic en el *  * Icono para agregar más volúmenes, LUN y qtrees de otros sistemas de almacenamiento.

5. Opcional: en la página Configuración de recursos, ingrese pares clave-valor personalizados para el complemento MySQL.
6. Revise el resumen y luego haga clic en **Finalizar**.

Las bases de datos se muestran junto con información como el nombre del host, los grupos de recursos y políticas asociados y el estado general.

Si desea proporcionar a los usuarios acceso a los recursos, debe asignar los recursos a los usuarios. Esto permite a los usuarios realizar las acciones para las que tienen permiso en los activos que les están asignados.

["Agregar un usuario o grupo y asignarle roles y activos"](#)

Después de agregar las bases de datos, puede modificar los detalles de la base de datos MySQL.

Crear políticas de respaldo para MySQL

Antes de usar SnapCenter para realizar copias de seguridad de los recursos MySQL, debe crear una política de copia de seguridad para el recurso o grupo de recursos que

desea respaldar. Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad.

Antes de empezar

- Debes haber definido tu estrategia de backup.

Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para bases de datos MySQL.

- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar hosts, configurar conexiones del sistema de almacenamiento y agregar recursos.
- El administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino si está replicando instantáneas a un espejo o bóveda.

Además, puede especificar configuraciones de replicación, scripts y aplicaciones en la política. Estas opciones ahorran tiempo cuando desea reutilizar la política para otro grupo de recursos.

Acerca de esta tarea

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.
 - Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad de instantáneas mayor que la cantidad especificada 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.
5. En la página Tipo de política, 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 deba pasarse al complemento en formato de clave-valor.

Puede proporcionar varios valores clave para pasarlos al complemento.
6. En la página Instantánea y replicación, realice los siguientes pasos:
 - a. Especifique el tipo de programación seleccionando **A pedido**, **Por hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

- a. En la sección Configuración de instantáneas, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página **Tipo de copia de seguridad**:

Si quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.  Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva 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 subyacente de ONTAP .
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Si la relación de protección en ONTAP es de tipo Mirror and Vault y selecciona solo esta opción, las instantáneas creadas en el servidor principal no se transferirán al destino, pero aparecerán en él. Si se selecciona esta instantánea desde el destino para realizar una operación de restauración, se muestra el siguiente mensaje de error: La ubicación secundaria no está disponible para la copia de seguridad almacenada/duplicada seleccionada. Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Ver "Ver copias de seguridad y clones relacionados con los recursos de MySQL en la página Topología" .

Para este campo...	Haz esto...
Actualizar SnapVault después de crear una copia de instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault). Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón Actualizar en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre SnapLock Vault, consulte Confirmar instantáneas en WORM en un destino de bóveda Ver "Ver copias de seguridad y clones relacionados con los recursos de MySQL en la página Topología" .
Recuento de reintentos por error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

8. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados a una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.  El nombre del grupo de recursos no debe exceder los 250 caracteres.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desee utilizar para el nombre de la instantánea. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

4. En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

Esto ayuda a filtrar la información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. En la página Configuración de la aplicación, haga lo siguiente:

- a. Haga clic en la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación de instantánea del grupo de consistencia	Seleccione Urgente, Medio o Relajado para especificar el tiempo de espera para que se complete la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

+

- Haga clic en la flecha **Scripts** e ingrese los comandos pre y post para las operaciones de inactividad, instantánea y activación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
- Haga clic en la flecha **Configuraciones personalizadas** e ingrese los pares clave-valor personalizados necesarios para todas las operaciones de protección de datos que utilicen este recurso.

Parámetro	Valor	Descripción
HABILITAR REGISTRO DE ARCHIVO	(T/N)	Permite que la gestión del registro de archivo elimine los registros de archivo.

Parámetro	Valor	Descripción
RETENCIÓN DE REGISTRO DE ARCHIVO	número_de_días	Especifica el número de días que se conservan los registros de archivo. Esta configuración debe ser igual o mayor que NTAP_SNAPSHOT_RETENTIONS.
DIRECCIÓN DE REGISTRO DE ARCHIVO	directorio_de_información_de_cambio/registros	Especifica la ruta al directorio que contiene los registros de archivo.
EXTRACCIÓN DEL REGISTRO DE ARCHIVO	extensión_de_archivo	Especifica la longitud de la extensión del archivo de registro de archivo. Por ejemplo, si el registro de archivo es log_backup_0_0_0_0.1615185519429 y el valor de file_extension es 5, entonces la extensión del registro retendrá 5 dígitos, que es 16151.
ARCHIVO_REGISTRO_BÚSQUEDA_RECURSIVA ARCH	(T/N)	Permite la gestión de registros de archivo dentro de 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 complemento MySQL para Linux y no son compatibles con las bases de datos MySQL registradas como un complemento centralizado de Windows.

- c. Haga clic en la flecha **Herramienta de copia de instantáneas** para seleccionar la herramienta para crear instantáneas:

Si quieres...	Entonces...
SnapCenter para utilizar el complemento para Windows y poner el sistema de archivos en un estado consistente antes de crear una instantánea. Para los recursos de Linux, esta opción no es aplicable.	Seleccione * SnapCenter con consistencia del sistema de archivos*.

Si quieres...	Entonces...
SnapCenter para crear una instantánea de nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
Ingresar el comando que se ejecutará en el host para crear copias instantáneas.	Seleccione Otro y luego ingrese el comando que se ejecutará en el host para crear una instantánea.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

Las políticas se enumeran en la sección Configurar programaciones para políticas seleccionadas.

- b. En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna **Horarios aplicados**.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El servidor SMTP debe configurarse en **Configuración > Configuración global**.

9. Revise el resumen y luego haga clic en **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos MySQL en sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene

habilitada la capacidad **SecondaryProtection**.

- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:

- a. Seleccione el tipo de política de replicación.

 No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.

 SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.

 Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:

- a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
- b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
- c. En el cuadro de diálogo Agregar programaciones de verificación *policy_name*, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema

de almacenamiento secundario.

e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para MySQL

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar copias de seguridad, restaurar o clonar bases de datos MySQL.

Antes de empezar

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP 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 al sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una nueva credencial mediante el cmdlet Add-SmCredential.

Este ejemplo muestra cómo crear una nueva credencial llamada FinanceAdmin con credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. Agregue el host de comunicación MySQL al servidor SnapCenter .

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode mysql
```

5. Instale el paquete y el complemento 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. Establezca la ruta a SQLLIB.

Para Windows, el complemento MySQL utilizará la ruta predeterminada para la carpeta SQLLIB:
"C:\Program Files\IBM\SQLLIB\BIN"

Si desea anular la ruta predeterminada, utilice el siguiente comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
MySQL -configSettings @{ "MySQL_SQLLIB_CMD" =  
"<custom_path>\IBM\SQLLIB\BIN" }
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Realizar una copia de seguridad de MySQL

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Antes de empezar

- Debes haber creado una política de respaldo.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.
- Para la operación de copia de seguridad basada en instantáneas, asegúrese de que todas las bases de datos de los inquilinos sean válidas y activas.
- Para los comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Seleccionar ** y, a continuación, seleccione el nombre del host y el tipo de recurso para filtrar los recursos. Luego puedes seleccionar  para cerrar el panel de filtro.

3. Seleccione el recurso que desea respaldar.
4. En la página Recursos, seleccione **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Configuración de la aplicación, haga lo siguiente:
 - Seleccione la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia, si es necesario, y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación "Instantánea del grupo de consistencia"	Seleccione Urgente , Medio o Relajado para especificar el tiempo de espera para que finalice la operación de instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

- Seleccione la flecha **Scripts** para ejecutar comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo.

También puede ejecutar comandos previos antes de salir de la operación de copia de seguridad. Los prescriptos y posscripts se ejecutan en el servidor SnapCenter .

- Seleccione la flecha **Configuraciones personalizadas** y luego ingrese los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.
- Seleccione la flecha **Herramienta Copiar Instantánea** para seleccionar la herramienta para crear Instantáneas:

Si quieres...	Entonces...
SnapCenter para crear una instantánea a nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
SnapCenter para usar el complemento para Windows para poner el sistema de archivos en un estado consistente y luego crear una instantánea	Seleccione * SnapCenter con consistencia del sistema de archivos*.
Para ingresar el comando para crear una instantánea	Seleccione Otro y luego ingrese el comando para crear una instantánea.

6. En la página Políticas, realice los siguientes pasos:

- Seleccione una o más políticas de la lista desplegable.



También puedes crear una política haciendo clic en *  *.

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- Seleccionar *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.

policy_name es el nombre de la política que usted seleccionó.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en **Configuración > Configuración global**.

8. Revise el resumen y luego seleccione **Finalizar**.

Se muestra la página de topología de recursos.

9. Seleccione **Hacer copia de seguridad ahora**.

10. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

- En configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

Para obtener información, consulte: ["No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"](#)

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar.

Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese script, el comando `do_start method` inicia el servicio del complemento VMware de SnapCenter. Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

Se muestra la solicitud de nombre de usuario y contraseña.

2. Agregue 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 respaldo mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
5. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

Este ejemplo muestra cómo realizar una copia de seguridad 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 una copia de seguridad 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 del trabajo (en ejecución, completado o fallido) mediante el cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Supervise los detalles del trabajo de respaldo, como la identificación y el nombre del respaldo, para realizar una operación de restauración o clonación 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de grupos de recursos

Un grupo de recursos es una colección de recursos en un host. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio "snapmirror all". Sin embargo, si está utilizando el rol "vsadmin", entonces no se requiere el privilegio "snapmirror all".

Acerca de esta tarea

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o seleccionando  , y luego seleccionando la etiqueta. Luego puedes seleccionar  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 MySQL

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:

- a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en instancias de MySQL en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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 operaciones de copia de seguridad de MySQL

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter, los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de copia de seguridad.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	a. En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. b. Seleccione la operación y luego haga clic en Cancelar trabajo.
Panel de actividades	a. Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Ver copias de seguridad y clones de MySQL en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario.

Acerca de esta tarea

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .
-  muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .



La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página de topología del recurso seleccionado.

4. Revise la **tarjeta de resumen** para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario y secundario.

La sección **Tarjeta de resumen** muestra el número total de copias de seguridad basadas en instantáneas 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración de SnapLock más largo se recupera de ONTAP.

Después de realizar una copia de seguridad a pedido, al hacer clic en el botón **Actualizar** se actualizan los detalles de la copia de seguridad o la clonación.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

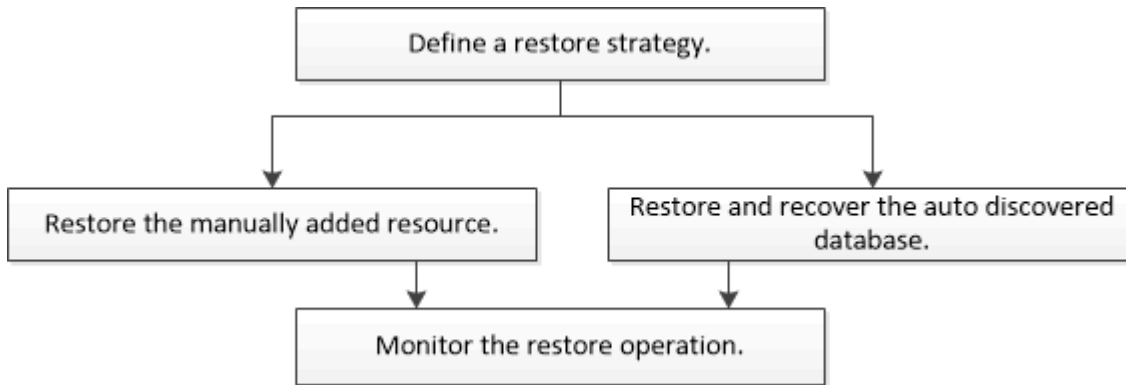
7. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en .
8. Si desea dividir un clon, seleccione el clon de la tabla y luego haga clic en .

Restaurar MySQL

Restaurar flujo de trabajo

El flujo de trabajo de restauración y recuperación incluye la planificación, la ejecución de las operaciones de restauración y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de restauración:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

["Guía de referencia de cmdlets del software SnapCenter"](#) .

Restaurar y recuperar una copia de seguridad de un recurso agregado manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



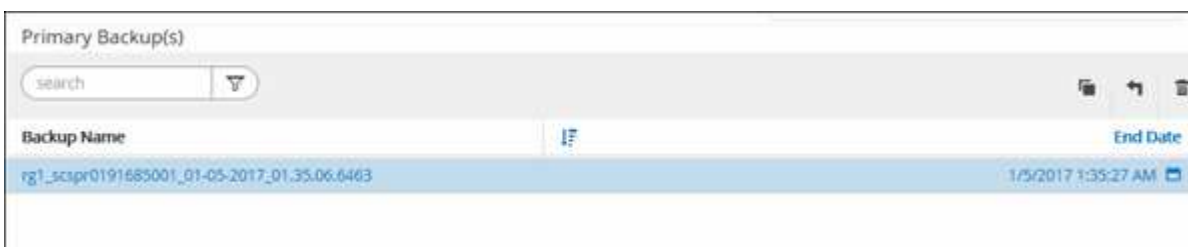
Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.



Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01:35:06.6463	1/5/2017 1:35:27 AM

6. En la página Restaurar alcance, seleccione **Recurso completo**.
 - 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 instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

Puede seleccionar varios LUN.



Si selecciona **Todos**, se restaurarán todos los archivos en los volúmenes, qtrees o LUN.

7. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no están disponibles para los recursos descubiertos automáticamente.

8. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no están disponibles para los recursos descubiertos automáticamente.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets Get-SmBackup y Get-SmBackupReport.

Este ejemplo muestra información sobre todas las copias de seguridad 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	

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet `Restore-SmBackup`.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar y recuperar una copia de seguridad de una base de datos descubierta automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de una o más copias de seguridad.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.
- Para los comandos de pre-restauración, post-restauración, montaje y desmontaje, debe verificar si los

comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:

- 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 los comandos no existen en la lista de comandos, la operación fallará.

Acerca de esta tarea

- Para los recursos descubiertos automáticamente, la restauración es compatible con SFSR.
- No se admite la recuperación automática en puntos específicos ni en momentos concretos.
- 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 izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con el tipo, el host, los grupos de recursos y políticas asociados y el estado.



Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra "No protegido" en la columna Estado general. Esto puede significar que el recurso no está protegido o que fue respaldado por un usuario diferente.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. En la página Restaurar ámbito, seleccione **Recurso completo** para restaurar los volúmenes de datos configurados de la base de datos MySQL.

7. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.

Los comandos de desmontaje no están disponibles para los recursos descubiertos automáticamente.

8. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.

Los comandos de montaje no están disponibles para los recursos descubiertos automáticamente.

9. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Restaurar recursos mediante cmdlets de PowerShell

Restaurar una copia de seguridad de un recurso incluye iniciar una sesión de conexión con el servidor SnapCenter , enumerar las copias de seguridad y recuperar información de las copias de seguridad, y restaurar una copia de seguridad.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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

Este ejemplo muestra información detallada sobre la copia de seguridad 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. Restaure datos de la copia de seguridad mediante el cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar las operaciones de restauración de MySQL

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso

-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Clonar copias de seguridad de recursos de MySQL

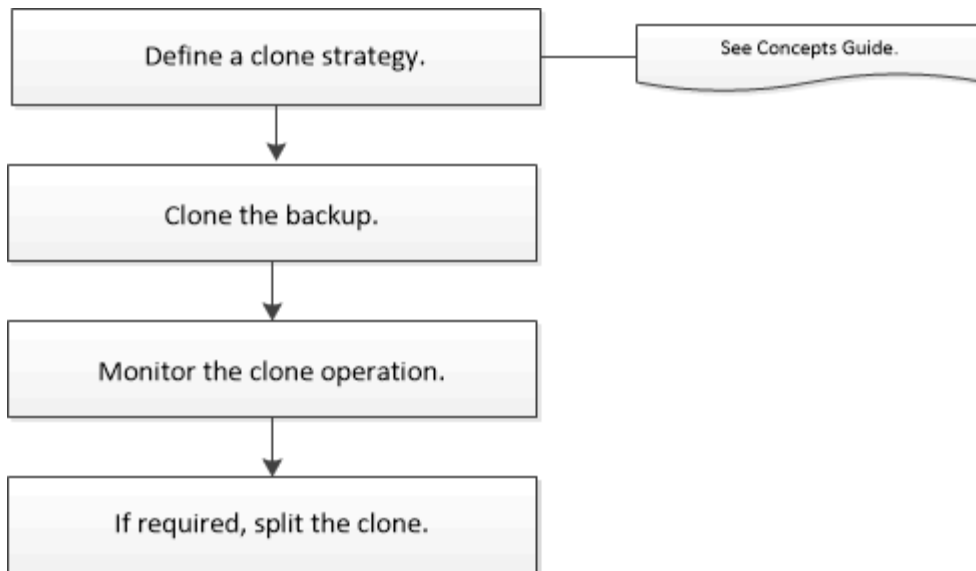
Flujo de trabajo de clonación

El flujo de trabajo de clonación incluye la realización de la operación de clonación y la supervisión de la operación.

Acerca de esta tarea

- Puedes clonar en el servidor MySQL de origen.
- Puede clonar copias de seguridad de recursos por los siguientes motivos:
 - Para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de recursos actuales durante los ciclos de desarrollo de aplicaciones
 - Para herramientas de extracción y manipulación de datos al rellenar almacenes de datos
 - Para recuperar datos que fueron borrados o modificados por error

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de clonación:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen información detallada sobre los cmdlets de PowerShell.

Clonar una copia de seguridad de MySQL

Puede utilizar SnapCenter para clonar una copia de seguridad. Puede clonar desde una copia de seguridad primaria o secundaria.

Antes de empezar

- Deberías haber realizado una copia de seguridad de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados que alojan los volúmenes estén en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Para los comandos previos o posteriores a la clonación, debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde las siguientes rutas:
 - 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 los comandos no existen en la lista de comandos, la operación fallará. * Para la versión MySQL 5.7, debe establecer IGNORE_MYSQLX_PORT = true (por defecto falso) en el archivo de propiedades MySQL.

Acerca de esta tarea

- No se pueden proteger las instancias MySQL clonadas.
- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["Dividir un volumen FlexClone de su volumen principal"] .
- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con información como el tipo, el host, los grupos de recursos y políticas asociados y el estado.

3. Seleccione el recurso o grupo de recursos.

Debe seleccionar un recurso si selecciona un grupo de recursos.

Se muestra la página de topología de recursos o grupos de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. Seleccione la copia de seguridad de datos de la tabla y luego haga clic en .
6. En la página Ubicación, realice las siguientes acciones:

Para este campo...	Haz esto...
Servidor clonado	Seleccione un host en el que se debe crear el clon.
Puerto	Proporcione el puerto en el que se iniciará la instancia MySQL clonada.
Dirección IP de exportación de NFS	Introduzca las direcciones IP o los nombres de host a los que se exportarán los volúmenes clonados.

7. En la página Scripts, realice los siguientes pasos:



Los scripts se ejecutan en el host del complemento.

- a. Introduzca los comandos para pre-clonar o post-clonar que deben ejecutarse antes o después de la operación de clonación, respectivamente.
 - Comando de preclonación: eliminar bases de datos existentes con el mismo nombre
 - Comando posterior a la clonación: verificar una base de datos o iniciar una base de datos.
- b. Introduzca el comando de montaje para montar un sistema de archivos en un host.

Comando de montaje para un volumen o qtree en una máquina Linux:

Ejemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

9. Revise el resumen y luego haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
PS C:\> Open-SmConnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. Recupere las copias de seguridad para realizar la operación de clonación mediante el cmdlet `Get-SmBackup`.

Este ejemplo muestra que hay dos copias de seguridad 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 clonación desde una copia de seguridad existente y especifique las direcciones IP de exportación NFS en las que se exportan los volúmenes clonados.

Este ejemplo muestra que la copia de seguridad 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_mysqlid_3306_scs000211748_0  
6-26-2024_06.08.35.4307" -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqlid_3306"}  
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```



Si no se especifica `NFSExportIPs`, el valor predeterminado se exporta al host de destino clonado.

4. Verifique que las copias de seguridad se hayan clonado correctamente utilizando el cmdlet `Get-SmCloneReport` para ver los detalles del trabajo de clonación.

Puede ver detalles como el ID del clon, la fecha y hora de inicio, 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          :
```

Supervisar las operaciones de clonación de MySQL

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone , consulte "[Dividir un volumen FlexClone de su volumen principal](#)".
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Eliminar o dividir clones de bases de datos MySQL después de actualizar SnapCenter

Después de actualizar a SnapCenter 4.3, ya no verá los clones. Puede eliminar el clon o dividir los clones desde la página Topología del recurso desde el cual se crearon los clones.

Acerca de esta tarea

Si desea localizar la huella de almacenamiento de los clones ocultos, ejecute el siguiente comando: `Get-SmClone -ListStorageFootprint`

Pasos

1. Elimine las copias de seguridad de los recursos clonados mediante el cmdlet `remove-smbbackup`.
2. Elimine el grupo de recursos de los recursos clonados mediante el cmdlet `remove-smresourcegroup`.
3. Elimine la protección del recurso clonado mediante el cmdlet `remove-smprotectresource`.
4. Seleccione el recurso principal en la página Recursos.

Se muestra la página de topología de recursos.

5. Desde la vista Administrar copias, seleccione los clones de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).

6. Seleccione los clones y luego haga clic  Para eliminar clones o hacer clic  Para dividir los clones.

7. Haga clic en **Aceptar**.

Proteja las aplicaciones mediante complementos compatibles con NetApp

Complementos compatibles con NetApp

Descripción general de los complementos compatibles con NetApp

Puede utilizar los complementos compatibles con NetApp , como MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB y el complemento de almacenamiento para las aplicaciones que utiliza y luego usar SnapCenter para realizar copias de seguridad, restaurar o clonar estas aplicaciones. Los complementos compatibles con NetApp actúan como componentes del lado del host del software NetApp SnapCenter , lo que permite la protección de datos y la gestión de recursos teniendo en cuenta las aplicaciones.

Cuando se instalan complementos compatibles con NetApp , puede usar SnapCenter con la tecnología NetApp SnapMirror para crear copias reflejadas de conjuntos de respaldo en otro volumen y usar la tecnología NetApp SnapVault para realizar la replicación de respaldo de disco a disco. Los complementos compatibles con NetApp se pueden utilizar en entornos Windows y Linux.



SnapCenterCLI no admite los comandos de complementos 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 complementos compatibles con NetApp desde la página Agregar host.

["Agregue hosts e instale paquetes de complementos en hosts remotos."](#)



La política de soporte de SnapCenter cubrirá el soporte para el marco del complemento, el motor principal y las API asociadas. El soporte no cubrirá el código fuente del complemento ni los scripts asociados creados en el marco del complemento.

Qué puede hacer con los complementos compatibles con NetApp

Puede utilizar los complementos compatibles con NetApp , como MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB y el complemento de almacenamiento para operaciones de protección de datos.

- Agregue recursos como bases de datos, instancias, documentos o espacios de tabla.
- Crear copias de seguridad.
- Restaurar desde copias de seguridad.
- Copias de seguridad clonadas.
- Programar operaciones de respaldo.
- Supervisar operaciones de copia de seguridad, restauración y clonación.
- Ver informes de operaciones de copia de seguridad, restauración y clonación.

Puede utilizar los complementos compatibles con NetApp para operaciones de protección de datos.

- Tome instantáneas del grupo de consistencia de los volúmenes de almacenamiento en los clústeres de ONTAP .
- Realice copias de seguridad de aplicaciones personalizadas mediante el marco de creación de scripts previos y posteriores integrado

Puede realizar una copia de seguridad de un volumen ONTAP , un LUN o un Qtree.

- Actualice las instantáneas tomadas en el servidor principal a un servidor secundario de ONTAP , aprovechando la relación de replicación existente (SnapVault/ SnapMirror/replicación unificada) mediante la política de SnapCenter

Los recursos primarios y secundarios de ONTAP pueden ser ONTAP FAS, AFF, ASA, ONTAP Select o Cloud Volumes ONTAP.

- Recupere el volumen ONTAP , LUN o archivos completos.

Debe proporcionar la ruta del archivo correspondiente manualmente, ya que las funciones de exploración o indexación no están integradas en el producto.

No se admite la restauración de Qtree ni de directorio, pero puede clonar y exportar solo el Qtree si el alcance de la copia de seguridad está definido en un nivel de Qtree.

Funciones de los complementos compatibles con NetApp

SnapCenter se integra con la aplicación complementaria y con las tecnologías NetApp en el sistema de almacenamiento. Para trabajar con complementos compatibles con NetApp , como MongoDB, ORASCPM (Aplicaciones Oracle), SAP ASE, SAP MaxDB y el complemento de almacenamiento, utilice la interfaz gráfica de usuario de SnapCenter .

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter proporciona estandarización y consistencia entre complementos y entornos. La interfaz de SnapCenter le permite completar operaciones consistentes de respaldo, restauración, recuperación y clonación en todos los complementos, utilizar informes centralizados, usar vistas de panel de un vistazo, configurar el control de acceso basado en roles (RBAC) y monitorear trabajos en todos los complementos.

- **Administración central automatizada**

Puede programar operaciones de respaldo, configurar la retención de respaldo basada en políticas y realizar operaciones de restauración. También puede supervisar su entorno de forma proactiva configurando SnapCenter para enviar alertas por correo electrónico.

- **Tecnología NetApp Snapshot sin interrupciones**

SnapCenter utiliza la tecnología NetApp Snapshot con los complementos compatibles con NetApp para realizar copias de seguridad de los recursos. Las instantáneas consumen un espacio de almacenamiento mínimo.

Los complementos compatibles con NetApp también ofrecen los siguientes beneficios:

- Compatibilidad con flujos de trabajo de copia de seguridad, restauración y clonación
- Seguridad respaldada por RBAC y delegación de roles centralizada

También puede configurar las credenciales para que los usuarios autorizados de SnapCenter tengan permisos a nivel de aplicación.

- Creación de copias puntuales y con uso eficiente del espacio de recursos para pruebas o extracción de datos mediante la tecnología NetApp FlexClone

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

- Compatibilidad con la función de instantánea del grupo de consistencia (CG) de ONTAP como parte de la creación de copias de seguridad.
- Capacidad de ejecutar múltiples copias de seguridad simultáneamente en múltiples hosts de recursos

En una sola operación, las instantáneas se consolidan cuando los recursos de un solo host comparten el mismo volumen.

- Capacidad de crear instantáneas mediante comandos externos.
- Capacidad para crear instantáneas consistentes con el sistema de archivos en entornos Windows.

Tipos de almacenamiento compatibles con los complementos de NetApp

SnapCenter admite una amplia gama de tipos de almacenamiento en máquinas físicas y virtuales. Debe verificar la compatibilidad con su tipo de almacenamiento antes de instalar complementos compatibles con NetApp .

Máquina	Tipo de almacenamiento
Montajes directos físicos y NFS en los hosts de VM (no se admiten VMDK ni LUN RDM).	LUN conectados a FC
Montajes directos físicos y NFS en los hosts de VM (no se admiten VMDK ni LUN RDM).	LUN conectados a iSCSI
Montajes directos físicos y NFS en los hosts de VM (no se admiten VMDK ni LUN RDM).	Volúmenes conectados a NFS
VMware ESXi	Almacenes de datos vVol tanto en NFS como en SAN El almacén de datos vVol solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP necesarios para el complemento compatible con NetApp

Los privilegios mínimos de ONTAP necesarios varían según los complementos de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: privilegios mínimos necesarios para ONTAP 9.12.1 y versiones posteriores
 - registro de soporte automático de generación de eventos
 - Mostrar historial laboral
 - parada de trabajo
 - Mostrar atributo lun
 - lun crear
 - eliminar lun
 - geometría lun
 - agregar igroup lun
 - crear igroup lun
 - eliminar igroup lun
 - Cambiar nombre de igroup lun
 - Programa de igroup de Lun
 - Asignación de LUN a nodos de informes adicionales
 - creación de mapeo LUN
 - eliminar mapeo lun
 - Mapeo de LUN: eliminar nodos de informes
 - espectáculo de mapeo de lun
 - modificar lun
 - volumen de movimiento de LUN
 - lun sin conexión
 - lun en línea
 - cambio de tamaño de lun
 - serie lun
 - espectáculo de almuerzo
 - interfaz de red
 - regla de adición de política de SnapMirror
 - regla de modificación de política de SnapMirror
 - regla de eliminación de política de SnapMirror
 - Mostrar política de Snapmirror
 - restauración de SnapMirror
 - espectáculo de Snapmirror
 - historial de programas de Snapmirror
 - actualización de SnapMirror
 - actualización-ls-set de snapmirror
 - Lista de destinos de Snapmirror
 - versión

- crear clon de volumen
- espectáculo de clonación de volumen
- inicio de división de clonación de volumen
- clonación de volumen división parada
- creación de volumen
- destrucción de volumen
- clonar archivo de volumen crear
- archivo de volumen mostrar-uso-de-disco
- volumen fuera de línea
- volumen en línea
- modificar volumen
- creación de qtree de volumen
- eliminar volumen qtree
- modificar volumen qtree
- espectáculo de qtree de volumen
- restricción de volumen
- espectáculo de volumen
- crear instantánea de volumen
- eliminar instantánea de volumen
- modificar instantánea de volumen
- cambio de nombre de instantánea de volumen
- restauración de instantánea de volumen
- archivo de restauración de instantánea de volumen
- Mostrar instantánea de volumen
- desmontar volumen
- CIFs de vserver
- creación de recurso compartido cifs de vserver
- Eliminar recurso compartido CIF de vserver
- Mostrar copia de sombra de CIF de vserver
- Mostrar el recurso compartido de cifs de vserver
- Mostrar cifs de vserver
- Crear política de exportación de vserver
- Eliminar política de exportación de vserver
- Crear regla de política de exportación de vserver
- Mostrar regla de política de exportación de vserver
- Mostrar política de exportación de vserver
- Mostrar conexión iscsi de vserver

- espectáculo vserver
- Comandos de solo lectura: privilegios mínimos necesarios para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red

Prepare los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para complementos compatibles con NetApp

Puede utilizar un complemento de SnapCenter con la tecnología ONTAP SnapMirror para crear copias reflejadas de conjuntos de copias de seguridad en otro volumen, y con la tecnología ONTAP SnapVault para realizar la replicación de copias de seguridad de disco a disco para el cumplimiento de estándares y otros fines relacionados con la gobernanza. Antes de realizar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y 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 ; no crean una programación ONTAP separada.



Si llega 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 del almacenamiento primario (el volumen de origen) al almacenamiento secundario (el volumen de destino). Cuando inicializa la relación, ONTAP transfiere los bloques de datos referenciados en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debes utilizar relaciones de abanico.

SnapCenter admite la gestión de relaciones SnapMirror con versiones flexibles. Para obtener detalles sobre las relaciones de SnapMirror con versiones flexibles y cómo configurarlas, consulte la ["Documentación de ONTAP"](#).

Definir una estrategia de backup

Definir una estrategia de respaldo antes de crear sus trabajos de respaldo le garantiza que tendrá los respaldos que necesita para restaurar o clonar sus recursos con éxito. Su acuerdo de nivel de servicio (SLA), su objetivo de tiempo de recuperación (RTO) y su objetivo de punto de recuperación (RPO) determinan en gran medida su estrategia de respaldo.

Acerca de esta tarea

Un SLA define el nivel de servicio que se espera y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RTO es el tiempo en el que se debe restaurar un proceso comercial después de una interrupción en el servicio. RPO define la estrategia para la edad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA, RTO y RPO contribuyen a la estrategia de protección de datos.

Pasos

1. Determina cuándo debes realizar copias de seguridad de tus recursos.

2. Decide cuántos trabajos de respaldo necesitas.
3. Decide cómo nombrar tus copias de seguridad.
4. Decida si desea instantáneas del grupo de consistencia y decida las opciones adecuadas para eliminarlas.
5. Decida si desea utilizar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
6. Determine el período de retención de las instantáneas en el sistema de almacenamiento de origen y el destino SnapMirror .
7. Determine si desea ejecutar algún comando antes o después de la operación de respaldo y proporcione un script previo o posterior.

Estrategia de respaldo para complementos compatibles con NetApp

Programaciones de respaldo de recursos de complementos compatibles con NetApp

El factor más crítico para determinar un cronograma de respaldo es la tasa de cambio del recurso. Cuanto más a menudo realice copias de seguridad de sus recursos, menos registros de archivo tendrá que utilizar SnapCenter para restaurar, lo que puede generar operaciones de restauración más rápidas.

Es posible que hagas una copia de seguridad de un recurso muy utilizado cada hora, mientras que es posible que hagas una copia de seguridad de un recurso poco utilizado una vez al día. Otros factores incluyen la importancia del recurso para su organización, su acuerdo de nivel de servicio (SLA) y su objetivo de punto de recuperación (RPO).

SLA define el nivel de servicio esperado y aborda muchas cuestiones relacionadas con el servicio, incluida la disponibilidad y el rendimiento del servicio. RPO define la estrategia para la edad de los archivos que deben recuperarse del almacenamiento de respaldo para que las operaciones normales se reanuden después de una falla. SLA y RPO contribuyen a la estrategia de protección de datos.

Los programas de respaldo constan de dos partes, como se indica a continuación:

- Frecuencia de respaldo

La frecuencia de copia de seguridad (con qué frecuencia se deben realizar las copias de seguridad), también llamada tipo de programación para algunos complementos, es parte de una configuración de política. Por ejemplo, puede configurar la frecuencia de la copia de seguridad como horaria, diaria, semanal o mensual. Puede acceder a las políticas en la GUI de SnapCenter haciendo clic en **Configuración > Políticas**.

- Programaciones de copias de seguridad

Las programaciones de copias de seguridad (exactamente cuándo se deben realizar las copias de seguridad) son parte de la configuración de un recurso o de un grupo de recursos. Por ejemplo, si tiene un grupo de recursos que tiene una política configurada para copias de seguridad semanales, puede configurar la programación para realizar copias de seguridad todos los jueves a las 10:00 p. m. Puede acceder a las programaciones del grupo de recursos en la GUI de SnapCenter haciendo clic en **Recursos**, luego seleccionando el complemento apropiado y haciendo clic en **Ver > Grupo de recursos**.

Número de trabajos de respaldo necesarios

Los factores que determinan la cantidad de trabajos de respaldo que necesita incluyen el tamaño del recurso, la cantidad de volúmenes utilizados, la tasa de cambio del recurso y su Acuerdo de Nivel de Servicio (SLA).

La cantidad de trabajos de respaldo que elija generalmente dependerá de la cantidad de volúmenes en los que coloque sus recursos. Por ejemplo, si coloca un grupo de recursos pequeños en un volumen y un recurso grande en otro volumen, puede crear un trabajo de respaldo para los recursos pequeños y un trabajo de respaldo para el recurso grande.

Tipos de estrategias de restauración compatibles con recursos de complementos compatibles con NetApp agregados manualmente

Debe definir una estrategia antes de poder realizar con éxito operaciones de restauración mediante SnapCenter. Hay dos tipos de estrategias de restauración para los recursos de complementos compatibles con NetApp agregados manualmente.



No es posible recuperar recursos de complementos compatibles con NetApp agregados manualmente.

Restauración completa de recursos

- Restaura todos los volúmenes, qtrees y LUN de un recurso



Si el recurso contiene volúmenes o qtrees, las instantáneas tomadas después de la instantánea seleccionada para restaurar en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

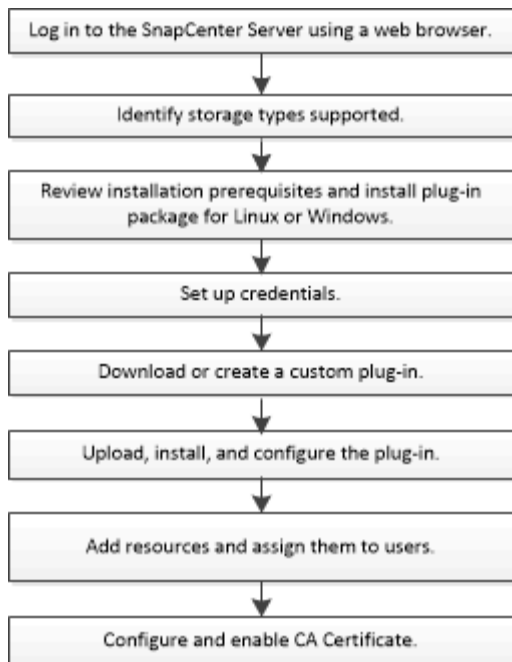
Restauración a nivel de archivo

- Restaura archivos de volúmenes, qtrees o directorios
- Restaura solo los LUN seleccionados

Prepárese para instalar los complementos compatibles con NetApp

Flujo de trabajo de instalación de complementos compatibles con SnapCenter NetApp

Debe instalar y configurar los complementos compatibles con NetApp de SnapCenter si desea proteger los recursos de NetApp complementos.



Requisitos previos para agregar hosts e instalar paquetes de complementos para Windows, Linux o AIX

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos. Los complementos compatibles con NetApp son compatibles con entornos Windows, Linux y AIX.



Las aplicaciones de almacenamiento y Oracle son compatibles con AIX.

- Debe tener instalado Java 11 en su host Linux, Windows o AIX.



IBM Java no es compatible con hosts Windows y Linux.

- Al instalar un complemento 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, Oracle Applications, SAP ASE, SAP MaxDB y el complemento de almacenamiento, deben estar disponibles en el host del cliente desde donde se realiza la operación de agregar host.

General

Si está utilizando iSCSI, el servicio iSCSI debería estar ejecutándose.

Hosts de Windows

- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Si administra nodos de clúster en SnapCenter, debe tener un usuario con privilegios administrativos para todos los nodos del clúster.
- Debe elegir manualmente el complemento SnapCenter para Microsoft Windows.

Hosts Linux y AIX



Las aplicaciones de almacenamiento y Oracle son compatibles con AIX.

- Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root.
- Debes tener instalado Java 11 en tu host Linux.

Si utiliza Windows Server 2019 o Windows Server 2016 para el host de SnapCenter Server, debe instalar Java 11. La herramienta Matriz de Interoperabilidad (IMT) contiene la información más reciente sobre los requisitos.

["Descargar JAVA para Linux"](#)

["Descargar JAVA para AIX"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Debe configurar privilegios de sudo para el usuario que no es root para proporcionar acceso a varias rutas. Agregue las siguientes líneas al archivo `/etc/sudoers` utilizando la utilidad `visudo` para Linux.



Asegúrese de estar utilizando la versión 1.8.7 o posterior de Sudo.

```
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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host AIX

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de complementos de SnapCenter para AIX.



Las aplicaciones de almacenamiento y Oracle son compatibles con AIX.



El complemento SnapCenter para UNIX, que forma parte del paquete de complementos SnapCenter para AIX, no admite grupos de volúmenes simultáneos.

Artículo	Requisitos
Sistemas operativos	AIX 7.1 o posterior
RAM mínima para el complemento SnapCenter en el host	4 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 IBM Java Si ha actualizado JAVA a la última versión, debe asegurarse de que la opción JAVA_HOME ubicada en <code>/var/opt/snapcenter/spl/etc/spl.properties</code> esté configurada en la versión de JAVA correcta y en la ruta correcta.

Para obtener la información más reciente sobre las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Configurar privilegios de sudo para usuarios no root para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no root instale el paquete de complementos de SnapCenter para AIX e inicie el proceso de complemento. Los procesos del complemento se ejecutarán como un usuario no root efectivo. Debe configurar privilegios de sudo para el usuario que no sea root para proporcionar acceso a varias rutas.

Lo que necesitarás

- Sudo versión 1.8.7 o posterior.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos del código de autenticación de mensajes: MAC hmac-sha2-256 y MAC 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

Debe configurar los privilegios de sudo para el usuario no root para proporcionar acceso a las siguientes rutas:

- `/inicio/USUARIO_AIX/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/instalación/complementos/desinstalar`
- `/ubicación_personalizada/ NetApp/snapcenter/spl/bin/spl`

Pasos

1. Inicie sesión en el host AIX en el que desea instalar el paquete de complementos de SnapCenter para AIX.
2. Agregue las siguientes líneas al archivo `/etc/sudoers` utilizando la utilidad visudo para 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/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si tiene una configuración RAC, junto con los 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 no root que usted creó.

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 SnapCenter Server está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si SnapCenter Server está instalado en el host Linux.



El ejemplo debe utilizarse únicamente como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	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 complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	5 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows. Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" . Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."

Requisitos de host para instalar el paquete de complementos de SnapCenter para Linux y AIX

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de complementos de SnapCenter para Linux o AIX.



Las aplicaciones de almacenamiento y Oracle son compatibles con AIX.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux • Servidor empresarial SUSE Linux (SLES)
RAM mínima para el complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 Oracle Java o OpenJDK Si ha actualizado JAVA a la última versión, 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 correcta.

Para obtener la información más reciente sobre las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#)

Configurar credenciales para complementos compatibles con NetApp

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en bases de datos o sistemas de archivos de Windows.

Antes de empezar

- Hosts Linux o AIX

Debe configurar credenciales para instalar complementos en hosts Linux o AIX.

Debe configurar las credenciales para el usuario root o para un usuario no root que tenga privilegios de sudo para instalar e iniciar el proceso del complemento.

Mejor práctica: Si bien se le permite crear credenciales para Linux después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

- Hosts de Windows

Debe configurar las credenciales de Windows antes de instalar complementos.

Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.

- Aplicaciones de complementos compatibles con NetApp

El complemento utiliza las credenciales que se seleccionan o crean al agregar un recurso. Si un recurso no requiere credenciales durante las operaciones de protección de datos, puede configurar las credenciales como **Ninguno**.

Acerca de esta tarea

Si configura 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 de respaldo al nombre de usuario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página **Credenciales**, especifique la información necesaria para configurar las credenciales:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. - Administrador del dominio o cualquier miembro del grupo de administradores Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son: <i>NetBIOS\Nombre de usuario</i> <i>Dominio FQDN\Nombre de usuario</i> - 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 donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es: <i>NombreDeUsuario</i>
Password	Introduzca la contraseña utilizada para la autenticación.
Tipo de autenticación	Seleccione el tipo de autenticación que desea utilizar.
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no sea root.  Aplicable únicamente a usuarios de Linux y AIX.

5. Haga clic en **Aceptar**.

Una vez que termine de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

Configurar gMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrada de grupo (gMSA) que proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

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 sea miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Cree y configure su gMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Añade objetos de computadora 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,...>  
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de  
servicio.
```

4. Configure el gMSA en sus hosts:
 - a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, 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 su host.
- b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
- c. Verifique su cuenta 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 .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

Instalar los complementos compatibles con NetApp

Agregar hosts e instalar paquetes de complementos en hosts remotos

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar los paquetes de complementos. Los complementos se instalan automáticamente en los hosts remotos. Puede agregar un host e instalar los paquetes de complementos para un host individual o para un clúster.

Antes de empezar

- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Debe asegurarse de que el servicio de cola de mensajes esté ejecutándose.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar una cuenta de servicio administrada grupal en Windows Server 2016 o posterior para aplicaciones personalizadas"](#)

- Para el host de Windows, debe asegurarse de seleccionar el complemento SnapCenter para Windows.

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .
- Si instala complementos en un clúster (WSFC), los complementos se instalan en todos los nodos del clúster.

Pasos

1. En el panel de navegación izquierdo, seleccione **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host: • Ventanas • Linux • AIX  Los complementos compatibles con NetApp se pueden utilizar en entornos Windows, Linux y AIX.  Las aplicaciones de almacenamiento y Oracle son compatibles con AIX.
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN. En entornos Windows, la dirección IP solo es compatible con hosts de dominio no confiables si se resuelve en el FQDN. Puede ingresar las direcciones IP o FQDN de un host independiente. Si está agregando un host mediante SnapCenter y el host es parte de un subdominio, debe proporcionar el FQDN.

Para este campo...	Haz esto...
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree credenciales nuevas. Las credenciales deben tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea instalar.

Puede instalar los siguientes complementos de la lista:

- MongoDB
- ORASCPM (mostrado como Aplicaciones Oracle)
- SAP ASE
- SAP MaxDB
- Almacenamiento

6. (Opcional) Seleccione **Más opciones** para instalar los otros complementos.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.

Para este campo...	Haz esto...
Ruta de instalación	Los complementos compatibles con NetApp se pueden instalar en un sistema Windows o en un sistema Linux. • Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es <code>C:\Program Files\NetApp\SnapCenter</code>. Opcionalmente, puedes personalizar la ruta. • Para el paquete de complementos de SnapCenter para Linux y el paquete de complementos de SnapCenter para AIX, la ruta predeterminada es <code>/opt/NetApp/snapcenter</code>. Opcionalmente, puedes personalizar la ruta.
Omitir comprobaciones de preinstalación	Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	Para el host de Windows, seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento.  Proporcione el nombre gMSA en el siguiente formato: <code>domainName\accountName\$</code>.  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.

7. Seleccione **Enviar**.

Si no ha seleccionado la casilla **Omitir comprobaciones previas**, se valida el host para verificar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell, la versión de .NET, la ubicación (para complementos de Windows) y la versión de Java (para complementos de Linux) se verifican según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando 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 digital y luego seleccione **Confirmar y Enviar**.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

Los archivos de registro específicos de la instalación se encuentran en `/custom_location/snapcenter/ registros`.

Instalar paquetes de complementos de SnapCenter para Linux, Windows o AIX en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de complementos de SnapCenter para Linux, Windows o AIX en varios hosts simultáneamente mediante el cmdlet de PowerShell `Install-SmHostPackage`.

Antes de empezar

El usuario que agrega un host debe tener derechos administrativos en el host.



Las aplicaciones de almacenamiento y Oracle son compatibles con AIX.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet `Open-SmConnection` y luego ingrese sus credenciales.
3. Instale el complemento en varios hosts utilizando el cmdlet `Install-SmHostPackage` y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Puede utilizar la opción `-skipprecheck` cuando haya instalado los complementos manualmente y no desee validar si el host cumple con los requisitos para instalar el complemento.

4. Introduzca sus credenciales para la instalación remota.

Instale los complementos compatibles con NetApp en hosts Linux mediante la interfaz de línea de comandos

Debe instalar los complementos compatibles con NetApp mediante la interfaz de usuario (UI) de SnapCenter . Si su entorno no permite la instalación remota del complemento desde la interfaz de usuario de SnapCenter , puede instalar los complementos compatibles con NetApp en modo consola o en modo silencioso mediante la interfaz de línea de comandos (CLI).

Pasos

1. Copie el archivo de instalación del paquete de complementos de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\ NetApp\ SnapCenter\Package Repository al host donde desea instalar los complementos compatibles con NetApp .

Puede acceder a esta ruta desde el host donde está instalado SnapCenter Server.

2. Desde el símbolo del sistema, navegue hasta el directorio donde copió el archivo de instalación.

3. Instalar el complemento:

```
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 especifica el puerto de comunicación HTTPS de SMCORE.
- -DSERVER_IP especifica la dirección IP del servidor SnapCenter .
- -DSERVER_HTTPS_PORT especifica el puerto HTTPS del servidor SnapCenter .
- -DUSER_INSTALL_DIR especifica el directorio donde desea instalar el paquete de complementos de SnapCenter para Linux.
- _DINSTALL_LOG_NAME especifica 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. Agregue el host al servidor SnapCenter mediante el cmdlet Add-Smhost y los parámetros necesarios.

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 cmdlets del software SnapCenter"](#) .

5. Inicie sesión en SnapCenter y cargue el complemento compatible con NetApp desde la interfaz de usuario o mediante cmdlets de PowerShell.

Puede cargar el complemento compatible con NetApp desde la interfaz de usuario consultando ["Agregar hosts e instalar paquetes de complementos en hosts remotos"](#) sección.

La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen más información sobre los cmdlets de PowerShell.

Supervisar el estado de instalación de los complementos compatibles con NetApp

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

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



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

Para obtener información sobre cómo generar un CSR, consulte ["Cómo generar un archivo CSR de certificado"](#)



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

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

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

En esta ventana del asistente...	Haz lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y luego haga clic en Siguiente .
Formato de archivo de importación	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en Siguiente .
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en Finalizar para iniciar la importación.



El certificado de importación debe incluirse junto 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 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 utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Huella digital**.
 - d. Copia los caracteres hexadecimales del cuadro.
 - e. Eliminar los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

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

Get-ChildItem -Path Certificado:\LocalMachine\Mi

- b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

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

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando 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
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando 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 CA para el servicio de complementos 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 por 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. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave
privada en el almacén de claves a la misma contraseña utilizada para el
almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *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. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar 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 agregar 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 /opt/NetApp/snapcenter/scc/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se

agregó al almacén de claves.

7. Cambie la contraseña de clave privada agregada 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 de alias en el certificado de CA es largo y contiene espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a un nombre simple:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure el nombre de 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 en el archivo `agent.properties` contra la clave `CRL_PATH`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Configurar el certificado CA para el servicio de complementos 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 por 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 correspondiente a la clave *KEYSTORE_PASS*.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool con su ruta completa.

```
C:\Archivos de programa\Java\<versión_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves:

```
keytool -keypasswd -alias "nombre_alias_en_certificado" -keystore keystore.jks
```

Actualice lo mismo para la clave *KEYSTORE_PASS* en el archivo *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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregar un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe agregar 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:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo *keystore.jks*.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado CA que tenga clave privada y pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados agregados en el almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada 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 "nombre_de_alias_en_certificado_de_CA" -keystore keystore.jks
```

8. Configure el nombre de 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 para el certificado CA relacionado, consulte ["Cómo actualizar el archivo de lista de revocación de certificados en SnapCenter CA Certificate"](#) .
- 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 en el archivo *agent.properties* contra la clave `CRL_PATH`.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Prepárese para la protección de datos

Requisitos previos para utilizar los complementos compatibles con NetApp

Antes de utilizar los complementos compatibles con SnapCenter NetApp, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter Server.

- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento y creando credenciales, si corresponde.
- Agregue hosts e instale y cargue los complementos.
- Si corresponde, instale Java 11 en el host del complemento.
- Si tiene varias rutas de datos (LIF) o una configuración 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 agregan a la política de exportación de almacenamiento NFS en la máquina virtual de almacenamiento (SVM) para los volúmenes clonados. Si desea tener una dirección IP específica o restringirla a un subconjunto de direcciones IP, ejecute la CLI `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 desea replicación de respaldo.
- Asegúrese de que el puerto 9090 no esté en uso en otra aplicación del host.

El puerto 9090 debe reservarse para el uso de complementos compatibles con NetApp, además de los demás puertos requeridos por SnapCenter.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger los recursos de complementos compatibles con NetApp

Antes de utilizar SnapCenter, es útil comprender los conceptos básicos relacionados con las operaciones de copia de seguridad, clonación y restauración que desea realizar. Interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos suelen ser bases de datos, sistemas de archivos de Windows o máquinas virtuales que usted respalda o clona con SnapCenter.
- Un grupo de recursos de SnapCenter es una colección de recursos en un host o clúster.

Cuando se realiza una operación en un grupo de recursos, dicha operación se realiza en los recursos definidos en el grupo de recursos según la programación que especifique para el grupo de recursos.

Puede realizar una copia de seguridad a pedido de un solo recurso o de un grupo de recursos. También puede realizar copias de seguridad programadas para recursos individuales y grupos de recursos.

- Las políticas especifican la frecuencia de las copias de seguridad, la retención de copias, la replicación, los scripts y otras características de las operaciones de protección de datos.

Cuando crea un grupo de recursos, selecciona una o más políticas para ese grupo. También puede seleccionar una política cuando realiza una copia de seguridad a pedido para un solo recurso.

Piense en un grupo de recursos como si definiera *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una política como si definiera *cómo* desea protegerla. Si está realizando una copia de seguridad de todas las bases de datos o de todos los sistemas de archivos de un host, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host.

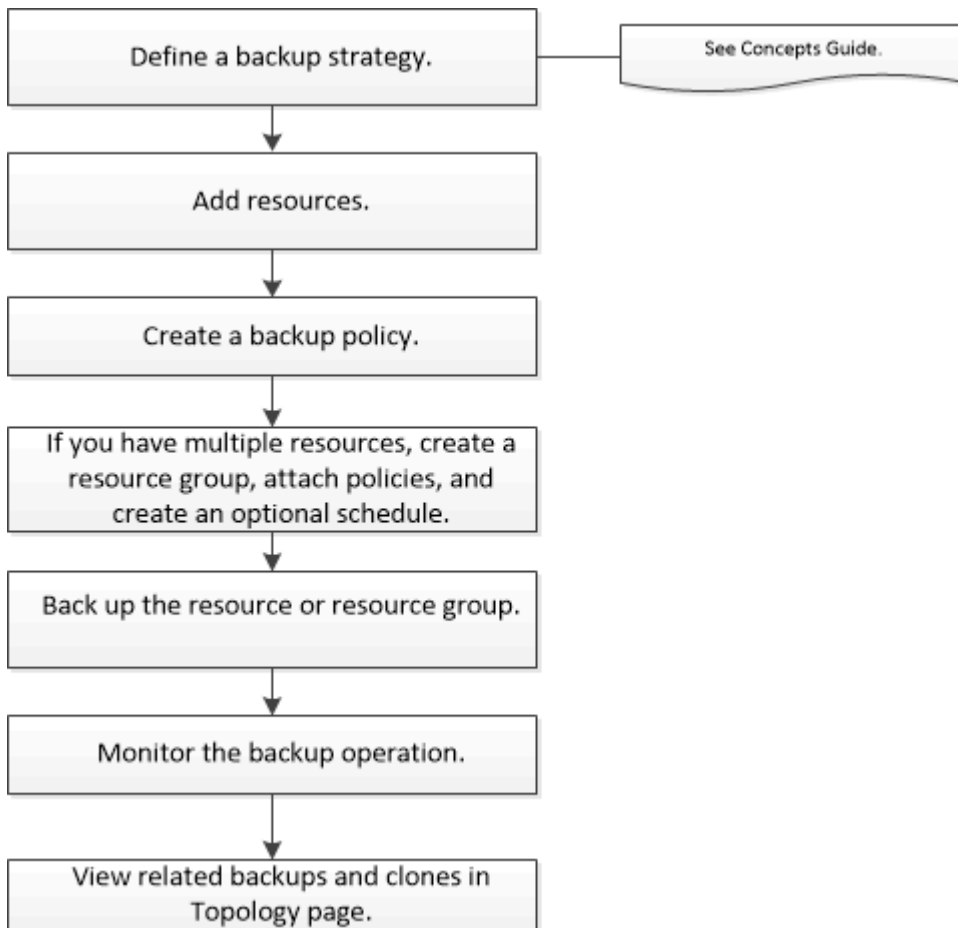
Luego, puede adjuntar dos políticas al grupo de recursos: una política diaria y una política por hora. Cuando crea el grupo de recursos y adjunta las políticas, puede configurar el grupo de recursos para realizar una copia de seguridad basada en archivos diariamente y otra programación que realice una copia de seguridad basada en instantáneas cada hora.

Realizar copias de seguridad de los recursos de complementos compatibles con NetApp

Realizar copias de seguridad de los recursos de complementos compatibles con NetApp

El flujo de trabajo de respaldo incluye la planificación, la identificación de los recursos para el respaldo, la administración de políticas de respaldo, la creación de grupos de recursos y la asociación de políticas, la creación de respaldos y la supervisión de las operaciones.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de copia de seguridad:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. Para obtener información detallada sobre los cmdlets de PowerShell, utilice la ayuda de cmdlets de SnapCenter o consulte la ["Guía de referencia de cmdlets del software SnapCenter"](#)

Agregar recursos a los complementos compatibles con NetApp

Debes agregar los recursos que deseas respaldar o clonar. Dependiendo de su entorno, los recursos pueden ser instancias de bases de datos o colecciones que desea respaldar o clonar.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts, crear conexiones del sistema de almacenamiento y agregar credenciales.
- Debes haber cargado los complementos en SnapCenter Server.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Agregar recurso**.
3. En la página Proporcionar detalles de recursos, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca el nombre del recurso.
Host name	Seleccione el host.
Tipo	Seleccione el tipo. El tipo lo define el usuario según el archivo de descripción del complemento. Por ejemplo, base de datos e instancia. En caso de que el tipo seleccionado tenga un padre, ingrese los detalles del padre. Por ejemplo, si el tipo es Base de datos y el padre es Instancia, ingrese los detalles de la Instancia.
Nombre de la credencial	Seleccione Credencial o cree una nueva credencial.
Senderos del monte	Introduzca las rutas de montaje donde se monta el recurso. Esto solo se aplica a un host de Windows.

4. En la página Proporcionar espacio de almacenamiento, seleccione un sistema de almacenamiento y elija uno o más volúmenes, LUN y qtrees, y luego seleccione **Guardar**.

Opcional: Seleccione el  Icono para agregar más volúmenes, LUN y qtrees de otros sistemas de almacenamiento.



Los complementos compatibles con NetApp no admiten la detección automática de recursos. Los detalles de almacenamiento de los entornos físicos y virtuales tampoco se descubren automáticamente. Debe proporcionar la información de almacenamiento para los entornos físicos y virtuales al crear los recursos.

5. En la página Configuración de recursos, proporcione pares clave-valor personalizados para el recurso.



Asegúrese de que el nombre de las claves personalizadas esté en mayúsculas.

Resource settings ⓘ

Name	Value
HOST	localhost
PORT	3306
MASTER_SLAVE	NO

Para conocer los parámetros del complemento correspondiente, consulte "[Parámetros para configurar el recurso](#)".

6. Revise el resumen y luego seleccione **Finalizar**.

Resultado

Los recursos se muestran junto con información como el tipo, el nombre del host o clúster, los grupos de recursos y políticas asociados y el estado general.



Debe 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 asignar activos a esos usuarios. Esto permite a los usuarios realizar las acciones para las que tienen permiso en los activos que les están asignados.

Después de agregar los recursos, puede modificar los detalles del recurso. Si un recurso de complementos compatibles con NetApp tiene copias de seguridad asociadas, no se pueden modificar los siguientes campos: nombre del recurso, tipo de recurso y nombre del host.

Parámetros para configurar el recurso

Si agrega los complementos manualmente, puede usar los siguientes parámetros para configurar el recurso en la página Configuración de recursos.

Complemento para MongoDB

Configuración de recursos:

- MONGODB_APP_SERVER=(para el tipo de recurso como clúster fragmentado) o MONGODB_REPLICASET_SERVER=(para el tipo de recurso como conjunto de réplicas)
- OPLOG_PATH=(Parámetro opcional en caso de que se proporcione desde el archivo MongoDB.properties)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN para autenticación LDAP y None para otras)

Debe proporcionar los siguientes parámetros en el archivo MongoDB.properties:

- DESACTIVAR_INICIO_DE_PARADA_SERVICIOS=
 - N si los servicios de inicio/parada los realiza el complemento.
 - Y si los servicios de inicio/**detención los realiza el usuario.
 - El parámetro opcional cuyo valor predeterminado se establece en N.
- OPLOG_PATH_= (Parámetro opcional en caso de que ya se proporcione como par clave-valor personalizado en SnapCenter).

Complemento para MaxDB

Configuración de recursos:

- XUSER_ENABLE (Y|N) habilita o deshabilita el uso de un xuser para MaxDB de modo que no se requiera una contraseña para el usuario de la base de datos.
- HANDLE_LOGWRITER (Y|N) ejecuta operaciones de suspensión del escritor de registro (N) o de reanudación del escritor de registro (Y).
- DBMCLICMD (path_to_dbmcli_cmd) especifica la ruta al comando dbmcli de MaxDB. Si no se configura, se utiliza dbmcli en la ruta de búsqueda.



Para el entorno de Windows, la ruta debe estar entre comillas dobles ("...").

- SQLCLICMD (path_to_sqlcli_cmd) especifica la ruta al comando sqlcli de MaxDB. Si no se establece la ruta, se utiliza sqlcli en la ruta de búsqueda.
- MAXDB_UPDATE_HIST_LOG (Y|N) indica al programa de respaldo de MaxDB si debe actualizar el registro del historial de MaxDB.
- MAXDB_CHECK_SNAPSHOT_DIR: Por ejemplo, SID1:directorio[,directorio...]; [SID2:directorio[,directorio...]] verifica que una operación de copia de instantánea de Snap Creator sea exitosa y garantiza que se cree la instantánea.

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 copia de seguridad de la base de datos se marca como Fallida en el historial de copias de seguridad.

- **MAXDB_BACKUP_TEMPLATES:** especifica una plantilla de respaldo para cada base de datos.

La plantilla debe existir y ser un tipo de plantilla de respaldo externa. Para habilitar la integración de instantáneas para MaxDB 7.8 y versiones posteriores, debe tener la funcionalidad de servidor en segundo plano MaxDB y una plantilla de respaldo MaxDB ya configurada del tipo EXTERNO.

- **MAXDB_BG_SERVER_PREFIX:** especifica el prefijo para el nombre del servidor de fondo.

Si se configura el parámetro MAXDB_BACKUP_TEMPLATES, también debe configurar el parámetro MAXDB_BG_SERVER_PREFIX. Si no establece el prefijo, se utiliza el valor predeterminado na_bg_.

Complemento para SAP ASE

Configuración de recursos:

- **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 bases de datos si se utiliza la construcción "ALL".

Puede especificar varias bases de datos utilizando 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.

Requerido para UNIX. Este parámetro es necesario si el usuario que ejecuta los comandos de inicio y detención del Agente Snap Creator (normalmente el usuario root) y el usuario que ejecuta el comando isql son diferentes.

- **SYBASE_TRAN_DUMP** db_name:directory_path le 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 requiera un volcado de transacción.

- **SYBASE_TRAN_DUMP_COMPRESS** (Y|N) habilita o deshabilita la compresión de volcado de transacciones nativa de Sybase.
- **SYBASE_ISQL_CMD** (por ejemplo, /opt/sybase/OCS-15_0/bin/isql) define la ruta al comando isql.
- **SYBASE_EXCLUDE_TEMPDB** (Y|N) le permite excluir automáticamente las bases de datos temporales creadas por el usuario.

Complemento para aplicaciones Oracle (ORASCPM)

Configuración de recursos:

- **SQLPLUS_CMD** especifica la ruta a SQLplus.
- **ORACLE_DATABASES** enumera las bases de datos Oracle que se respaldarán y el usuario correspondiente (database:usuario).
- **CNTL_FILE_BACKUP_DIR** especifica el directorio para la copia de seguridad del archivo de control.
- **ORA_TEMP** especifica el directorio para archivos temporales.
- **ORACLE_HOME** especifica el directorio donde está instalado el software de Oracle.

- ARCHIVE_LOG_ONLY especifica si se debe realizar una copia de seguridad de los registros de archivo o no.
- 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 volver a exportarse mientras se ejecuta `/bin/su <user running sqlplus> -c sqlplus /nolog <cmd>`. Este suele ser el caso 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 recursos de complementos compatibles con NetApp

Antes de usar SnapCenter para realizar copias de seguridad de recursos específicos del complemento compatible con NetApp, debe crear una política de copia de seguridad para el recurso o grupo de recursos que desea respaldar.

Antes de empezar

- Deberías haber definido tu estrategia de backup.

Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para los complementos compatibles con NetApp.

- Deberías estar preparado para la protección de datos.

La preparación para la protección de datos incluye tareas como instalar SnapCenter, agregar hosts, crear conexiones al sistema de almacenamiento y agregar recursos.

- Las máquinas virtuales de almacenamiento (SVM) deben asignarse a usted para operaciones de espejo o bóveda.

El administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino si está replicando instantáneas a un espejo o bóveda.

- Deberías haber agregado manualmente los recursos que deseas proteger.

Acerca de esta tarea

- Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad. Además, puede especificar configuraciones de replicación, scripts y aplicaciones.
- Especificar opciones en una política ahorra tiempo cuando desea reutilizar la política para otro grupo de recursos.
- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.
 - Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas que la cantidad especificada 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.



Las configuraciones principales de SnapLock se administran en la política de respaldo de SnapCenter y las configuraciones secundarias de SnapLock son administradas por ONTAP.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre y los detalles de la política.
5. En la página Tipo de política, 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 deba pasarse al complemento en formato de clave-valor.

Puede proporcionar varios valores clave para pasarlos al complemento.

6. En la página Instantánea y replicación, realice los siguientes pasos:
 - a. Especifique el tipo de programación seleccionando **A pedido**, **Por hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de copia de seguridad al crear un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de respaldo, pero le permite asignar diferentes programas de respaldo a cada política.



Si lo ha programado para las 2:00 a. m., el cronograma no se activará durante el horario de verano (DST).

- a. En la sección Configuración de instantáneas, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página **Tipo de copia de seguridad**:

Si quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.  Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva 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 subyacente de ONTAP .
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 **Seleccionar opciones de replicación secundaria**, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Si la relación de protección en ONTAP es de tipo Mirror and Vault y selecciona solo esta opción, las instantáneas creadas en el servidor principal no se transferirán al destino, pero aparecerán en él. Si se selecciona esta instantánea desde el destino para realizar una operación de restauración, se muestra el siguiente mensaje de error: La ubicación secundaria no está disponible para la copia de seguridad almacenada/duplicada seleccionada. Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Ver "Vea las copias de seguridad y clones relacionados con los recursos de complementos compatibles con NetApp en la página Topología".
Actualizar SnapVault después de crear una copia de instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault). Durante la replicación secundaria, el tiempo de expiración de SnapLock carga el tiempo de expiración de SnapLock principal. Al hacer clic en el botón Actualizar en la página Topología, se actualiza el tiempo de vencimiento de SnapLock primario y secundario que se recuperan de ONTAP. Cuando SnapLock está configurado solo en el secundario de ONTAP conocido como SnapLock Vault, al hacer clic en el botón Actualizar en la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP. Para obtener más información sobre SnapLock Vault, consulte Confirmar instantáneas en WORM en un destino de bóveda. Ver "Vea las copias de seguridad y clones relacionados con los recursos de complementos compatibles con NetApp en la página Topología".

Para este campo...	Haz esto...
Recuento de reintentos por error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario para evitar alcanzar el límite máximo de instantáneas en el almacenamiento secundario.

8. Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger. Le permite realizar una copia de seguridad de todos los datos asociados a una aplicación determinada simultáneamente. También debe adjuntar 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 luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione Nuevo grupo de recursos.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos. Nota: El nombre del grupo de recursos no debe exceder los 250 caracteres.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos. Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

Para este campo...	Haz esto...
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea. Por ejemplo, <i>customtext_resource group_policy_hostname</i> o <i>resource group_hostname</i>. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

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 ayuda a filtrar la información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y luego 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 Copias de seguridad para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación de instantánea del grupo de consistencia	Seleccione Urgente, Medio o Relajado para especificar el tiempo de espera para que se complete la operación de Instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

+

- a. Seleccione la flecha Scripts e ingrese los comandos pre y post para operaciones de inactividad, instantánea y desactivación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
- b. Seleccione la flecha Configuraciones personalizadas e ingrese los pares clave-valor personalizados necesarios para todas las operaciones de protección de datos que utilicen este recurso.

Parámetro	Valor	Descripción
HABILITAR REGISTRO DE ARCHIVO	(T/N)	Permite que la gestión del registro de archivo elimine los registros de archivo.
RETENCIÓN DE REGISTRO DE ARCHIVO	número_de_días	Especifica el número de días que se conservan los registros de archivo. Esta configuración debe ser igual o mayor que NTAP_SNAPSHOT_RETENTIONS.
DIRECCIÓN DE REGISTRO DE ARCHIVO	directorio_de_información_de_cambio/registros	Especifica la ruta al directorio que contiene los registros de archivo.

Parámetro	Valor	Descripción
EXTRACCIÓN DEL REGISTRO DE ARCHIVO	extensión_de_archivo	Especifica la longitud de la extensión del archivo de registro de archivo. Por ejemplo, si el registro de archivo es log_backup_0_0_0_0.161518551942 9 y el valor de file_extension es 5, entonces la extensión del registro retendrá 5 dígitos, que es 16151.
ARCHIVO_REGISTRO_BÚSQUEDA_RECURSIVA ARCH	(T/N)	Permite la gestión de registros de archivo dentro de subdirectorios. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

- c. Seleccione la flecha **Herramienta Copiar Instantánea** para seleccionar la herramienta para crear Instantáneas:

Si quieres...	Entonces...
SnapCenter para utilizar el complemento para Windows y poner el sistema de archivos en un estado consistente antes de crear una instantánea. Para los recursos de Linux, esta opción no es aplicable.	Seleccione * SnapCenter con consistencia del sistema de archivos*. Esta opción no es aplicable al complemento de SnapCenter para la base de datos SAP HANA.
SnapCenter para crear una instantánea de nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
Ingresar el comando que se ejecutará en el host para crear instantáneas.	Seleccione Otro y luego ingrese el comando que se ejecutará en el host para crear una instantánea.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puedes crear una política seleccionando *  *.

Las políticas se enumeran en la sección **Configurar programaciones para políticas seleccionadas**.

- b. En la columna **Configurar horarios**, seleccione *  * para la política que desea configurar.

- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y seleccione Aceptar.

Donde *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados. Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Desde la lista desplegable **Preferencias de correo electrónico** en la página **Notificación**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y del destinatario, y el asunto del correo electrónico. El servidor SMTP debe configurarse en **Configuración > Configuración global**.

9. Revise el resumen y luego seleccione **Finalizar**.

Cree grupos de recursos y habilite la protección secundaria para los recursos en los sistemas ASA r2

Debe crear el grupo de recursos para agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.
- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, `customtext_resource group_policy_hostname` o `resource group_hostname`. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:
 - a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la

SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:
 - a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.
 - b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.
 - c. En el cuadro de diálogo Agregar programaciones de verificación policy_name, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.
 - e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Cree una conexión al 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

- Debería 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 las instalaciones del complemento no estén en curso.

Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como "No disponible para respaldo" o "No en 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 diferentes clústeres. Cada sistema de almacenamiento compatible con SnapCenter debe tener un nombre único y una dirección IP LIF de administración única.

Pasos

1. Inicie una sesión de conexión de PowerShell Core mediante el cmdlet `Open-SmConnection`.

Este ejemplo abre una sesión de PowerShell:

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

2. Cree una nueva conexión al sistema de almacenamiento mediante el cmdlet `Add-SmStorageConnection`.

Este ejemplo crea una nueva conexión al sistema de almacenamiento:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una nueva credencial mediante el cmdlet `Add-SmCredential`.

Este ejemplo crea una nueva credencial llamada `FinanceAdmin` con credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Realizar copias de seguridad de recursos de complementos individuales compatibles con NetApp

Si un recurso de complementos compatibles con NetApp individual no es parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos. Puede realizar una copia de seguridad del recurso a pedido o, si el recurso tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Antes de empezar

- Debes haber creado una política de respaldo.
- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Hacer clic  y luego seleccione el nombre del host y el tipo de recurso para filtrar los recursos. Luego puedes hacer clic  para cerrar el panel de filtro.

3. Haga clic en el recurso del cual desea realizar una copia de seguridad.
4. En la página Recursos, si desea utilizar un nombre personalizado, seleccione la casilla de verificación **Usar formato de nombre personalizado para la copia de instantánea** y luego ingrese un formato de nombre personalizado para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

5. En la página Configuración de la aplicación, haga lo siguiente:
 - a. Haga clic en la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales:

Habilite la copia de seguridad del grupo de consistencia, si es necesario, y realice las siguientes tareas:

Para este campo...	Haz esto...
Dedique tiempo a esperar hasta que se complete la operación de instantánea del grupo de consistencia	Seleccione Urgente, Medio o Relajado para especificar el tiempo de espera para que se complete la operación de Instantánea. Urgente = 5 segundos, Medio = 7 segundos y Relajado = 20 segundos.
Deshabilitar la sincronización de WAFL	Seleccione esta opción para evitar forzar un punto de consistencia WAFL .

+

- a. Haga clic en la flecha **Scripts** para ejecutar comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo. También puede ejecutar comandos previos antes de salir de la operación de copia de seguridad.

Los prescriptos y posscripts se ejecutan en el servidor SnapCenter .

- b. Haga clic en la flecha **Configuraciones personalizadas** y luego ingrese 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 quieres...	Entonces...
SnapCenter para tomar una instantánea del nivel de almacenamiento	Seleccione * SnapCenter sin consistencia del sistema de archivos*.
SnapCenter para usar el complemento para Windows para poner el sistema de archivos en un estado consistente y luego tomar una instantánea	Seleccione * SnapCenter con consistencia del sistema de archivos*.
Para ingresar el comando para crear una instantánea	Seleccione Otro y luego ingrese el comando para crear una instantánea.

6. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas

seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en **Configuración > Configuración global**.

8. Revise el resumen y luego haga clic en **Finalizar**.

Se muestra la página de topología de recursos.

9. Haga clic en **Hacer copia de seguridad ahora**.

10. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet Open-SmConnection.

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

Se muestra la solicitud de nombre de usuario y contraseña.

2. Agregue recursos mediante el cmdlet Add-SmResources.

Este ejemplo agrega recursos:

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode  
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database  
-StorageFootPrint (  
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QTREE_NAME"="qtree  
Voll1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Cree una política de respaldo mediante el cmdlet Add-SmPolicy.

Este ejemplo crea una nueva política de respaldo:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'  
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Agregue un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

Este ejemplo 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.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dum  
myPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName"  
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'  
-usesnapcenterwithoutfilesystemconsistency
```

5. Inicie un nuevo trabajo de respaldo mediante el cmdlet New-SmBackup.

```
New-SMBackup -DatasetName  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy  
test2
```

6. Vea el estado del trabajo de respaldo mediante el cmdlet Get-SmBackupReport.

Este ejemplo muestra un informe de resumen de trabajos de todos los trabajos que se ejecutaron 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.sscore.test.com
```

Realizar copias de seguridad de grupos de recursos de complementos compatibles con NetApp

Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se realizan automáticamente según la programación.

Antes de empezar

- Debe haber creado un grupo de recursos con una política adjunta.

- Si desea realizar una copia de seguridad de un recurso que tiene una relación SnapMirror con un almacenamiento secundario, la función de ONTAP asignada al usuario de almacenamiento debe incluir el privilegio “snapmirror all”. Sin embargo, si está utilizando el rol “vsadmin”, entonces no se requiere el privilegio “snapmirror all”.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.

Puede buscar el grupo de recursos ingresando el nombre del grupo de recursos en el cuadro de búsqueda o haciendo clic en  y seleccionando la etiqueta. Luego puedes hacer clic  para cerrar el panel de filtro.

3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y haga clic en **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si ha asociado varias políticas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.
 - En configuraciones de MetroCluster , es posible que SnapCenter no pueda detectar una relación de protección después de una conmutación por error.

"No se puede detectar la relación entre SnapMirror o SnapVault después de una conmutación por error de MetroCluster"

- Si está realizando una copia de seguridad de los datos de la aplicación en VMDK y el tamaño del montón de Java para el SnapCenter Plug-in for VMware vSphere no es lo suficientemente grande, la copia de seguridad podría fallar. Para aumentar el tamaño del montón de Java, ubique el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese guión, el `do_start method` El comando inicia el servicio del complemento VMware de SnapCenter . Actualice ese comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M .`

Supervisar las operaciones de respaldo de recursos del complemento compatibles con NetApp

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso

-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.
 - d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Cancelar operaciones de copia de seguridad para complementos compatibles con NetApp

Puede cancelar operaciones de copia de seguridad que estén en cola.

Lo que necesitarás

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o desde el panel **Actividad**.
- No se puede cancelar una operación de copia de seguridad en ejecución.
- Puede utilizar la GUI de SnapCenter , los cmdlets de PowerShell o los comandos CLI para cancelar las operaciones de copia de seguridad.
- El botón **Cancelar trabajo** está deshabilitado para las operaciones que no se pueden cancelar.
- Si seleccionó **Todos los miembros de este rol pueden ver y operar en objetos de otros miembros** en la página Usuarios\Grupos al crear un rol, puede cancelar las operaciones de respaldo en cola de otros miembros mientras usan ese rol.

Pasos

1. Ejecute una de las siguientes acciones:

Desde...	Acción
Página de monitorización	- En el panel de navegación izquierdo, haga clic en Monitor > Trabajos. - Seleccione la operación y luego haga clic en Cancelar trabajo.
Panel de actividades	- Después de iniciar la operación de copia de seguridad, haga clic en ** en el panel Actividad para ver las cinco operaciones más recientes. - Seleccione la operación. - En la página Detalles del trabajo, haga clic en Cancelar trabajo.

La operación se cancela y el recurso vuelve al estado anterior.

Vea las copias de seguridad y clones relacionados con los recursos de complementos compatibles con NetApp en la página Topología

Cuando se prepara para realizar una copia de seguridad o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad y clones en el almacenamiento primario y secundario. En la página Topología, puede ver todas las copias de seguridad y clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad y clones y luego seleccionarlos para realizar operaciones de protección de datos.

Acerca de esta tarea

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

-  muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.
-  muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad del espejo en la vista de topología no incluye la copia de seguridad de versión flexible.



muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .

La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si ha creado 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad mostradas es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad del espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página de topología del recurso seleccionado.

4. Revise la tarjeta Resumen para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el recurso de la aplicación se distribuye en varios volúmenes, el tiempo de expiración de SnapLock para la copia de seguridad será el tiempo de expiración de SnapLock más largo configurado para una instantánea en un volumen. El tiempo de expiración de SnapLock más largo se recupera de ONTAP.

Después de realizar una copia de seguridad a pedido, al hacer clic en el botón **Actualizar** se actualizan los detalles de la copia de seguridad o la clonación.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación, cambio de nombre y eliminación.



No se puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el sistema de almacenamiento secundario.



No se puede cambiar el nombre de las copias de seguridad que están en el sistema de almacenamiento principal.

7. Si desea eliminar un clon, seleccione el clon de la tabla y haga clic en  para eliminar el clon.

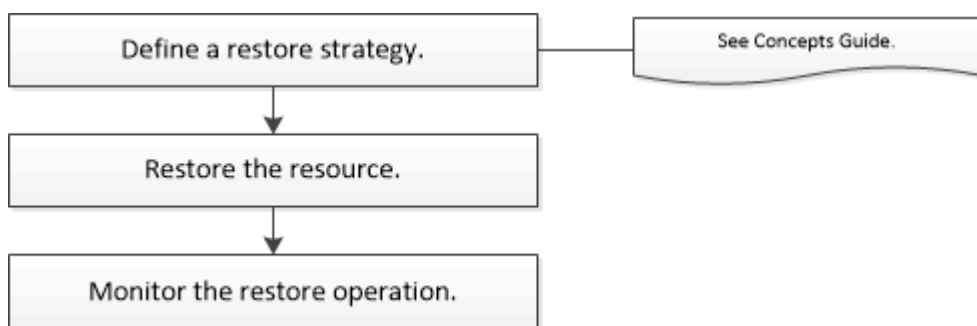
Restaurar recursos de complementos compatibles con NetApp

Restaurar recursos de complementos compatibles con NetApp

El flujo de trabajo de restauración y recuperación incluye la planificación, la ejecución de las operaciones de restauración y la supervisión de las operaciones.

Acerca de esta tarea

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de restauración:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. Para obtener información sobre los cmdlets de PowerShell, utilice la ayuda de cmdlets de SnapCenter o consulte la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Restaurar una copia de seguridad de recursos

Puede utilizar SnapCenter para restaurar recursos. Las capacidades de las operaciones de restauración dependen del complemento que utilice.

Antes de empezar

- Debes haber realizado una copia de seguridad del recurso o del grupo de recursos.
- El administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) tanto para los volúmenes de origen como para los de destino si está replicando instantáneas a un espejo o bóveda.
- Debe haber cancelado cualquier operación de respaldo que esté actualmente en curso para el recurso o grupo de recursos que desea restaurar.

Acerca de esta tarea

- La operación de restauración predeterminada solo restaura objetos de almacenamiento. Las operaciones de restauración a nivel de aplicación solo se pueden realizar si el complemento compatible con NetApp

proporciona esa capacidad.

- 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con información como el tipo, el nombre del host o clúster, los grupos de recursos y políticas asociados y el estado.



Aunque una copia de seguridad puede ser para un grupo de recursos, al restaurarla debe seleccionar los recursos individuales que desea restaurar.

Si el recurso no está protegido, se muestra *No protegido* en la columna **Estado general**.

El estado *No protegido* en la columna **Estado general** puede significar que el recurso no está protegido o que un usuario diferente realizó una copia de seguridad del recurso.

3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en

Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. En la página Restaurar alcance, seleccione **Recurso completo** o **Nivel de archivo**.

- a. Si seleccionó **Recurso completo**, se restaura la copia de seguridad del recurso.

Si el recurso contiene volúmenes o qtrees como huella de almacenamiento, las instantáneas más nuevas en dichos volúmenes o qtrees se eliminan y no se pueden recuperar. Además, si algún otro recurso está alojado en los mismos volúmenes o qtrees, ese recurso también se elimina.

- b. Si seleccionó **Nivel de archivo**, puede seleccionar **Todos**, o seleccionar volúmenes o qtrees y luego ingresar la ruta relacionada con los volúmenes o qtrees seleccionados, 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 **Todos**, se restaurarán todos los archivos en los volúmenes, qtrees o LUN.

7. En la página **Operaciones previas**, ingrese los comandos de restauración previa y de desmontaje

para ejecutar antes de realizar un trabajo de restauración.

8. En la página **Operaciones posteriores**, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.
9. En la página **Notificación**, de la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración global**.

10. Revise el resumen y luego haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

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

2. Recupere la información sobre una o más copias de seguridad que desee restaurar mediante los cmdlets `Get-SmBackup` y `Get-SmBackupReport`.

Este ejemplo muestra información sobre todas las copias de seguridad 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			

Este ejemplo muestra información detallada sobre la copia de seguridad del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "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. Restaure datos de la copia de seguridad mediante el cmdlet `Restore-SmBackup`.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Supervisar las operaciones de restauración de recursos del complemento compatible con NetApp

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Copias de seguridad de recursos de complementos compatibles con Clonar NetApp

Copias de seguridad de recursos de complementos compatibles con Clonar NetApp

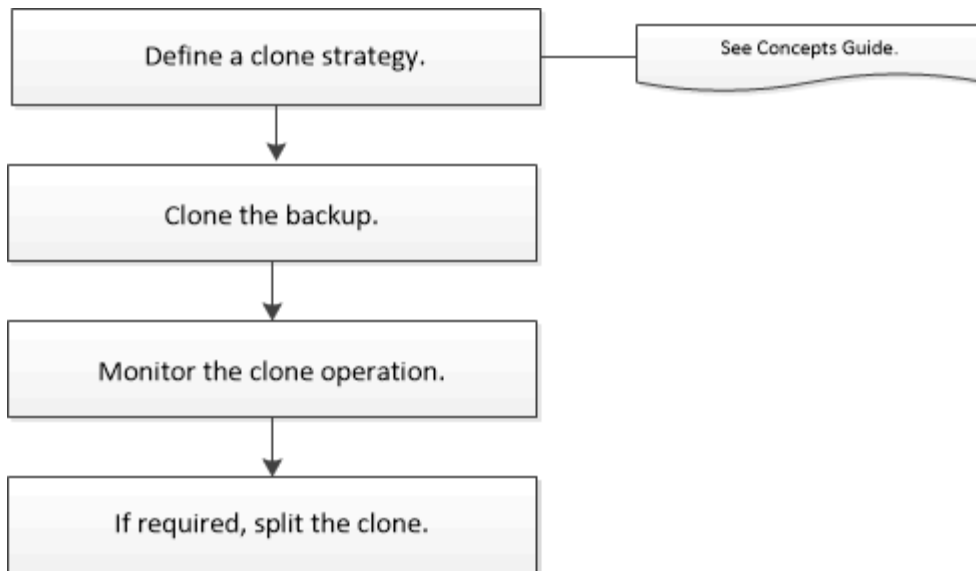
El flujo de trabajo de clonación incluye la realización de la operación de clonación y la supervisión de la operación.

Acerca de esta tarea

Puede clonar copias de seguridad de recursos por los siguientes motivos:

- Para probar la funcionalidad que debe implementarse utilizando la estructura y el contenido de recursos actuales durante los ciclos de desarrollo de aplicaciones
- Para herramientas de extracción y manipulación de datos al rellenar almacenes de datos
- Para recuperar datos que fueron borrados o modificados por error

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar la operación de clonación:



También puede utilizar cmdlets de PowerShell manualmente o en scripts para realizar operaciones de copia de seguridad, restauración y clonación. Para obtener información detallada sobre los cmdlets de PowerShell, utilice la ayuda de cmdlets de SnapCenter o consulte la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Clonar desde una copia de seguridad

Puede utilizar SnapCenter para clonar una copia de seguridad. Puede clonar desde una copia de seguridad primaria o secundaria. Las capacidades de las operaciones de clonación dependen del complemento que utilice.

Antes de empezar

- Debes haber realizado una copia de seguridad de los recursos o del grupo de recursos.
- La operación de clonación predeterminada solo clona objetos de almacenamiento. Las operaciones de clonación a nivel de aplicación solo se pueden realizar si el complemento compatible con NetApp proporciona esa capacidad.
- Debe asegurarse de que los agregados que alojan los volúmenes estén 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 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 .

Interfaz de usuario de SnapCenter

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.

Los recursos se muestran junto con información como el tipo, el nombre del host o clúster, los grupos de recursos y políticas asociados y el estado.

3. Seleccione el recurso o grupo de recursos.

Debe seleccionar un recurso si selecciona un grupo de recursos.

Se muestra la página de topología de recursos o grupos de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. Seleccione la copia de seguridad de datos de la tabla y luego haga clic en  .
6. En la página Ubicaciones, realice lo siguiente:

Para este campo...	Haz esto...
Servidor clonado	De forma predeterminada, se completa el host de origen. Si desea especificar un host diferente, seleccione el host en el que se debe montar el clon y se instala el complemento.
Sufijo de clonación	Esto es obligatorio cuando el destino del clon es el mismo que el origen. Introduzca un sufijo que se agregará al nombre del recurso recién clonado. El sufijo garantiza que el recurso clonado sea único en el host. Por ejemplo, rs1_clone. Si está clonando en el mismo host que el recurso original, debe proporcionar un sufijo para diferenciar el recurso clonado del recurso original; de lo contrario, la operación falla.

Si el recurso seleccionado es un LUN y está clonando desde una copia de seguridad secundaria, se enumeran los volúmenes de destino. Una sola fuente puede tener múltiples volúmenes de destino.

7. En la página **Configuración**, realice lo siguiente:

Para este campo...	Haz esto...
Nombre del iniciador	Introduzca el nombre del iniciador del host, que es un IQDN o WWPN.
Protocolo de grupo I	Seleccione el protocolo Igroup.



La página de configuración se muestra solo si el tipo de almacenamiento es LUN.

- En la página **Scripts**, ingrese los comandos para la clonación previa o posterior que deben ejecutarse antes o después de la operación de clonación, respectivamente. Introduzca el comando de montaje para montar un sistema de archivos en un host.

Por ejemplo:

- Comando de preclonación: eliminar bases de datos existentes con el mismo nombre
- Comando posterior a la clonación: verificar una base de datos o iniciar una base de datos.

Comando de montaje para un volumen o qtree en una máquina Linux:
`mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>`

- En la página **Notificación**, de la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico.

- Revise el resumen y haga clic en **Finalizar**.
- Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Cmdlets de PowerShell

Pasos

- Inicie una sesión de conexión con el servidor SnapCenter para un usuario específico mediante el cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- Enumere las copias de seguridad que se pueden clonar mediante el cmdlet `Get-SmBackup` o `Get-SmResourceGroup`.

Este ejemplo muestra información sobre todas las copias de seguridad 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			

Este ejemplo muestra información sobre un grupo de recursos específico:

```
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                   : {}
HostResourceMapping        : {}
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 clonación desde un grupo de recursos de clonación o una copia de seguridad existente utilizando el cmdlet `New-SmClone`.

Este ejemplo crea un clon a partir de una copia de seguridad especificada 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. Vea el estado del trabajo de clonación mediante el cmdlet `Get-SmCloneReport`.

Este ejemplo muestra un informe clonado para el ID de trabajo especificado:

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId         : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources      : {Don, Betty, Bobby, Sally}
ClonedResources      : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError           :
```

Supervisar las operaciones de clonación de recursos del complemento compatibles con NetApp

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.

2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.
4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Proteger los sistemas de archivos Unix

Qué puede hacer con el complemento SnapCenter para sistemas de archivos Unix

Cuando el complemento para sistemas de archivos Unix está instalado en su entorno, puede usar SnapCenter para realizar copias de seguridad, restaurar y clonar sistemas de archivos Unix. También puede realizar tareas que respalden dichas operaciones.

- Descubra recursos
- Realizar copias de seguridad de los sistemas de archivos Unix
- Programar operaciones de respaldo
- Restaurar copias de seguridad del sistema de archivos
- Copias de seguridad del sistema de archivos clonado
- Supervisar operaciones de copia de seguridad, restauración y clonación

Configuraciones compatibles

Artículo	Configuración compatible
Entornos	• Servidor físico • Servidor virtual Almacenes de datos vVol tanto en NFS como en SAN. Los almacenes de datos vVol solo se pueden aprovisionar con ONTAP Tools para VMware vSphere.
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux • Servidor empresarial SUSE Linux (SLES)
Sistemas de archivos	• SAN: ◦ Sistemas de archivos basados en LVM y no basados en LVM ◦ LVM sobre VMDK ext3, ext4 y xfs • NFS: NFS v3, NFS v4.x
Protocolos	• FC • FCoE • iSCSI • Sistema Nacional de Archivos

Artículo	Configuración compatible
Multitrayecto	Sí

Limitaciones

- No se admite la combinación de RDM y discos virtuales en un grupo de volúmenes.
- No se admite la restauración a nivel de archivo.

Sin embargo, puede realizar manualmente una restauración a nivel de archivo clonando la copia de seguridad y luego copiando los archivos manualmente.

- No se admite la combinación de sistemas de archivos distribuidos en VMDK que provienen de almacenes de datos NFS y VMFS.
- NVMe no es compatible.
- No se admite el aprovisionamiento.

Funciones

- Permite que el complemento para Oracle Database realice operaciones de protección de datos en bases de datos Oracle mediante el manejo de la pila de almacenamiento del host subyacente en sistemas Linux o AIX
- Admite protocolos de sistema de archivos de red (NFS) y red de área de almacenamiento (SAN) en un sistema de almacenamiento que ejecuta ONTAP.
- Para los sistemas Linux, se admiten bases de datos Oracle en LUN VMDK y RDM cuando implementa el SnapCenter Plug-in for VMware vSphere y registra el complemento con SnapCenter.
- Admite Mount Guard para AIX en sistemas de archivos SAN y diseño LVM.
- Admite el sistema de archivos con registro mejorado (JFS2) con registro en línea en sistemas de archivos SAN y diseño LVM solo para sistemas AIX.

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

- Automatiza operaciones de copia de seguridad, restauración y clonación teniendo en cuenta las aplicaciones para sistemas de archivos UNIX en su entorno SnapCenter

Instalar el complemento SnapCenter para sistemas de archivos Unix

Requisitos previos para agregar hosts e instalar el paquete de complementos para Linux

Antes de agregar un host e instalar el paquete de complementos para Linux, debe completar todos los requisitos.

- Si está utilizando iSCSI, el servicio iSCSI debe estar ejecutándose.
- Puede utilizar la autenticación basada en contraseña para el usuario root o no root o la autenticación basada en clave SSH.

El complemento SnapCenter para sistemas de archivos Unix puede ser instalado por un usuario que no sea root. Sin embargo, debe configurar los privilegios de sudo para que el usuario no root pueda instalar e iniciar el proceso del complemento. Después de instalar el complemento, los procesos se ejecutarán como un usuario no root efectivo.

- Cree credenciales con modo de autenticación como Linux para el usuario de instalación.
- Debes tener instalado Java 11 en tu 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 el shell predeterminado para la instalación del complemento.

Requisitos del host Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de complementos de SnapCenter para Linux.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux • Servidor empresarial SUSE Linux (SLES)
RAM mínima para el complemento SnapCenter en el host	2 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB  Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.

Artículo	Requisitos
Paquetes de software necesarios	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 última versión, 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 correcta.

Para obtener la información más reciente sobre las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Agregar hosts e instalar el paquete de complementos para Linux mediante GUI

Puede utilizar la página Agregar host para agregar hosts y luego instalar el paquete de complementos de SnapCenter para Linux. Los complementos se instalan automáticamente en los hosts remotos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo...	Haz esto...
Tipo de host	Seleccione Linux como tipo de host.
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN. Si está agregando un host mediante SnapCenter y el host es parte de un subdominio, debe proporcionar el FQDN.

Para este campo...	Haz esto...
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó.  El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección Seleccionar complementos para instalar, seleccione **Sistemas de archivos Unix**.

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	Mantenga 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 instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.
Ruta de instalación	La ruta predeterminada es <code>/opt/NetApp/snapcenter</code>. Opcionalmente puedes personalizar la ruta. Si utiliza la ruta personalizada, asegúrese de que el contenido predeterminado de los sudoers se actualice con la ruta personalizada.
Omitir comprobaciones de preinstalación opcionales	Seleccione esta casilla de verificación si ya ha instalado los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla de verificación Omitir comprobaciones previas, se valida el host para verificar si cumple con los requisitos para instalar el complemento.



El script de verificación previa no valida el estado del firewall del puerto del complemento si está especificado en las reglas de rechazo del firewall.

Se muestran mensajes de error o advertencia apropiados si no se cumplen los requisitos mínimos. 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, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Verifique la huella digital y luego haga clic en **Confirmar y enviar**.



SnapCenter no admite el algoritmo ECDSA.



La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

Los archivos de registro específicos de la instalación se encuentran en */custom_location/snapcenter/logs*.

Resultado

Todos los sistemas de archivos montados en el host se descubren automáticamente y se muestran en la página Recursos. Si no se muestra nada, haga clic en **Actualizar recursos**.

Supervisar el estado de la instalación

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
 - a. Haga clic en **Filtro**.
 - b. Opcional: especifique la fecha de inicio y finalización.
 - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
 - d. En el menú desplegable Estado, seleccione el estado de la 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 el servicio de Loader de complementos de SnapCenter

El servicio SnapCenter Plug-in Loader carga el paquete de complementos para Linux para interactuar con el servidor SnapCenter. El servicio SnapCenter Plug-in Loader se instala cuando instala el paquete de complementos de SnapCenter para Linux.

Acerca de esta tarea

Después de instalar el paquete de complementos de SnapCenter para Linux, el servicio SnapCenter Plug-in Loader se inicia automáticamente. Si el servicio SnapCenter Plug-in Loader no se inicia automáticamente, debe:

- Asegúrese de que el directorio donde está funcionando el complemento no se elimine
- Aumentar el espacio de memoria asignado a la máquina virtual Java

El archivo `spl.properties`, que se encuentra en `/custom_location/NetApp/snapcenter/spl/etc/`, contiene los siguientes parámetros. A estos parámetros se les asignan valores predeterminados.

Nombre del parámetro	Descripción
NIVEL DE REGISTRO	Muestra los niveles de registro admitidos. Los valores posibles son TRACE, DEBUG, INFO, WARN, ERROR y FATAL.
PROTOCOLO SPL	Muestra el protocolo compatible con SnapCenter Plug-in Loader. Sólo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.
PROTOCOLO DEL SERVIDOR SNAPCENTER	Muestra el protocolo compatible con SnapCenter Server. Sólo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.

Nombre del parámetro	Descripción
SALTAR ACTUALIZACIÓN DE JAVAHOME	De forma predeterminada, el servicio SPL detecta la ruta de Java y actualiza el parámetro JAVA_HOME. Por lo tanto, el valor predeterminado se establece en FALSO. Puede establecerlo en VERDADERO si desea deshabilitar el comportamiento predeterminado y corregir manualmente la ruta de Java.
CONTRASEÑA DEL ALMACÉN DE LLAVES SPL	Muestra la contraseña del archivo del almacén de claves. Puede cambiar este valor solo si cambia la contraseña o crea un nuevo archivo de almacén de claves.
SPL_PORT	Muestra el número de puerto en el que se ejecuta el servicio SnapCenter Plug-in Loader . Puede agregar el valor si falta el valor predeterminado.  No debe cambiar el valor después de instalar los complementos.
HOST DEL SERVIDOR SNAPCENTER	Muestra la dirección IP o el nombre de host del servidor SnapCenter .
RUTA DEL ALMACÉN DE LLAVES SPL	Muestra la ruta absoluta del archivo del almacén de claves.
PUERTO DEL SERVIDOR SNAPCENTER	Muestra el número de puerto en el que se ejecuta el servidor SnapCenter .

Nombre del parámetro	Descripción
CONTEO MÁXIMO DE REGISTROS	Muestra la cantidad de archivos de registro del Loader de complementos de SnapCenter que se conservan en la carpeta <code>/custom_location/snapcenter/spl/logs</code>. El valor predeterminado se establece en 5000. Si el recuento es mayor que el valor especificado, se conservan los últimos 5000 archivos modificados. La verificación de la cantidad de archivos se realiza automáticamente cada 24 horas desde que se inicia el servicio SnapCenter Plug-in Loader .  Si elimina manualmente el archivo <code>spl.properties</code>, la cantidad de archivos que se conservarán se establecerá en 9999.
JAVA_HOME	Muestra la ruta absoluta del directorio JAVA_HOME que se utiliza para iniciar el servicio SPL. Esta ruta se determina durante la instalación y como parte del inicio de SPL.
TAMAÑO MÁXIMO DE REGISTRO	Muestra el tamaño máximo del archivo de registro de trabajo. Una vez que se alcanza el tamaño máximo, el archivo de registro se comprime y los registros se escriben en el nuevo archivo de ese trabajo.
RETENCIÓN DE REGISTROS DE LOS ÚLTIMOS DÍAS	Muestra el número de días que se conservan los registros.
HABILITAR VALIDACIÓN DE CERTIFICADO	Se muestra como verdadero cuando la validación del certificado CA está habilitada para el host. Puede habilitar o deshabilitar este parámetro editando <code>spl.properties</code> o utilizando la GUI o el cmdlet de SnapCenter .

Si alguno de estos parámetros no está asignado 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 cualquier problema relacionado con los valores asignados a los parámetros. Después de modificar el archivo `spl.properties`, debe reiniciar el servicio SnapCenter Plug-in Loader .

Pasos

1. Realice una de las siguientes acciones, según sea necesario:
 - Inicie el servicio SnapCenter Plug-in Loader :

- Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
- Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- Detener el servicio de Loader de complementos de SnapCenter :
 - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



Puede utilizar la opción `-force` con el comando `stop` para detener a la fuerza el servicio SnapCenter Plug-in Loader . Sin embargo, debe tener cuidado antes de hacerlo porque también termina las operaciones existentes.

- Reinicie el servicio del Loader de complementos de SnapCenter :
 - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Encuentre el estado del servicio Loader de complementos 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`
- Encuentre el cambio en el servicio SnapCenter Plug-in Loader :
 - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurar el certificado de CA con el servicio SnapCenter Plug-in Loader (SPL) en el host Linux

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



SPL utiliza el archivo `'keystore.jks'`, que se encuentra en `'/var/opt/snapcenter/spl/etc'` como almacén de confianza y almacén de claves.

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

Pasos

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

Es el valor correspondiente a la clave 'SPL_KEYSTORE_PASS'.

2. Cambiar la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave
privada en el almacén de claves a 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.

3. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves SPL y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para el almacén de confianza SPL

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

Pasos

1. Navegue a la carpeta que contiene el almacén de claves SPL: */var/opt/snapcenter/spl/etc*.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
. Agregar un certificado raíz o intermedio:
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza SPL.
```



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

Configurar el par de claves firmadas de CA para el almacén de confianza SPL

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

Pasos

1. Navegue a la carpeta que contiene el almacén de claves de SPL `/var/opt/snapcenter/spl/etc`.
2. Localice el archivo `'keystore.jks'`.
3. Enumere los certificados agregados en el almacén de claves:

```
keytool -list -v -keystore keystore.jks
. Agregue el certificado CA que tenga clave privada y pública.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Enumere los certificados agregados en el almacén de claves.
```

```
keytool -list -v -keystore keystore.jks
. Verifique que el almacén de claves contenga el alias correspondiente
al nuevo certificado de CA, que se agregó al almacén de claves.
. Cambie la contraseña de clave privada agregada para el certificado de
CA a la contraseña del almacén de claves.
```

La contraseña del almacén de claves SPL predeterminada es el valor de la clave `SPL_KEYSTORE_PASS` en el archivo `spl.properties`.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Si el nombre de alias en el certificado de CA es largo y contiene
espacios o caracteres especiales ("*", ",", "), cambie el nombre de alias a
un nombre simple:
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure el nombre de alias desde el almacén de claves ubicado en el
archivo spl.properties.
```

Actualice este valor con la clave `SPL_CERTIFICATE_ALIAS`.

4. Reinicie el servicio después de configurar el par de claves firmadas por 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 para SPL es `/var/opt/snapcenter/spl/etc/crl`.

Pasos

1. Puede modificar y actualizar el directorio predeterminado en el archivo `spl.properties` contra la clave `SPL_CRL_PATH`.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet `run Set-SmCertificateSettings`.
- Puede mostrar el estado del certificado de los complementos mediante `Get-SmCertificateSettings`.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.
- *  * indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.

Instalar el SnapCenter Plug-in for VMware vSphere

Si su base de datos o sistema de archivos está almacenado en máquinas virtuales (VM), o si desea proteger las VM y los almacenes de datos, debe implementar el SnapCenter Plug-in for VMware vSphere .

Para obtener información sobre la implementación, consulte ["Descripción general de la implementación"](#) .

Implementar certificado de CA

Para configurar el certificado CA con el SnapCenter Plug-in for VMware vSphere, consulte ["Crear o importar certificado SSL"](#) .

Configurar el archivo CRL

El SnapCenter Plug-in for VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL para el SnapCenter Plug-in for VMware vSphere es `/opt/netapp/config/crl`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Prepárese para proteger los sistemas de archivos Unix

Antes de realizar cualquier operación de protección de datos, como copias de seguridad, clonación o restauración, debe configurar su entorno. También puede configurar el servidor SnapCenter para utilizar la tecnología SnapMirror y SnapVault .

Para aprovechar la tecnología SnapVault y SnapMirror , debe configurar e inicializar una relación de protección de datos entre los volúmenes de origen y destino en el dispositivo de almacenamiento. Puede utilizar NetAppSystem Manager o puede utilizar la línea de comandos de la consola de almacenamiento para realizar estas tareas.

Antes de utilizar el complemento para sistemas de archivos Unix, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y realizar las tareas previas requeridas.

- Instalar y configurar SnapCenter Server. ["Más información"](#)
- Configure el entorno de SnapCenter agregando conexiones del sistema de almacenamiento. ["Más información"](#)



SnapCenter no admite varias SVM con el mismo nombre en diferentes clústeres. Cada SVM registrado con SnapCenter mediante el registro SVM o el registro de clúster debe ser único.

- Agregue hosts, instale los complementos y descubra los recursos.
- Si utiliza SnapCenter Server para proteger sistemas de archivos Unix que residen en LUN o VMDK de

VMware RDM, debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter.

- Instale Java en su host Linux.
- Configure SnapMirror y SnapVault en ONTAP, si desea replicación de copia de seguridad.

Realizar copias de seguridad de los sistemas de archivos Unix

Descubra los sistemas de archivos UNIX disponibles para realizar copias de seguridad

Después de instalar el complemento, todos los sistemas de archivos de ese host se detectan automáticamente y se muestran en la página Recursos. Puede agregar estos sistemas de archivos a grupos de recursos para realizar operaciones de protección de datos.

Antes de empezar

- Debe haber completado tareas como instalar el servidor SnapCenter , agregar hosts y crear conexiones del sistema de almacenamiento.
- Si los sistemas de archivos residen en un disco de máquina virtual (VMDK) o en una asignación de dispositivos sin procesar (RDM), debe implementar el SnapCenter Plug-in for VMware vSphere y registrar el complemento con SnapCenter.

Para obtener más información, consulte ["Implementar el SnapCenter Plug-in for VMware vSphere"](#) .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 información como el tipo, el nombre de host, los grupos de recursos y políticas asociados y el estado.

Crear políticas de respaldo para sistemas de archivos Unix

Antes de utilizar SnapCenter para realizar copias de seguridad de sistemas de archivos Unix, debe crear una política de copia de seguridad para el recurso o el grupo de recursos que desea respaldar. Una política de copias de seguridad es un conjunto de reglas que rigen cómo administrar, programar y conservar las copias de seguridad. También puede especificar la configuración de replicación, script y tipo de copia de seguridad. La creación de una política ahorra tiempo cuando desea reutilizarla en otro recurso o grupo de recursos.

Antes de empezar

- Debe estar preparado para la protección de datos completando tareas como instalar SnapCenter, agregar

hosts, descubrir los sistemas de archivos y crear conexiones del sistema de almacenamiento.

- Si está replicando instantáneas en un espejo o almacenamiento secundario de bóveda, el administrador de SnapCenter debe haberle asignado las SVM para los volúmenes de origen y destino.
- Revise los requisitos previos y las limitaciones específicos de la sincronización activa de SnapMirror . Para obtener información, consulte "[Límites de objetos para la sincronización activa de SnapMirror](#)" .

Acerca de esta tarea

- SnapLock
 - Si se selecciona la opción 'Conservar las copias de seguridad durante una cantidad específica de días', el período de retención de SnapLock debe ser menor o igual a los días de retención mencionados.

Al especificar un período de bloqueo de instantáneas se evita la eliminación de las instantáneas hasta que expire el período de retención. Esto podría llevar a retener una cantidad mayor de instantáneas que la cantidad especificada 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Seleccione **Sistemas de archivos Unix** de la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Nombre, ingrese el nombre y los detalles de la política.
6. En la página Copia de seguridad y replicación, realice las siguientes acciones:
 - a. Especifique la configuración de la copia de seguridad.
 - b. Especifique la frecuencia de programación seleccionando **A pedido**, **Cada hora**, **Diariamente**, **Semanalmente** o **Mensualmente**.
 - c. En la sección Seleccionar opciones de replicación secundaria, seleccione una o ambas de las siguientes opciones de replicación secundaria:

Para este campo...	Haz esto...
Actualizar SnapMirror después de crear una copia de Snapshot local	Seleccione este campo para crear copias reflejadas de los conjuntos de copias de seguridad en otro volumen (replicación SnapMirror). Esta opción debe estar habilitada para la sincronización activa de SnapMirror .
Actualizar SnapVault después de crear una copia de instantánea local	Seleccione esta opción para realizar la replicación de copia de seguridad de disco a disco (copias de seguridad de SnapVault).

Para este campo...	Haz esto...
Recuento de reintentos de error	Introduzca el número máximo de intentos de replicación que se pueden permitir antes de que se detenga la operación.

7. En la página Retención, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionados en la página Copia de seguridad y replicación:

Si quieres...	Entonces...
Mantenga una cierta cantidad de instantáneas	Seleccione Copias para conservar y luego especifique la cantidad de instantáneas que desea conservar. Si el número de instantáneas excede el número especificado, las instantáneas se eliminan primero, comenzando por las copias más antiguas.  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 subyacente de ONTAP .  Debe establecer el recuento de retención en 2 o más si planea habilitar la replicación de SnapVault . Si establece el recuento de retención en 1, la operación de retención puede fallar porque la primera instantánea es la instantánea de referencia para la relación SnapVault hasta que se replique una instantánea más nueva en el destino.
Conservar las instantáneas durante un número determinado de días	Seleccione Conservar copias durante y, a continuación, especifique la cantidad 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 del Snaplock debe ser inferior a 100 años.

8. Seleccione 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.

- En la página Script, ingrese la ruta y los argumentos del prescript o postscript que desea ejecutar antes o después de la operación de respaldo, respectivamente.



Debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento 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.

- Revise el resumen y luego haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas para sistemas de archivos Unix

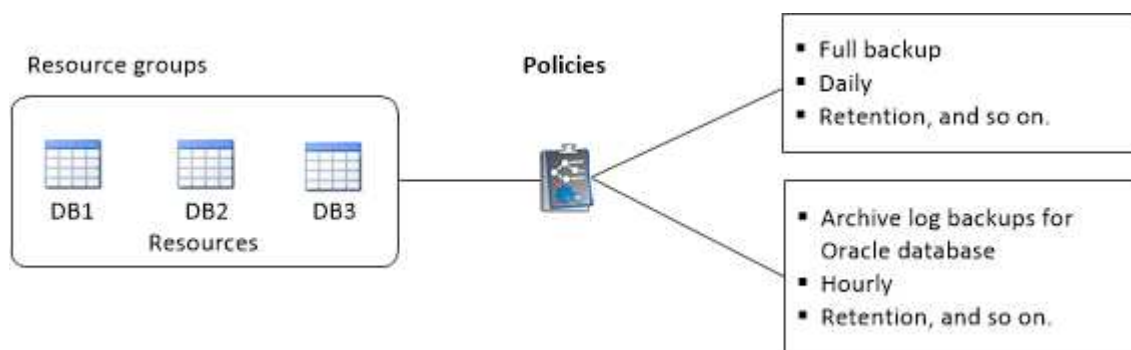
Un grupo de recursos es un contenedor donde se agregan recursos que desea respaldar y proteger. Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados con los sistemas de archivos.

Acerca de esta tarea

- Una base de datos con archivos en grupos de discos ASM debe estar en estado "MONTAR" o "ABIERTO" para verificar sus copias de seguridad mediante la utilidad Oracle DBVERIFY.

Adjunte una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

La siguiente imagen ilustra la relación entre recursos, grupos de recursos y políticas para bases de datos:



- Para las políticas habilitadas para SnapLock , para ONTAP 9.12.1 y versiones anteriores, si especifica un período de bloqueo de instantáneas, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de vencimiento de SnapLock . El administrador de almacenamiento debe limpiar manualmente los clones después del tiempo de vencimiento de SnapLock .
- No se admite agregar 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 agregar nuevos sistemas de archivos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror . Puede agregar recursos al grupo de recursos solo en estado normal o de conmutación por recuperación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:
 - a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione la casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

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 Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, realice lo siguiente:
 - Seleccione la flecha Scripts e ingrese los comandos pre y post para operaciones de inactividad, instantánea y desactivación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
 - Seleccione una de las opciones de consistencia de la copia de seguridad:
 - Seleccione **Consistente en el sistema de archivos** si desea asegurarse de que los datos almacenados en caché del sistema de archivos se vacíen antes de crear la copia de seguridad y que no se permitan operaciones de entrada o salida en el sistema de archivos mientras se crea la copia de seguridad.



Para que el sistema de archivos sea consistente, se tomarán instantáneas del grupo de consistencia para los LUN involucrados en el grupo de volúmenes.

- Seleccione **Consistente ante fallos** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacíen antes de crear la copia de seguridad.



Si ha agregado diferentes sistemas de archivos en el grupo de recursos, entonces todos los volúmenes de diferentes sistemas de archivos en el grupo de recursos se colocarán en un grupo de consistencia.

7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

9. Revise el resumen y luego 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 agregar los recursos que están en los sistemas ASA r2. También puede aprovisionar la protección secundaria mientras crea el grupo de recursos.

Antes de empezar

- Debe asegurarse de no agregar recursos de ONTAP 9.x y de ASA r2 al mismo grupo de recursos.
- Debe asegurarse de no tener 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 inició sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se coloca en modo de mantenimiento mientras se crean los grupos de consistencia primario y secundario. Una vez creados los grupos de consistencia

primarios y secundarios, el grupo de recursos sale del modo de mantenimiento.

- SnapCenter no admite protección secundaria para un recurso clonado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

- a. Introduzca un nombre para el grupo de recursos en el campo Nombre.



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

- b. Ingrese una o más etiquetas en el campo Etiqueta para ayudarlo a buscar el grupo de recursos más adelante.

Por ejemplo, si agrega RR.HH. como etiqueta a varios grupos de recursos, más tarde podrá encontrar todos los grupos de recursos asociados con la etiqueta RR.HH.

- c. Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

- d. Especifique los destinos de los archivos de registro de archivo que no desea respaldar.



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

4. En la página Recursos, seleccione el nombre del host de la base de datos de la lista desplegable **Host**.



Los recursos aparecen en la sección Recursos disponibles solo si se descubren correctamente. Si ha agregado recursos recientemente, aparecerán en la lista de recursos disponibles solo después de actualizar su lista de recursos.

5. Seleccione los recursos ASA r2 de la sección Recursos disponibles y muévelos a la sección Recursos seleccionados.
6. En la página Configuración de la aplicación, seleccione la opción de copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:

- a. Seleccione una o más políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones de la política para la que desea configurar una programación.

- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

Las programaciones de respaldo de terceros no son compatibles cuando se superponen con las programaciones de respaldo de SnapCenter .

8. Si la protección secundaria está habilitada para la política que ha seleccionado, se mostrará la página Protección secundaria y deberá realizar los siguientes pasos:

- a. Seleccione el tipo de política de replicación.



No se admite la política de replicación sincrónica.

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

- c. En los menús desplegables Clúster de destino y SVM de destino, seleccione el clúster emparejado y la SVM que desee utilizar.



SnapCenter no admite el emparejamiento de clústeres y SVM. Debe utilizar el Administrador del sistema o las CLI de ONTAP para realizar el emparejamiento de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos se mostrarán en la sección Recursos protegidos secundarios.

1. En la página de Verificación, realice los siguientes pasos:

- a. Haga clic en **Cargar localizadores** para cargar los volúmenes SnapMirror o SnapVault para realizar la verificación en el almacenamiento secundario.

- b. Hacer clic  en la columna Configurar programaciones para configurar la programación de verificación para todos los tipos de programación de la política.

- c. En el cuadro de diálogo Agregar programaciones de verificación *policy_name*, realice las siguientes acciones:

Si quieres...	Haz esto...
Ejecutar la verificación después de la copia de seguridad	Seleccione Ejecutar verificación después de la copia de seguridad .
Programar una verificación	Seleccione Ejecutar verificación programada y luego seleccione el tipo de programación de la lista desplegable.

- d. Seleccione **Verificar en ubicación secundaria** para verificar sus copias de seguridad en el sistema de almacenamiento secundario.

- e. Haga clic en **Aceptar**.

Los programas de verificación configurados se enumeran en la columna Programas aplicados.

2. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

3. Revise el resumen y luego haga clic en **Finalizar**.

Realizar copias de seguridad de los sistemas de archivos Unix

Si un recurso no forma parte de ningún grupo de recursos, puedes realizar una copia de seguridad del recurso desde la página Recursos.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Ruta** en la lista Ver.
3. Hacer clic  y luego seleccione el nombre del host y los sistemas de archivos Unix para filtrar los recursos.
4. Seleccione el sistema de archivos del cual desea realizar una copia de seguridad.
5. En la página Recursos, puede realizar los siguientes pasos:
 - a. Seleccione la casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

Por ejemplo, `customtext_policy_hostname` o `resource_hostname`. De forma predeterminada, se agrega una marca de tiempo al nombre de la instantánea.

6. En la página Configuración de la aplicación, realice lo siguiente:
 - Seleccione la flecha Scripts e ingrese los comandos pre y post para operaciones de inactividad, instantánea y desactivación del modo inactivo. También puede ingresar los comandos previos que se ejecutarán antes de salir en caso de falla.
 - Seleccione una de las opciones de consistencia de la copia de seguridad:
 - Seleccione **Consistente en el sistema de archivos** si desea asegurarse de que los datos almacenados en caché del sistema de archivos se vacíen antes de crear la copia de seguridad y que no se realicen operaciones en el sistema de archivos mientras se crea la copia de seguridad.
 - Seleccione **Consistente ante fallos** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacíen antes de crear la copia de seguridad.
7. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.



Puede crear una política haciendo clic en  .

En la sección Configurar programaciones para políticas seleccionadas, se enumeran las políticas seleccionadas.

- b. Hacer clic  en la columna Configurar programaciones para configurar una programación para la política que desee.
- c. En la ventana Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione OK .

policy_name es el nombre de la política que ha seleccionado.

Los horarios configurados se enumeran en la columna Horarios aplicados.

8. En la página de Notificación, seleccione los escenarios en los que desea enviar los correos electrónicos desde la lista desplegable **Preferencia de correo electrónico**.

Debe especificar las direcciones de correo electrónico del remitente y del destinatario, así como el asunto del correo electrónico. Si desea adjuntar el informe de la operación de respaldo realizada en el recurso, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell. `Set-SmSmtServer` .

9. Revise el resumen y luego haga clic en **Finalizar**.

Se muestra la página de topología.

10. Haga clic en **Hacer copia de seguridad ahora**.
11. En la página Copia de seguridad, realice los siguientes pasos:

- a. Si ha aplicado varias políticas al recurso, en la lista desplegable Política, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

Realizar copias de seguridad de los grupos de recursos de los sistemas de archivos Unix

Puede realizar una copia de seguridad de los sistemas de archivos Unix definidos en el grupo de recursos. Puede realizar una copia de seguridad de un grupo de recursos a pedido desde la página Recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, las copias de seguridad se crean de acuerdo con la programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y el complemento apropiado de la lista.

2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
3. Ingrese el nombre del grupo de recursos en el cuadro de búsqueda o haga clic en  y seleccione la etiqueta.

Hacer clic  para cerrar el panel de filtro.

4. En la página Grupo de recursos, seleccione el grupo de recursos que desea respaldar.
5. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si tiene varias políticas asociadas con el grupo de recursos, seleccione la política de respaldo que desea utilizar en la lista desplegable **Política**.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según la configuración de retención especificada para el tipo de programación.

- b. Seleccione **Copia de seguridad**.
6. Supervise el progreso seleccionando **Monitor > Trabajos**.

Supervisar la copia de seguridad de los sistemas de archivos Unix

Aprenda a supervisar el progreso de las operaciones de respaldo y de protección de datos.

Supervisar las operaciones de copia de seguridad de los sistemas de archivos Unix

Puede supervisar el progreso de diferentes operaciones de respaldo mediante la página SnapCenterJobs. Es posible que desees verificar el progreso para determinar cuándo está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Trabajos**.
3. En la página Empleos, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de copia de seguridad.
 - b. Especifique las fechas de inicio y finalización.
 - c. En la lista desplegable **Tipo**, seleccione **Copia de seguridad**.

- d. En el menú desplegable **Estado**, seleccione el estado de la copia de seguridad.
 - e. Haga clic en **Aplicar** para ver las operaciones completadas exitosamente.
4. Seleccione un trabajo de respaldo y luego haga clic en **Detalles** para ver los detalles del trabajo.



Aunque el estado del trabajo de respaldo se muestra  , al hacer clic en los detalles del trabajo, es posible que vea que algunas de las tareas secundarias de la operación de respaldo aún están en progreso 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 de la operación seleccionada.

Supervisar las operaciones de protección de datos en el panel Actividad

El panel Actividad muestra las cinco operaciones más recientes realizadas. El panel Actividad también muestra cuándo se inició la operación y el estado de la operación.

El panel Actividad muestra información sobre operaciones de copia de seguridad, restauración, clonación y copia de seguridad programada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. Hacer clic  en el panel Actividad 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**.

Ver sistemas de archivos Unix protegidos en la página Topología

Cuando se prepara para realizar una copia de seguridad, restaurar o clonar un recurso, puede resultarle útil ver una representación gráfica de todas las copias de seguridad, los sistemas de archivos restaurados y los clones en el almacenamiento primario y secundario.

Acerca de esta tarea

En la página Topología, puede ver todas las copias de seguridad, los sistemas de archivos restaurados y los clones que están disponibles para el recurso o grupo de recursos seleccionado. Puede ver los detalles de esas copias de seguridad, sistemas de archivos restaurados y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Puede revisar los siguientes íconos en la vista Administrar copias para determinar si las copias de seguridad y los clones están disponibles en el almacenamiento primario o secundario (copias espejo o copias de bóveda).

•



muestra la cantidad de copias de seguridad y clones que están disponibles en el almacenamiento principal.

•



muestra la cantidad de copias de seguridad y clones que se reflejan en el almacenamiento secundario mediante la tecnología SnapMirror .

•



muestra la cantidad de copias de seguridad y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault .

La cantidad de copias de seguridad mostradas incluye las copias de seguridad eliminadas del almacenamiento secundario. Por ejemplo, si creó 6 copias de seguridad utilizando una política para conservar solo 4 copias de seguridad, la cantidad de copias de seguridad que se muestra es 6.



Los clones de una copia de seguridad de un espejo de versión flexible en un volumen de tipo bóveda de espejo se muestran en la vista de topología, pero el recuento de copias de seguridad de espejo en la vista de topología no incluye la copia de seguridad de versión flexible.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzada como SnapMirror Business Continuity [SM-BC]), puede ver los siguientes íconos adicionales:

•



El sitio de réplica está activo.

•



El sitio de réplica está inactivo.

•



No se ha restablecido la relación de espejo secundario o bóveda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página Topología del recurso seleccionado.

4. Revise la tarjeta Resumen para ver un resumen de la cantidad de copias de seguridad y clones disponibles en el almacenamiento primario 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 SnapLock , al hacer clic en el botón **Actualizar** se actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de vencimiento de SnapLock primario y secundario recuperado de ONTAP.

Cuando el sistema de archivos se distribuye en varios volúmenes, el tiempo de vencimiento de SnapLock para la copia de seguridad será el tiempo de vencimiento de SnapLock más largo establecido para una

instantánea en un volumen. El tiempo de expiración 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 respaldo de SnapCenter consultando a ONTAP los sitios principales y de réplica. Una programación semanal también realiza esta actividad para 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 Async Mirror o Async MirrorVault con el nuevo destino principal se deben configurar manualmente después de la conmutación por error. Desde ONTAP 9.15.1 en adelante, Async Mirror o Async MirrorVault se configura automáticamente en el nuevo destino principal.
- Después de la conmutación por error, se debe crear una copia de seguridad para que SnapCenter esté al tanto de la conmutación por error. Puede hacer clic en **Actualizar** sólo después de haber creado una copia de seguridad.

5. En la vista Administrar copias, haga clic en **Copias de seguridad** o **Clones** desde el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Los detalles de las copias de seguridad y clones se muestran en formato de tabla.

6. Seleccione la copia de seguridad de la tabla y luego haga clic en los íconos de protección de datos para realizar operaciones de restauración, clonación y eliminación.



No puede cambiar el nombre ni eliminar las copias de seguridad que se encuentran en el almacenamiento secundario.

7. Si desea eliminar un clon, seleccione el clon de la tabla y luego haga clic en  .

Ejemplo que muestra copias de seguridad 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 el servidor SnapCenter , enumerar las copias de seguridad y recuperar su información y restaurar la copia de seguridad.

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 la copia de seguridad de la ubicación principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Ruta** o **Grupo de recursos** en la lista **Ver**.

3. Seleccione el sistema de archivos desde la vista de detalles o desde la vista de detalles del grupo de recursos.

Se muestra la página de topología.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o reflejado).

5. Seleccione la copia de seguridad de la tabla y luego haga clic en *  *.

6. En la página Restaurar ámbito:

- Para los sistemas de archivos NFS, de manera predeterminada se selecciona la restauración **Conectar y copiar**. También puedes seleccionar **Volumen Revertido** o **Restauración Rápida**.
- Para sistemas de archivos que no sean NFS, el alcance de 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, ingrese comandos de restauración previos para ejecutar antes de realizar un trabajo de restauración.
8. En la página PostOps, ingrese los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.



Debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento en la ubicación `_/opt/NetApp/snapcenter/scc/etc/allowed_commands.config_path`.

9. En la página Notificación, en la lista desplegable **Preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.

También debe especificar las direcciones de correo electrónico del remitente y del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de restauración realizada, deberá seleccionar **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell `Set-SmSmtServer`.

10. Revise el resumen y luego 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 un grupo de volúmenes, el contenido antiguo del sistema de archivos no se elimina. Solo se copiará el contenido del sistema de archivos clonado al sistema de archivos de origen. Esto es aplicable cuando hay varios sistemas de archivos en el grupo de volúmenes y se restaura el sistema de archivos NFS predeterminado.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Supervisar las operaciones de restauración de sistemas de archivos Unix

Puede supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página **Trabajos**. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los estados posteriores a la restauración describen las condiciones del recurso después de una operación de restauración y cualquier acción de restauración adicional que pueda realizar.

Los siguientes iconos aparecen en la página **Trabajos** e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan 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 luego 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 de la operación seleccionada.

Clonar sistemas de archivos Unix

Copia de seguridad del sistema de archivos clonado de Unix

Puede utilizar SnapCenter para clonar el sistema de archivos Unix utilizando la copia de seguridad del sistema de archivos.

Antes de empezar

- Puede omitir la actualización del archivo `fstab` estableciendo el valor de `SKIP_FSTAB_UPDATE` en **true** en el archivo `agent.properties` ubicado en `/opt/NetApp/snapcenter/scc/etc`.

- Puede tener un nombre de volumen de clon estático y una ruta de unión configurando el valor de `USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT` en **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 manualmente el archivo `fstab` actualizado si no prefiere actualizar el `fstab` mediante SnapCenter.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Ruta** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione el sistema de archivos desde la vista de detalles o desde la vista de detalles del grupo de recursos.

Se muestra la página de topología.

4. Desde la vista Administrar copias, seleccione las copias de seguridad de Copias locales (principales), Copias espejo (secundarias) o Copias de bóveda (secundarias).
5. Seleccione la copia de seguridad de la tabla y luego haga clic en *  *.
6. En la página Ubicación, realice las siguientes acciones:

Para este campo...	Haz esto...
Servidor clonado	De forma predeterminada, se completa el host de origen.
Punto de montaje de clonación	Especifique la ruta donde se montará el sistema de archivos.

7. En la página Scripts, realice los siguientes pasos:
 - a. Introduzca los comandos para pre-clonar o post-clonar que deben ejecutarse antes o después de la operación de clonación, respectivamente.



Debe verificar si los comandos existen en la lista de comandos disponible en el host del complemento desde la ruta `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`.

8. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. Si desea adjuntar el informe de la operación de clonación realizada, seleccione **Adjuntar informe de trabajo**.



Para recibir notificaciones por correo electrónico, debe haber especificado los detalles del servidor SMTP mediante la GUI o el comando de PowerShell Set-SmSmtServer.

9. Revise el resumen y luego haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Dividir un clon

Puede utilizar SnapCenter para dividir un recurso clonado del recurso principal. El clon que se divide se vuelve independiente del recurso principal.

Acerca de esta tarea

- No es posible realizar la operación de división de clon en un clon intermedio.

Por ejemplo, después de crear clone1 a partir de una copia de seguridad de la base de datos, puede crear una copia de seguridad de clone1 y luego clonar esta copia de seguridad (clone2). Después de crear el clon2, el clon1 es un clon intermedio y no se puede realizar la operación de división de clon en el clon1. Sin embargo, puede realizar la operación de división de clon en clone2.

Después de dividir el clon2, puede realizar la operación de división de clon en el clon1 porque el clon1 ya no es el clon intermedio.

- Cuando se divide un clon, se eliminan las copias de seguridad y los trabajos de clonación del clon.
- Para obtener información sobre las operaciones de división de volumen de FlexClone, consulte ["Dividir un volumen FlexClone de su volumen principal"](#).
- Asegúrese de que el volumen o agregado en el sistema de almacenamiento esté en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página **Recursos**, seleccione la opción adecuada de la lista Ver:

Opción	Descripción
Para aplicaciones de bases de datos	Seleccione Base de datos de la lista Ver.
Para sistemas de archivos	Seleccione Ruta de la lista Ver.

3. Seleccione el recurso apropiado de la lista.

Se muestra la página de topología de recursos.

4. Desde la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y luego haga clic en *  *.
5. Revise el tamaño estimado del clon que se va a dividir y el espacio requerido disponible en el agregado y luego haga clic en **Iniciar**.
6. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

La operación de división de clones deja de responder si se reinicia el servicio SMCORE. Debe ejecutar el

cmdlet Stop-SmJob para detener la operación de división de clonación y luego volver a intentarla.

Si desea un tiempo de sondeo más largo o más corto para verificar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer el intervalo de tiempo para que SMCore sondee el estado de la operación de división del clon. El valor está en milisegundos y el valor predeterminado es 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

La operación de inicio de división de clonación falla si se está realizando una copia de seguridad, una restauración u otra división de clonación. Debe reiniciar la operación de división de clones solo después de que se completen las operaciones en ejecución.

Información relacionada

["La clonación o verificación de SnapCenter falla con el agregado no existente"](#)

Supervisar operaciones de clonación de sistemas de archivos Unix

Puede supervisar el progreso de las operaciones de clonación de SnapCenter mediante la página Trabajos. Es posible que desee verificar el progreso de una operación para determinar cuándo se completó o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

-  En curso
-  Completado exitosamente
-  Fallido
-  Completado con advertencias o no se pudo iniciar debido a advertencias
-  En cola
-  Cancelado

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Empleos**, realice los siguientes pasos:
 - a. Hacer clic  para filtrar la lista de modo que solo se incluyan las operaciones de clonación.
 - 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 de clonación.
 - e. Haga clic en **Aplicar** para ver las operaciones que se completaron correctamente.

4. Seleccione el trabajo de clonación y luego haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Proteger las aplicaciones que se ejecutan en Azure NetApp Files

Proteger las aplicaciones que se ejecutan en Azure NetApp Files

SnapCenter admite la protección de sus 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 respaldo de Azure NetApp Files que amplía las capacidades de protección de datos de Azure NetApp Files al proporcionar una solución de respaldo completamente administrada para recuperación, archivo y cumplimiento a largo plazo.

Azure NetApp Files es una solución de almacenamiento premium que puede resultar costosa para la retención de copias de seguridad a largo plazo. Para optimizar los costos, puede mover las copias de seguridad del almacenamiento de Azure NetApp Files a un almacén de objetos de Azure. A partir de SnapCenter 6.0.1, puede realizar copias de seguridad y clonar aplicaciones que residen en Azure NetApp Files en Azure Blob Storage (almacén de objetos). Puede mantener dos copias de sus datos: copias de instantáneas de volumen en el almacenamiento de Azure NetApp Files para la recuperación a corto plazo y otra copia en Azure Blob Storage para la recuperación a largo plazo.

Cuando una política con copia de seguridad de Azure NetApp Files está habilitada y asociada a un recurso, SnapCenter controla la creación de instantáneas de volumen y su respaldo en Azure Blob Storage. SnapCenter crea la Bóveda de respaldo y habilita la copia de seguridad para el volumen. Si ha habilitado la copia de seguridad para el volumen, SnapCenter utiliza la bóveda existente.

Limitaciones

- Las funcionalidades de almacenamiento de objetos para FAS, ASA o AFF ONTAP y Amazon FSx for NetApp ONTAP no son compatibles.
- Los flujos de trabajo de montaje y catálogo de Oracle y SAP HANA no son compatibles con las copias de seguridad de almacenamiento de objetos, pero sí con las instantáneas.
- Los clones de Oracle PDB no son compatibles con las copias de seguridad de almacenamiento de objetos, pero sí con las instantáneas.
- No se admiten la verificación de copias de seguridad desde el almacenamiento de objetos, la compatibilidad con API REST, la gestión del ciclo de vida de los clones desde el almacenamiento de objetos ni las funciones de informes para las copias de seguridad del almacenamiento de objetos.
- No se admite la restauración desde copias de seguridad en Azure Blob Storage a Azure NetApp Files . También puedes utilizar la opción de clonar.
- No se admite la división de clones.

Instalar SnapCenter y crear credenciales

Instalar SnapCenter en una máquina virtual de Azure

Puede descargar el SnapCenter software desde el sitio de soporte de NetApp e instalarlo en la máquina virtual de Azure.

Antes de empezar

- Asegúrese de que la máquina virtual de Azure Windows cumpla con los requisitos para la instalación de SnapCenter Server. Para obtener más información, consulte ["Requisitos para instalar SnapCenter Server"](#) .
- Si es nuevo en Azure NetApp Files y no tiene una cuenta de NetApp existente, asegúrese de haberse registrado para poder acceder al software SnapCenter . Para más información, véase ["Regístrese para acceder al SnapCenter software"](#) .

Pasos

1. Descargue el paquete de instalación de SnapCenter Server desde ["Sitio de soporte de NetApp"](#) .
2. Inicie la instalación de SnapCenter Server haciendo doble clic en el archivo .exe descargado.

Después de iniciar la instalación, se realizan todas las comprobaciones previas y, si no se cumplen los requisitos mínimos, se muestran mensajes de error o advertencia correspondientes. Puede ignorar los mensajes de advertencia y continuar con la instalación; sin embargo, los errores deberían solucionarse.

3. Revise los valores previamente completados necesarios para la instalación de SnapCenter Server y modifíquelos si es necesario.

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



El carácter especial "%" no es compatible con la ruta personalizada de la base de datos del repositorio. Si incluye "%" en la ruta, la instalación fallará.

4. Haga clic en **Instalar ahora**.

Si ha especificado algún valor que no es válido, se mostrarán los mensajes de error correspondientes. Debe volver a ingresar los valores y luego iniciar la instalación.



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

Sin embargo, si hace clic en **Cancelar** cuando se realizan las operaciones "Reinicio del sitio de SnapCenter Server" o "Esperando a que se inicie SnapCenter Server", la instalación continuará sin cancelar la operación.

Registre el producto para habilitar el soporte

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 *Acerca de SnapCenter*, anote la instancia de SnapCenter , un número de 20 dígitos que comienza con 971.
3. Hacer clic <https://register.netapp.com> .
4. Haga clic en *No soy un cliente registrado de NetApp *.
5. Especifique sus datos para registrarse.

6. Deje el campo SN de referencia de NetApp en blanco.
7. Seleccione * SnapCenter* en el menú desplegable Línea de productos.
8. Seleccione el proveedor de facturación.
9. Introduzca el ID de instancia de SnapCenter de 20 dígitos.
10. Haga clic en **Enviar**.

Crear la credencial 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 la entidad de servicio en Azure.
- Asegúrese de tener a mano el ID de inquilino, el ID de cliente y la clave secreta asociados con la entidad de servicio.
 - El identificador de inquilino se puede encontrar en el Portal de Azure, en la página Descripción general del identificador de Entra.
 - El ID del cliente también se conoce como ID de la aplicación para la entidad principal del servicio/aplicación empresarial. Esto se puede encontrar en el Portal de Azure, en la página Descripción general de la aplicación empresarial que ha creado para que actúe como entidad de servicio para SnapCenter.
 - La clave secreta del cliente también se conoce como valor secreto. Puede crear este secreto de cliente en Azure Portal navegando a **Registros de aplicaciones** en ID de entrada. Después de seleccionar la aplicación empresarial que creó, navegue a **Certificados y secretos** y luego a **Nuevo secreto de cliente**.



Sólo se puede acceder al valor secreto cuando se crea. No podrás acceder a él más tarde.

- Es necesario conceder permisos al principal del servicio. El rol de Colaborador permitirá que la entidad de servicio realice las acciones necesarias en Azure. Esto se puede conceder desde la página de Control de acceso (IAM) dentro de la página Suscripción.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, especifique la siguiente información necesaria para crear la credencial.

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para la credencial.
Modo de autenticación	Seleccione Credenciales de Azure de la lista desplegable.

Para este campo...	Haz esto...
Identificación del inquilino	Introduzca el ID del inquilino.
ID de cliente	Introduzca el ID del cliente.
Clave secreta del cliente	Introduzca la clave secreta del cliente.

5. Haga clic en **Aceptar**.

Configurar 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 identificador de suscripción, las credenciales de Azure y la cuenta de Azure NetApp .



Las licencias estándar y las licencias basadas en capacidad no son necesarias 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 de las respectivas listas desplegables.
4. Haga clic en **Enviar**.

Cree las credenciales para agregar el host del complemento

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter .

Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, especifique la siguiente información necesaria para crear la credencial.

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para la credencial.
Modo de autenticación	Seleccione el modo de autenticación de la lista desplegable.

Para este campo...	Haz esto...
Tipo de autenticación	Seleccione Basado en contraseña o Basado en clave SSH (solo para host Linux).
Nombre de usuario	Especifique el nombre de usuario.
Password	Si ha seleccionado la autenticación basada en contraseña, especifique la contraseña.
Clave privada SSH	Si ha seleccionado la autenticación basada en clave SSH, especifique la clave privada.
Utilice privilegios de sudo	Seleccione la casilla de verificación Usar privilegios de sudo si está creando credenciales para un usuario que no es root.  Esto solo se aplica a usuarios de Linux.

5. Haga clic en **Aceptar**.

Proteger las bases de datos de SAP HANA

Agregar hosts e instalar el complemento de SnapCenter para la base de datos SAP HANA

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar los paquetes de complementos. Los complementos se instalan automáticamente en los hosts remotos.

Antes de empezar

- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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 realizando la instalación en el host centralizado, asegúrese de que el software del 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 de HDB de forma remota.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** 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 Nombre de host, ingrese el nombre de dominio completo (FQDN) o la dirección IP del host.
 - c. En el campo Credenciales, ingrese la credencial que creó.
5. En la sección Seleccionar complementos para instalar, seleccione los complementos 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 luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.

9. Supervisar el progreso de la instalación.

Agregar base de datos SAP HANA

Debe agregar la base de datos SAP HANA manualmente.

Acerca de esta tarea

Los recursos deben agregarse manualmente si el complemento está instalado en un servidor centralizado. Si el complemento SAP HANA está instalado en el host de la base de datos HANA, el sistema HANA se descubre automáticamente.



El descubrimiento automático no es compatible con la configuración de múltiples hosts de HANA, deben agregarse únicamente a través del complemento centralizado.

Pasos

1. En el panel de navegación izquierdo, seleccione el complemento SnapCenter para la base de datos SAP HANA de la lista desplegable y luego haga clic en **Recursos**.
2. En la página Recursos, haga clic en **Agregar base de datos SAP HANA**.
3. En la página Proporcionar detalles de recursos, realice las siguientes acciones:
 - a. Ingrese el tipo de recurso como Contenedor único, Contenedor de base de datos multiinquilino o Volumen sin datos.
 - b. Introduzca el nombre del sistema SAP HANA.
 - c. Introduzca el ID del sistema (SID).
 - d. Seleccione el host del complemento.
 - e. Introduzca la clave para conectarse al sistema SAP HANA.
 - f. Introduzca el nombre de usuario para el cual está configurada la clave de almacenamiento de usuario seguro de 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 grupo de capacidad y los volúmenes asociados.
 - c. Haga clic en **Guardar**.
5. Revise el resumen y luego haga clic en **Finalizar**.

Crear políticas de respaldo para bases de datos de SAP HANA

Antes de usar SnapCenter para realizar copias de seguridad de los recursos de base de datos de SAP HANA, debe crear una política de copia de seguridad para el recurso o grupo de recursos que desea respaldar.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre de la política y la descripción.
5. En la página Tipo de política, realice los siguientes pasos:
 - a. Seleccione *** Azure NetApp Files*** como tipo de almacenamiento.
 - b. Seleccione **Basado en archivo** si desea realizar una verificación de integridad de la base de datos.
 - c. Seleccione **Basado en instantánea** si desea crear una copia de seguridad utilizando la tecnología de instantánea.
6. En la página Instantánea y copia de seguridad, realice los siguientes pasos:
 - a. Seleccione la frecuencia de la copia de seguridad programada.
 - 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 adjunte políticas de respaldo de SAP HANA

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger.

Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados con una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos.

Para este campo...	Haz esto...
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

- En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.
- Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
- En la página Políticas, realice los siguientes pasos:
 - Seleccione una o más políticas de la lista desplegable.
 - En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
 - En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.
- En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
- Revise el resumen y luego haga clic en **Finalizar**.

Realice una copia de seguridad de las bases de datos de SAP HANA que se ejecutan en Azure NetApp Files

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Pasos

- En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
- En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.
- Seleccione el recurso que desea respaldar.
- En la página Recursos, seleccione **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.
- En la página Configuración de la aplicación, haga lo siguiente:
 - Seleccione la flecha **Copias de seguridad** para configurar opciones de copia de seguridad adicionales.
 - Seleccione la flecha **Scripts** para ejecutar comandos previos y posteriores para operaciones de inactividad, instantánea y desactivación del modo inactivo.
 - Seleccione la flecha **Configuraciones personalizadas** y luego ingrese los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.
 - Seleccione la **Herramienta de copia de instantáneas > SnapCenter sin consistencia del sistema de archivos** para crear instantáneas.

La opción **Consistencia del sistema de archivos** solo se aplica a aplicaciones que se ejecutan en hosts de Windows.

6. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.
 - b. Seleccione *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.

policy_name es el nombre de la política que usted seleccionó.

7. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario, y el asunto del correo electrónico. El SMTP también debe configurarse en **Configuración > Configuración global**.

8. Revise el resumen y luego seleccione **Finalizar**.
9. Seleccione **Hacer copia de seguridad ahora**.
10. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si hay varias políticas asociadas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 > Trabajos**.

Realizar copias de seguridad de los grupos de recursos de SAP HANA

Un grupo de recursos es una colección de recursos en un host. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si hay varias políticas asociadas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.

Si la política seleccionada para la copia de seguridad a pedido está asociada con una programación de copia de seguridad, las copias de seguridad a pedido se conservarán según 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 de SAP HANA

Puede restaurar y recuperar datos de las copias de seguridad.

Acerca de esta tarea

Para los sistemas HANA detectados automáticamente, si se selecciona la opción **Recurso completo**, la restauración se realiza utilizando la tecnología de restauración de instantáneas de archivo único. Si la casilla de verificación **Restauración rápida** está seleccionada, se utiliza la tecnología de reversión de volumen.

Para los recursos agregados manualmente, siempre se utiliza la tecnología Volume Revert.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.
3. Seleccione el recurso o seleccione un grupo de recursos y luego seleccione un recurso en ese grupo.
4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento primario o secundario (duplicado o almacenado en bóveda).
5. En la tabla Copias de seguridad principales, seleccione la copia de seguridad que desea restaurar y luego haga clic en *  *.
6. En la página Restaurar alcance, seleccione **Recurso completo**.

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 Ámbito de recuperación, realice las siguientes acciones:
 - a. Seleccione **Recuperar al estado más reciente** si desea recuperar lo más cerca posible de la hora actual.
 - b. Seleccione **Recuperar al 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 a una copia de seguridad de datos específica.
 - d. Seleccione **Sin recuperación** si no desea recuperar ahora.
 - e. Especifique las ubicaciones de las copias de seguridad del registro.
 - f. Especifique la ubicación del catálogo de respaldo.
8. En la página Operaciones previas, ingrese los comandos de restauración previa y de desmontaje para ejecutar antes de realizar un trabajo de restauración.
9. En la página Operaciones posteriores, ingrese los comandos de montaje y restauración posterior para ejecutarlos después de realizar un trabajo de restauración.
10. En la página de Notificaciones, en la lista desplegable **Preferencias 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 del destinatario y el asunto del correo electrónico. El SMTP también debe configurarse en la página **Configuración > Configuración**

global.

11. Revise el resumen y luego haga clic en **Finalizar**.
12. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Clonar copia de seguridad de la base de datos de SAP HANA

Puede utilizar SnapCenter para clonar una base de datos de SAP HANA utilizando la copia de seguridad de la base de datos. Los clones creados son clones gruesos y se crean en el grupo de capacidad principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** según el tipo de recurso.
3. Seleccione el recurso o grupo de recursos.
4. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento principal.
5. Seleccione la copia de seguridad de datos de la tabla y luego haga clic en .
6. En la página Ubicación, realice las siguientes acciones:
 - a. Seleccione el host que tiene instalado el complemento SAP HANA para administrar el sistema HANA clonado.

Puede ser un host de complemento centralizado o un host de sistema HANA.



Si el complemento HANA está instalado en un host centralizado que administra bases de datos HANA en otros hosts, al crear o eliminar clones, SnapCenter omite intencionalmente las operaciones del lado del host (montar o desmontar el sistema de archivos) ya que el servidor de destino es un host centralizado. Debes usar scripts personalizados previos o posteriores a la clonación para realizar operaciones de montaje y desmontaje.

- a. Ingrese el SID de SAP HANA para clonar desde las copias de seguridad existentes.
- b. Introduzca las direcciones IP o los nombres de host a los que se exportarán los volúmenes clonados.
- c. Si los volúmenes ANF de la base de datos SAP HANA están configurados en un grupo de capacidad de QOS manual, especifique la QOS para los volúmenes clonados.

Si no se especifica la calidad de servicio para los volúmenes clonados, se utilizará la calidad de servicio del volumen de origen. Si se utiliza el grupo de capacidad de QOS automático, se ignorará el valor de QOS especificado.

7. En la página Scripts, realice los siguientes pasos:
 - a. Introduzca los comandos para pre-clonar o post-clonar que deben ejecutarse antes o después de la operación de clonación, respectivamente.
 - b. Introduzca el comando de montaje para montar un sistema de archivos en un host.

Si el sistema HANA de origen se detecta automáticamente y el complemento del host de destino clonado está instalado en el host SAP HANA, SnapCenter desmonta automáticamente los volúmenes

de datos HANA existentes en el host de destino clonado y monta los volúmenes de datos HANA recién clonados.

8. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y luego haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.



La división de clones está deshabilitada para los clones ANF porque el clon ANF ya es un volumen independiente creado a partir de la instantánea seleccionada.

Proteger las bases de datos de Microsoft SQL Server

Agregar hosts e instalar el complemento de SnapCenter para la base de datos de SQL Server

SnapCenter admite la protección de datos de instancias de SQL en recursos compartidos SMB en Azure NetApp Files. Se admiten configuraciones independientes y de grupo de disponibilidad (AG).

Debe utilizar la página Agregar host de SnapCenter para agregar hosts y luego instalar el paquete de complementos. Los complementos se instalan automáticamente en los hosts remotos.

Antes de empezar

- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento 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. Verifique que la pestaña **Hosts administrados** esté 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 Nombre de host, ingrese el nombre de dominio completo (FQDN) o la dirección IP del host.
 - c. En el campo Credenciales, ingrese la credencial que creó.
5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea 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 del host, ingrese la ruta SMB del directorio de registro del host y haga clic en **Guardar**.
9. Haga clic en **Enviar** y supervise el progreso de la instalación.

Crear políticas de respaldo para bases de datos de SQL Server

Puede crear una política de respaldo para el recurso o el grupo de recursos antes de usar SnapCenter para realizar un respaldo de los recursos de SQL Server, o puede crear una política de respaldo en el momento en que crea un grupo de recursos o realiza un respaldo de un solo recurso.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Haga clic en **Nuevo**.
4. En la página Nombre, ingrese el nombre de la política y la descripción.
5. En la página Tipo de política, realice los siguientes pasos:
 - a. Seleccione * Azure NetApp Files* como tipo de almacenamiento.
 - b. Seleccione el tipo de copia de seguridad.
 - i. Seleccione **Copia de seguridad completa y copia de seguridad de registros** si desea realizar una copia de seguridad de los archivos de base de datos y de los registros de transacciones.
 - ii. Seleccione **Copia de seguridad completa** si desea realizar una copia de seguridad sólo de los archivos de la base de datos.
 - iii. Seleccione **Copia de seguridad del registro** si desea realizar una copia de seguridad solo de los registros de transacciones.
 - iv. Seleccione **Copiar solo copia de seguridad** si desea realizar una copia de seguridad de sus recursos mediante otra aplicación.
 - c. En la sección Configuración del grupo de disponibilidad, realice las siguientes acciones:
 - i. Seleccione Realizar copia de seguridad en la réplica de copia de seguridad preferida si desea realizar una copia de seguridad solo en la réplica.
 - ii. Seleccione la réplica de AG principal o la réplica de AG secundaria para la copia de seguridad.
 - iii. Seleccione la prioridad de la copia de seguridad.
6. En la página Instantánea y copia de seguridad, realice los siguientes pasos:
 - a. Seleccione la frecuencia de la copia de seguridad programada.
 - b. Especifique la configuración de retención según el tipo de copia de seguridad 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 de Verificación, realice los siguientes pasos:
 - a. En la sección Ejecutar verificación para las siguientes programaciones de copias de seguridad, seleccione la frecuencia de la programación.
 - b. En la sección Opciones de verificación de consistencia de la base de datos, 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 verificación de integridad a la estructura física de la base de datos y detectar páginas rotas, fallas de suma de comprobación y fallas de hardware comunes que afectan la base de datos.

- ii. Seleccione **Suprimir todos los mensajes de información (NO_INFOMSGS)** para suprimir todos los mensajes informativos.

Seleccionado por defecto.

- iii. Seleccione **Mostrar todos los mensajes de error informados por objeto (ALL_ERRORMSGs)** para mostrar todos los errores informados por objeto.
- iv. Seleccione **No comprobar índices no agrupados (NOINDEX)** si no desea comprobar índices no agrupados.

La base de datos de SQL Server utiliza el Comprobador de consistencia de base de datos de Microsoft SQL Server (DBCC) 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 de instantánea de base de datos interna (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una copia de instantánea de base de datos interna.

- c. En la sección **Copia de seguridad del registro**, seleccione **Verificar copia de seguridad del registro al finalizar** para verificar la copia de seguridad del registro al finalizar.

- d. En la sección **Configuración del script de verificación**, ingrese la ruta y los argumentos del prescript o postscript que deben ejecutarse antes o después de la operación de verificación, respectivamente.

- 8. Revise el resumen y haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas de respaldo de SQL

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger.

Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados con una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos.
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.

4. En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.
5. Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.
 - b. En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
 - c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.
 - d. Seleccione el programador de Microsoft SQL Server.
7. En la página de Verificación, realice los siguientes pasos:
 - a. Seleccione el servidor de verificación.
 - b. Seleccione la política para la que desea configurar su programa de verificación y luego haga clic en *  *.
 - c. Seleccione **Ejecutar verificación después de la copia de seguridad** o **Ejecutar verificación programada**.
 - d. Haga clic en **Aceptar**.
8. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y luego haga clic en **Finalizar**.

Realizar copias de seguridad de bases de datos de SQL Server que se ejecutan en Azure NetApp Files

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Antes de empezar

Debe crear un equilibrador de carga si el clúster de conmutación por error de Windows de Azure no tiene una IP de clúster asignada o si no es accesible desde SnapCenter. La IP del balanceador de carga debe estar configurada y ser accesible desde el servidor SnapCenter .

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento 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 **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.
4. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.
 - b. Seleccionar *  * en la columna Configurar programaciones de la política para la que desea

configurar una programación.

- c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.

policy_name es el nombre de la política que usted seleccionó.

- d. Seleccione **Usar programador de Microsoft SQL Server** y, a continuación, seleccione la instancia del programador de la lista desplegable **Instancia del programador** que esté asociada con la política de programación.
5. En la página de Verificación, realice los siguientes pasos:
 - a. Seleccione el servidor de verificación.
 - b. Seleccione la política para la que desea configurar su programa de verificación y luego haga clic en .
 - c. Seleccione **Ejecutar verificación después de la copia de seguridad** o **Ejecutar verificación programada**.
 - d. Haga clic en Aceptar.
 6. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
 7. Revise el resumen y luego haga clic en **Finalizar**.
 8. Seleccione **Hacer copia de seguridad ahora**.
 9. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si hay varias políticas asociadas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar 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 > Trabajos**.

Realizar copias de seguridad de grupos de recursos de SQL Server

Puede realizar copias de seguridad de los grupos de recursos que constan de varios recursos. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si hay varias políticas asociadas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.
 - b. Después de realizar la copia de seguridad, seleccione **Verificar** para verificar la copia de seguridad a pedido.

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 respaldadas. La restauración de la base de datos es un proceso multifase que copia todos los datos y las páginas de registro de una copia de seguridad de SQL Server especificada a una base de datos especificada.

Acerca de esta tarea

Debe asegurarse de que la instancia de destino para la restauración esté configurada con un usuario de directorio activo que pertenezca al dominio de directorio activo de SMB AD y tenga permisos para configurar los permisos de archivo de forma adecuada. Debe configurar las credenciales en SnapCenter a nivel de instancia.

La autenticación SQL para la instancia de destino no será compatible con configuraciones SMB. La instancia de destino debe configurarse en SnapCenter con el usuario del directorio activo que tenga los permisos necesarios.

Si la cuenta de servicio de servicios del complemento SnapCenter no es un usuario de directorio activo, al realizar una restauración a un host alternativo, se requiere el usuario que tiene control total sobre los volúmenes de origen para poder suplantarlos y realizar la operación requerida.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de la lista.
4. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento.
5. Seleccione la copia de seguridad de la tabla y luego haga clic en el botón  icono.
6. En la página Restaurar ámbito, seleccione una de las siguientes opciones:
 - a. 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 realizaron las copias de seguridad.
 - b. Seleccione **Restaurar la base de datos en un host alternativo** si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o en uno diferente donde se realizan las copias de seguridad.
7. En la página Ámbito de recuperación, seleccione una de las siguientes opciones:
 - a. Seleccione **Ninguno** cuando necesite restaurar solo la copia de seguridad completa sin ningún registro.
 - b. Seleccione la operación de restauración de copia de seguridad actualizada **Todas las copias de seguridad de registros** para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa.
 - c. Seleccione **Por copias de seguridad de registros** para realizar una operación de restauración en un punto en el tiempo, que restaura la base de datos basándose en los registros de copia de seguridad

hasta el registro de copia de seguridad con la fecha seleccionada.

- d. Seleccione **Por fecha específica hasta** para especificar la fecha y la hora después de las cuales los registros de transacciones no se aplicarán a la base de datos restaurada.
 - e. Si ha seleccionado **Todas las copias de seguridad de registros, Por copias de seguridad de registros o Por fecha específica hasta** y los registros se encuentran en una ubicación personalizada, seleccione **Usar directorio de registros personalizado** y, a continuación, especifique la ubicación del registro.
8. En la página Preoperatorio y Postoperatorio, especifique los detalles requeridos.
 9. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
 10. Revise el resumen y luego haga clic en **Finalizar**.
 11. Supervise el proceso de restauración utilizando la página **Monitor > Trabajos**.

Copia de seguridad de la base de datos de clonación de SQL Server

Puede utilizar SnapCenter para clonar una base de datos SQL utilizando la copia de seguridad de la base de datos. Los clones creados son clones gruesos y se crean en el grupo de capacidad principal.

Acerca de esta tarea

Debe asegurarse de que la instancia de destino para el clon esté configurada con un usuario de directorio activo que pertenezca al dominio de directorio activo de SMB AD y tenga permisos para configurar los permisos de archivo de forma adecuada. Debe configurar las credenciales en SnapCenter a nivel de instancia.

La autenticación SQL para la instancia de destino no será compatible con configuraciones SMB. La instancia de destino debe configurarse en SnapCenter con el usuario del directorio activo que tenga los permisos necesarios.

Si la cuenta de servicio de servicios del complemento SnapCenter no es un usuario de directorio activo, al realizar la clonación, se requiere el usuario que tiene control total sobre los volúmenes de origen para poder suplantarlos y realizar la operación requerida.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de 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.
4. Desde la página de vista **Administrar copias**, seleccione la copia de seguridad del sistema de almacenamiento principal.
5. Seleccione la copia de seguridad y luego seleccione *  *.
6. En la página **Opciones de clonación**, proporcione todos los detalles requeridos.
7. En la página Ubicación, seleccione una ubicación de almacenamiento para crear un clon.

Si los volúmenes ANF de la base de datos de SQL Server están configurados en un grupo de capacidad de QOS manual, especifique la QOS para los volúmenes clonados.

Si no se especifica la calidad de servicio para los volúmenes clonados, se utilizará la calidad de servicio

del volumen de origen. Si se utiliza el grupo de capacidad de QOS automático, se ignorará el valor de QOS especificado.

8. En la página Registros, seleccione una de las siguientes opciones:
 - a. Seleccione **Ninguno** si desea clonar solo la copia de seguridad completa sin ningún registro.
 - b. Seleccione **Todas las copias de seguridad de registros** si desea clonar todas las copias de seguridad de registros disponibles con fecha posterior a la copia de seguridad completa.
 - c. Seleccione **Por copias de seguridad de registros hasta** 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**, ingrese el tiempo de espera del script, la ruta y los argumentos del prescript o postscript que se deben ejecutar antes o después de la operación de clonación, respectivamente.
10. En la página **Notificación**, de la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revise el resumen y luego seleccione **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

Realizar ciclo de vida de clonación

Con SnapCenter, puede crear clones desde un grupo de recursos o una base de datos. Puede realizar una clonación a pedido o programar operaciones de clonación recurrentes de un grupo de recursos o una base de datos. Si clona una copia de seguridad periódicamente, puede usar el clon para desarrollar aplicaciones, completar datos o recuperar datos.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de 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.
4. Desde la página de vista **Administrar copias**, seleccione la copia de seguridad del sistema de almacenamiento principal.
5. Seleccione la copia de seguridad y luego seleccione *  *.
6. En la página **Opciones de clonación**, proporcione todos los detalles requeridos.
7. En la página Ubicación, seleccione una ubicación de almacenamiento para crear un clon.

Si los volúmenes ANF de la base de datos de SQL Server están configurados en un grupo de capacidad de QOS manual, especifique la QOS para los volúmenes clonados.

Si no se especifica la calidad de servicio para los volúmenes clonados, se utilizará la calidad de servicio del volumen de origen. Si se utiliza el grupo de capacidad de QOS automático, se ignorará el valor de QOS especificado.

8. En la página **Script**, ingrese el tiempo de espera del script, la ruta y los argumentos del prescript o postscript que se deben ejecutar antes o después de la operación de clonación, respectivamente.
9. En la página Programación, realice una de las siguientes acciones:

- Seleccione **Ejecutar ahora** si desea ejecutar el trabajo de clonación inmediatamente.
 - Seleccione **Configurar programación** cuando desee determinar con qué frecuencia debe ocurrir la operación de clonación, cuándo debe comenzar la programación de clonación, en qué día debe ocurrir la operación de clonación, cuándo debe expirar la programación y si los clones deben eliminarse después de que expire la programación.
10. En la página **Notificación**, de la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
 11. Revise el resumen y luego seleccione **Finalizar**.
 12. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

Proteger las bases de datos de Oracle

Agregar hosts e instalar el complemento SnapCenter para la base de datos Oracle

Puede utilizar la página Agregar host para agregar hosts y luego instalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX. Los complementos se instalan automáticamente en los hosts remotos.

Puede agregar un host e instalar paquetes de complementos para un host individual o para un clúster. Si está instalando el complemento en un clúster (Oracle RAC), el complemento se instala en todos los nodos del clúster. Para Oracle RAC One Node, debe instalar el complemento en los nodos activos y pasivos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** 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 Nombre de host, ingrese el nombre de dominio completo (FQDN) o la dirección IP del host.
 - c. En el campo Credenciales, ingrese la credencial que creó.
5. En la sección Seleccionar complementos para instalar, seleccione los complementos que desea instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Haga clic en **Enviar**.
8. Verifique la huella digital y luego haga clic en **Confirmar y enviar**.

En una configuración de clúster, debe verificar la huella digital de cada uno de los nodos del clúster.

9. Supervisar el progreso de la instalación.

Crear políticas de respaldo para bases de datos de Oracle

Antes de utilizar SnapCenter para realizar copias de seguridad de los recursos de base de datos de Oracle, debe crear una política de copia de seguridad para el recurso o el grupo de recursos que desea respaldar.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Seleccione Oracle Database de la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Nombre, ingrese el nombre de la política y la descripción.
6. En la página Tipo de política, realice los siguientes pasos:
 - a. Seleccione * Azure NetApp Files* como tipo de almacenamiento.
 - b. Seleccione el tipo de copia de seguridad como copia de seguridad en línea o fuera de línea.
 - c. Si desea catalogar la copia de seguridad mediante Oracle Recovery Manager (RMAN), seleccione **Catalogar copia de seguridad con Oracle Recovery Manager (RMAN)**.
 - d. Si desea podar registros de archivo después de la copia de seguridad, seleccione **Podar registros de archivo después de la copia de seguridad**.
 - e. Especifique la configuración del registro de eliminación de archivo.
7. En la página Instantánea y copia de seguridad, realice los siguientes pasos:
 - a. Seleccione la frecuencia de la copia de seguridad programada.
 - 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, ingrese la ruta y los argumentos del prescript o postscript que desea ejecutar antes o después de la operación de respaldo, respectivamente.
9. En la página Verificación, seleccione la programación de copia de seguridad para la que desea realizar la operación de verificación e ingrese la ruta y los argumentos del prescript o postscript que desea ejecutar antes o después de la operación de verificación, respectivamente.
10. Revise el resumen y haga clic en **Finalizar**.

Crear grupos de recursos y adjuntar políticas de respaldo de Oracle

Un grupo de recursos es el contenedor al que debe agregar los recursos que desea respaldar y proteger.

Un grupo de recursos le permite realizar copias de seguridad de todos los datos asociados con una aplicación determinada simultáneamente. Se requiere un grupo de recursos para cualquier trabajo de protección de datos. También debe adjuntar 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, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, haga clic en **Nuevo grupo de recursos**.
3. En la página Nombre, realice las siguientes acciones:

Para este campo...	Haz esto...
Nombre	Introduzca un nombre para el grupo de recursos.
Etiquetas	Ingrese una o más etiquetas que le ayudarán a buscar posteriormente el grupo de recursos.
Utilice un formato de nombre personalizado para la copia de instantáneas	Seleccione esta casilla de verificación e ingrese el formato de nombre personalizado que desea utilizar para el nombre de la instantánea.
Destino del archivo de registro de archivo	Especifique los destinos de los archivos de registro de archivo.

- En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.
- Seleccione los recursos de la sección **Recursos disponibles** y luego haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
- En la página Políticas, realice los siguientes pasos:
 - Seleccione una o más políticas de la lista desplegable.
 - En la columna Configurar horarios, haga clic en *  * para la política que desea configurar.
 - En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego haga clic en **Aceptar**.
- En la página de Verificación, realice los siguientes pasos:
 - Seleccione el servidor de verificación.
 - Seleccione la política para la que desea configurar su programa de verificación y luego haga clic en *  .
 - Seleccione **Ejecutar verificación después de la copia de seguridad** o **Ejecutar verificación programada**.
 - Haga clic en **Aceptar**.
- En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
- Revise el resumen y luego haga clic en **Finalizar**.

Realizar copias de seguridad de bases de datos de Oracle que se ejecutan en Azure NetApp Files

Si un recurso aún no forma parte de ningún grupo de recursos, puede realizar una copia de seguridad del recurso desde la página Recursos.

Pasos

- En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.

2. En la página Recursos, seleccione **Base de datos** en la lista desplegable Ver.
3. En la página Recursos, seleccione **Usar formato de nombre personalizado para copia de instantánea** y luego ingrese el formato de nombre personalizado que desee usar para el nombre de la instantánea.
4. En la página Políticas, realice los siguientes pasos:
 - a. Seleccione una o más políticas de la lista desplegable.
 - b. Seleccione *  * en la columna Configurar programaciones de la política para la que desea configurar una programación.
 - c. En el cuadro de diálogo Agregar programaciones para la política *policy_name*, configure la programación y luego seleccione **Aceptar**.
5. En la página de Verificación, realice los siguientes pasos:
 - a. Seleccione el servidor de verificación.
 - b. Seleccione la política para la que desea configurar su programa de verificación y luego haga clic en *  *.
 - c. Seleccione **Ejecutar verificación después de la copia de seguridad** o **Ejecutar verificación programada**.
 - d. Haga clic en Aceptar.
6. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
7. Revise el resumen y luego haga clic en **Finalizar**.
8. Seleccione **Hacer copia de seguridad ahora**.
9. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si hay varias políticas asociadas al recurso, en la lista desplegable **Política**, seleccione la política que desea utilizar para la copia de seguridad.
 - b. Haga clic en **Copia de seguridad**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Realizar copias de seguridad de grupos de recursos de Oracle

Puede realizar copias de seguridad de los grupos de recursos que constan de varios recursos. Se realiza una operación de copia de seguridad en el grupo de recursos en todos los recursos definidos en el grupo de recursos.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista Ver.
3. En la página Grupos de recursos, seleccione el grupo de recursos que desea respaldar y luego seleccione **Hacer copia de seguridad ahora**.
4. En la página Copia de seguridad, realice los siguientes pasos:
 - a. Si hay varias políticas asociadas al grupo de recursos, en la lista desplegable **Política**, seleccione la política que desea utilizar 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 Oracle

En caso de pérdida de datos, puede utilizar SnapCenter para restaurar datos de una o más copias de seguridad en su sistema de archivos activo y luego recuperar la base de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de la lista.
4. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento principal.
5. Seleccione la copia de seguridad de la tabla y luego haga clic en *  *.
6. En la página Restaurar ámbito, realice las siguientes tareas:
 - a. Seleccione RAC si ha seleccionado una copia de seguridad 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 **Espacios de tabla** si desea restaurar solo los espacios de tabla.
 - iii. Seleccione **Rehacer archivos de registro** si desea restaurar los archivos de registro de rehacer de las bases de datos de espera de Data Guard o de espera de Data Guard activo.
 - iv. Seleccione **Bases de datos conectables** y especifique los PDB que desea restaurar.
 - v. Seleccione **Espacios de tabla de base de datos conectable (PDB)** y, a continuación, especifique la PDB y los espacios de tabla 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 realizaron las copias de seguridad.
 - vii. Seleccione **Restaurar la base de datos en un host alternativo** si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o en uno diferente donde se realizan 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 **Forzar restauración en el lugar** si desea realizar una restauración en el lugar en los escenarios en los que se agregan nuevos archivos de datos después de la copia de seguridad o cuando se agregan, eliminan o vuelven a crear LUN en un grupo de discos LVM.
7. En la página Ámbito de recuperación, seleccione una de las siguientes opciones:
 - a. Seleccione **Todos los registros** si desea recuperar la última transacción.
 - b. Seleccione **Hasta SCN (Número de cambio de sistema)** si desea recuperar un SCN específico.

- c. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
- d. Seleccione **Sin recuperación** si no desea recuperar.
- e. Seleccione **Especificar ubicaciones de registros de archivo externos** si desea especificar la ubicación de los archivos de registro de archivo externos.
8. En la página Preoperatorio y Postoperatorio, especifique los detalles requeridos.
9. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y luego haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor > Trabajos**.

Restaurar y recuperar espacios de tabla mediante la recuperación en un punto en el tiempo

Puede restaurar un subconjunto de espacios de tabla que se hayan dañado o eliminado sin afectar a los demás espacios de tabla de la base de datos. SnapCenter utiliza RMAN para realizar la recuperación en un punto en el tiempo (PITR) de los espacios de tabla.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de tipo instancia única (multiinquilino).
4. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento.

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione la copia de seguridad catalogada y luego haga clic en *  *.
6. En la página Restaurar ámbito, 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 **Espacios de tabla** si desea restaurar solo los espacios de tabla.
 - 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 Ámbito de recuperación, seleccione una de las siguientes opciones:
 - a. Seleccione **Hasta SCN (Número de cambio de sistema)** si desea recuperar un SCN específico.
 - b. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
8. En la página Preoperatorio y Postoperatorio, especifique los detalles requeridos.
9. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y luego haga clic en **Finalizar**.
11. Supervise el proceso de restauración utilizando la página **Monitor > Trabajos**.

Restaurar y recuperar bases de datos conectables mediante recuperación en un punto determinado del tiempo

Puede restaurar y recuperar una base de datos conectable (PDB) que se haya dañado o eliminado sin afectar a las otras PDB en la base de datos contenedora (CDB). SnapCenter utiliza RMAN para realizar la recuperación en un punto en el tiempo (PITR) del PDB.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de tipo instancia única (multiinquilino).
4. Desde la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento.

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione la copia de seguridad catalogada y luego haga clic en *  *.
6. En la página Restaurar ámbito, realice las siguientes tareas:
 - a. Seleccione **RAC** si ha seleccionado una copia de seguridad de una base de datos en el entorno RAC.
 - b. Dependiendo de si desea restaurar el PDB o los espacios de tabla en un PDB, realice una de las acciones:
 - Seleccione **Bases de datos conectables (PDB)** si desea restaurar una PDB.
 - Seleccione **Espacios de tabla de base de datos conectable (PDB)** si desea restaurar espacios de tabla en una PDB.
7. En la página Ámbito de recuperación, seleccione una de las siguientes opciones:
 - a. Seleccione **Hasta SCN (Número de cambio de sistema)** si desea recuperar un SCN específico.
 - b. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
8. En la página Preoperatorio y Postoperatorio, especifique los detalles requeridos.
9. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y luego haga clic en **Finalizar**.
11. Supervise el proceso de restauración utilizando la página **Monitor > Trabajos**.

Copia de seguridad de la base de datos Clonar Oracle

Puede utilizar SnapCenter para clonar una base de datos Oracle utilizando la copia de seguridad de la base de datos. Los clones creados son clones gruesos y se crean en el grupo de capacidad principal.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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. Desde la página de vista Administrar copias, seleccione la copia de seguridad del sistema de almacenamiento principal.
5. Seleccione la Copia de seguridad de datos y luego haga clic en *  *.
6. En la página Nombre, seleccione si desea clonar una base de datos (CDB o no CDB) o clonar una base de datos conectable (PDB).
7. En la página Ubicaciones, especifique los detalles requeridos.

Si los volúmenes ANF de la base de datos Oracle están configurados en un grupo de capacidad de QOS manual, especifique el QOS para los volúmenes clonados.

Si no se especifica la calidad de servicio para los volúmenes clonados, se utilizará la calidad de servicio del volumen de origen. Si se utiliza el grupo de capacidad de QOS automático, se ignorará el valor de QOS especificado.

8. En la página Credenciales, realice una de las siguientes acciones:
 - a. Para el nombre de credencial para el usuario del sistema, seleccione la credencial que se utilizará para definir la contraseña del usuario del sistema 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 habilitada para conectarse a la instancia de ASM en el host clonado.

De lo contrario, seleccione la credencial Oracle ASM configurada con el usuario “sys” o un usuario que tenga el privilegio “sysasm” aplicable al host clonado.

9. En la página Pre-Ops, especifique la ruta y los argumentos de los prescripts y, en la sección Configuración de parámetros de base de datos, modifique los valores de los parámetros de base de datos precargados que se utilizan para inicializar la base de datos.
10. En la página Postoperatorio, **Recuperar base de datos** y **Hasta cancelar** están seleccionados de manera predeterminada para realizar la recuperación de la base de datos clonada.
 - a. Si selecciona **Hasta cancelar**, SnapCenter realiza la recuperación montando la última copia de seguridad del registro que tiene la secuencia ininterrumpida de registros de archivo después de esa copia de seguridad de datos que se seleccionó para clonar.
 - b. Si selecciona **Fecha y hora**, SnapCenter recupera la base de datos hasta una fecha y hora especificadas.
 - c. Si selecciona **Hasta SCN**, SnapCenter recupera la base de datos hasta un SCN especificado.
 - d. Si selecciona **Especificar ubicaciones de registros de archivo externos**, SnapCenter identifica y monta la cantidad óptima de copias de seguridad de registros según el SCN especificado o la fecha y hora seleccionadas.
 - e. De forma predeterminada, 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.

Desmarque la casilla de verificación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En este escenario, si desea registrar la base de datos clonada con el catálogo RMAN externo donde la base de datos de origen ya está registrada, la operación falla.

- f. Seleccione la casilla de verificación **Crear archivo temporal para espacio de tabla temporal** si desea crear un archivo temporal para el espacio de tabla temporal predeterminado de la base de datos clonada.

- g. En **Ingresar entradas SQL para aplicar cuando se crea el clon**, agregue las entradas SQL que desea aplicar cuando se crea el clon.
- h. En **Ingresar scripts para ejecutar después de la operación de clonación**, especifique la ruta y los argumentos del postscript que desea ejecutar después de la operación de clonación.
11. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
12. Revise el resumen y luego seleccione **Finalizar**.
13. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

Clonar una base de datos conectable

Puede clonar una base de datos conectable (PDB) a una CDB de destino diferente o igual en el mismo host o en un host alternativo. También puede recuperar el PDB clonado en un SCN o fecha y hora deseados.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de tipo instancia única (multiinquilino).
4. Desde la página de vista Administrar copias, seleccione la copia de seguridad del sistema de almacenamiento principal.
5. Seleccione la copia de seguridad y luego haga clic en *  *.
6. En la página Nombre, seleccione **PDB Clone** y especifique los demás detalles.
7. En la página Ubicaciones, especifique los detalles requeridos.
8. En la página Pre-Ops, especifique la ruta y los argumentos de los prescripts y, en la sección Configuración de parámetros de base de datos, modifique los valores de los parámetros de base de datos precargados que se utilizan para inicializar la base de datos.
9. En la página Postoperatorio, **Hasta cancelar** está seleccionado de forma predeterminada para realizar la recuperación de la base de datos clonada.
 - a. Si selecciona **Hasta cancelar**, SnapCenter realiza la recuperación montando la última copia de seguridad del registro que tiene la secuencia ininterrumpida de registros de archivo después de esa copia de seguridad de datos que se seleccionó para clonar.
 - b. Si selecciona **Fecha y hora**, SnapCenter recupera la base de datos hasta una fecha y hora especificadas.
 - c. Si selecciona **Especificar ubicaciones de registros de archivo externos**, SnapCenter identifica y monta la cantidad óptima de copias de seguridad de registros según el SCN especificado o la fecha y hora seleccionadas.
 - d. De forma predeterminada, 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.

Desmarque la casilla de verificación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En este escenario, si desea registrar la base de datos clonada con el catálogo RMAN externo donde la base de datos de origen ya está registrada, la operación falla.
 - e. Seleccione la casilla de verificación **Crear archivo temporal para espacio de tabla temporal** si desea crear un archivo temporal para el espacio de tabla temporal predeterminado de la base de datos

clonada.

- f. En **Ingresar entradas SQL para aplicar cuando se crea el clon**, agregue las entradas SQL que desea aplicar cuando se crea el clon.
 - g. En **Ingresar scripts para ejecutar después de la operación de clonación**, especifique la ruta y los argumentos del postscript que desea ejecutar después de la operación de clonación.
10. En la página de Notificaciones, en la lista desplegable **Preferencias de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
 11. Revise el resumen y luego seleccione **Finalizar**.
 12. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

Administrar SnapCenter Server y complementos

Ver el panel de control

Descripción general del panel de control

Desde el panel de navegación izquierdo de SnapCenter , el Tablero le brinda un primer vistazo del estado de su sistema, incluida la actividad laboral reciente, alertas, resumen de protección, uso y eficiencia del almacenamiento, estado de los trabajos de SnapCenter (Copia de seguridad, Clonación, Restauración), estado de configuración para hosts independientes y de clúster de Windows, cantidad de máquinas virtuales de almacenamiento (SVM) administradas por SnapCenter y capacidad de licencia.

La información que se muestra en la vista del Panel depende del rol asignado al usuario que actualmente está conectado a SnapCenter. Es posible que algunos contenidos no se muestren si el usuario no tiene permiso para ver esa información.

En muchos casos, puedes ver más información sobre una pantalla colocando el cursor sobre **i**. En algunos casos, la información que se muestra en el panel está vinculada a información de origen detallada en las páginas de la GUI de SnapCenter , como Recursos, Monitor e Informes.

Actividades laborales recientes

El mosaico Actividades laborales recientes muestra la actividad laboral más reciente de cualquier trabajo de Copia de seguridad, Restauración y Clonación al que tenga acceso. Los trabajos en esta pantalla tienen uno de los siguientes estados: Completado, Advertencia, Fallido, En ejecución, En cola y Cancelado.

Al pasar el cursor sobre un trabajo se proporciona más información. Puede ver información adicional del trabajo haciendo clic en un número de trabajo específico, lo que lo redireccionará a la página Monitor. Desde allí, puede obtener detalles del trabajo o registrar información y generar un informe específico para ese trabajo.

Haga clic en **Ver todo** para ver un historial de todos los trabajos de SnapCenter .

Alertas

El mosaico Alertas muestra las últimas alertas críticas y de advertencia sin resolver para los hosts y el servidor SnapCenter .

El recuento total de alertas de categoría Crítica y Advertencia se muestra en la parte superior de la pantalla. Al hacer clic en los totales críticos o de advertencia, se le redirigirá a la página de Alertas con el filtro específico aplicado en la página de Alertas.

Al hacer clic en una alerta específica, se le redirigirá a la página Alertas para obtener detalles sobre esa alerta. Al hacer clic en **Ver todo** en la parte inferior de la pantalla, se le redirigirá a la página de Alertas para obtener una lista de todas las alertas.

Resumen de protección más reciente

El mosaico Resumen de protección más reciente le brinda el estado de protección de todas las entidades a las que tiene acceso. De forma predeterminada, la pantalla está configurada para proporcionar el estado de todos los complementos. Se proporciona información sobre el estado de los recursos respaldados en el

almacenamiento principal como instantáneas y en el almacenamiento secundario mediante las tecnologías SnapMirror y SnapVault . La disponibilidad de la información sobre el estado de protección para el almacenamiento secundario se basa en el tipo de complemento seleccionado.



Si está utilizando una política de protección de bóveda reflejada, los contadores del resumen de protección se muestran en el gráfico de resumen de SnapVault y no en el gráfico de SnapMirror

El estado de protección de los complementos individuales está disponible seleccionando un complemento en el menú desplegable. Un gráfico de anillo muestra el porcentaje de recursos protegidos del complemento seleccionado. Al hacer clic en un segmento de anillo, se le redirige a la página **Informes > Complemento**, que proporciona un informe detallado de toda la actividad de almacenamiento principal y secundario del complemento especificado.



Los informes sobre almacenamiento secundario se aplican únicamente a SnapVault ; los informes de SnapMirror no son compatibles.



SAP HANA proporciona información sobre el estado de protección para el almacenamiento primario y secundario para instantáneas. Solo el estado de protección de almacenamiento principal está disponible para las copias de seguridad basadas en archivos.

Estado de protección	Almacenamiento primario	Almacenamiento secundario
Con errores	Recuento de entidades que forman parte de un grupo de recursos, donde el grupo de recursos ejecutó una copia de seguridad, pero esta falló.	Recuento de entidades con copias de seguridad que no se pudieron transferir a un destino secundario.
Exitoso	Recuento de entidades en un grupo de recursos, donde se realizó una copia de seguridad exitosa del grupo de recursos.	Recuento de entidades con copias de seguridad que se han transferido correctamente a un destino secundario.
No configurado	Recuento de entidades que no forman parte de ningún grupo de recursos y que no han sido respaldadas.	Recuento de entidades que forman parte de uno o más grupos de recursos que no están configurados para que las copias de seguridad se transfieran a un destino secundario.
No iniciado	Recuento de entidades que forman parte de un grupo de recursos, pero no se ha ejecutado ninguna copia de seguridad.	No aplicable.



Si está utilizando SnapCenter Server 4.2 y una versión anterior del complemento (anterior a 4.2) para crear copias de seguridad, el mosaico **Resumen de protección más reciente** no muestra el estado de protección de SnapMirror de estas copias de seguridad.

Empleos

El mosaico Trabajos le proporciona un resumen de los trabajos de copia de seguridad, restauración y clonación a los que tiene acceso. Puede personalizar el período de tiempo para cualquier informe utilizando el menú desplegable. Las opciones de marco de tiempo se fijan en las últimas 24 horas, los últimos 7 días y los últimos 30 días. El informe predeterminado muestra los trabajos de protección de datos ejecutados durante los últimos 7 días.

La información de los trabajos de copia de seguridad, restauración y clonación se muestra en gráficos de anillos. Al hacer clic en un segmento de dona, se le redirige a la página Monitor con filtros de trabajo aplicados previamente a la selección.

Estado del trabajo	Descripción
Con errores	Recuento de trabajos que han fallado.
Advertencia	Recuento de trabajos que han experimentado un error.
Exitoso	Recuento de trabajos que se han completado con éxito.
Correr	Recuento de trabajos que se están ejecutando actualmente.

Almacenamiento

El mosaico Almacenamiento muestra el almacenamiento primario y secundario consumido por los trabajos de protección durante un período de 90 días, representa gráficamente las tendencias de consumo y calcula los ahorros de almacenamiento primario. La información de almacenamiento se actualiza una vez cada 24 horas a las 12 a. m.

El consumo total del día, que incluye la cantidad total de copias de seguridad disponibles en SnapCenter y el tamaño ocupado por estas copias de seguridad, se mostrará en la parte superior de la pantalla. Una copia de seguridad podría tener varias instantáneas asociadas y el recuento reflejará lo mismo. Esto se aplica tanto a las instantáneas primarias como a las secundarias. Por ejemplo, ha creado 10 copias de seguridad, de las cuales 2 se eliminan debido a la retención de copias de seguridad basada en políticas y 1 copia de seguridad es eliminada explícitamente por usted. De esta forma se mostrará un recuento de 7 copias de seguridad junto con el tamaño ocupado por estas 7 copias de seguridad.

El factor de ahorro de almacenamiento para el almacenamiento primario es la relación entre la capacidad lógica (ahorro de clones e instantáneas más el almacenamiento consumido) y la capacidad física del almacenamiento primario. Un gráfico de barras ilustra el ahorro de almacenamiento.

El gráfico de líneas representa por separado el consumo de almacenamiento primario y secundario día a día durante un período continuo de 90 días. Al pasar el cursor sobre los gráficos se obtienen resultados detallados día a día.



Si usa SnapCenter Server 4.2 y una versión anterior del complemento (anterior a 4.2) para crear copias de seguridad, el mosaico **Almacenamiento** no muestra la cantidad de copias de seguridad, el almacenamiento consumido por estas copias de seguridad, los ahorros de instantáneas, los ahorros de clones y el tamaño de las instantáneas.

Configuración

El mosaico Configuración proporciona información de estado consolidada para todos los hosts activos independientes y de clúster de Windows que SnapCenter administra y a los que usted tiene acceso. Esto incluye la información del estado del complemento asociado con esos hosts.

Al hacer clic en el número junto a Hosts, se le redirigirá a la sección Hosts administrados en la página Hosts. Desde allí, puede obtener información detallada de un host seleccionado.

Además, esta pantalla muestra la suma de las SVM independientes de ONTAP y las SVM de Cluster ONTAP que administra SnapCenter y a las que usted tiene acceso. Al hacer clic en el número junto a SVM, se le redirigirá a la página Sistemas de almacenamiento. Desde allí, puede obtener información detallada de un SVM seleccionado.

El estado de configuración del host se presenta como rojo (crítico), amarillo (advertencia) y verde (activo), junto con la cantidad de hosts en cada estado. Se proporcionan mensajes de estado para cada estado.

Estado de configuración	Descripción
Actualización obligatoria	Recuento de hosts que ejecutan complementos no compatibles y necesitan una actualización. Un complemento no compatible no es compatible con esta versión de SnapCenter.
Migración obligatoria	Recuento de hosts que ejecutan complementos no compatibles y necesitan migración. Un complemento no compatible no es compatible con esta versión de SnapCenter.
No hay complementos instalados	Recuento de hosts que se agregaron correctamente pero es necesario instalar los complementos o la instalación de los complementos falló.
Suspendida	Recuento de hosts cuyos horarios están suspendidos y se encuentran en mantenimiento.
Detenido	Recuento de hosts que están activos, pero los servicios del complemento no se están ejecutando.
Host caído	Recuento de hosts que están inactivos o no son accesibles.
Actualización disponible (opcional)	Cantidad de hosts donde hay una versión más nueva del paquete de complemento disponible para actualización.
Migración disponible (opcional)	Cantidad de hosts donde hay una versión más nueva del complemento disponible para la migración.

Estado de configuración	Descripción
Configurar el directorio de registro	Cantidad de hosts donde se debe configurar el directorio de registro para que SCSQL realice una copia de seguridad del registro de transacciones.
Configurar complementos de VMware	Cantidad de hosts donde es necesario agregar el SnapCenter Plug-in for VMware vSphere .
Desconocido	Recuento de hosts que se han registrado pero cuya instalación aún no se ha activado.
Correr	Recuento de hosts que están activos y complementos en ejecución. Y en el caso de los complementos SCSQL, se configuran el directorio de registro y el hipervisor.
Instalación/desinstalación de complementos	Recuento de hosts donde la instalación o desinstalación del complemento está en curso.

Cómo ver información en el panel de control

Desde el panel de navegación izquierdo de SnapCenter , puede ver varios mosaicos o pantallas del Tablero, junto con los detalles del sistema asociados. La cantidad de pantallas disponibles en el Tablero es fija y no se puede cambiar. El contenido proporcionado en cada pantalla depende del control de acceso basado en roles (RBAC).

Pasos

1. En el panel de navegación izquierdo, haga clic en **Panel de control**.
2. Haga clic en las áreas activas de cada pantalla para obtener información adicional.

Por ejemplo, al hacer clic en un gráfico de anillos en **Trabajos**, se le redirige a la página Monitor para obtener más información sobre su selección. Al hacer clic en un gráfico de anillos en **Resumen de protección**, se le redirigirá a la página Informes, que puede proporcionarle más información sobre su selección.

Solicitar informes de estado de los trabajos desde el panel de control

Puede solicitar informes sobre trabajos de copia de seguridad, restauración y clonación desde la página del Panel de control. Esto es útil si desea identificar la cantidad total de trabajos exitosos o fallidos en su entorno de SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Panel de control**
2. Localice el mosaico Trabajos en el Panel de Control y luego seleccione **Copia de Seguridad, Restaurar o Clonar**.

3. Utilizando el menú desplegable, seleccione el período de tiempo para el cual desea información de trabajos: 24 horas, 7 días o 30 días.

Los sistemas muestran un gráfico de anillos que cubre los datos.

4. Haga clic en el segmento de dona que representa la información del trabajo para el cual desea un informe.

Al hacer clic en el gráfico de anillos, se le redirige de la página del Panel a la página del Monitor. La página Monitor muestra los trabajos con el estado seleccionado en el gráfico de anillos.

5. Desde 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 únicamente para el trabajo seleccionado. Puede revisar el informe o descargarlo a su sistema local.

Solicitar informes del estado de protección desde el panel de control

Puede solicitar detalles de protección para recursos administrados por complementos específicos mediante el Panel de control. Para el resumen de protección de datos solo se consideran las copias de seguridad de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Panel de control**.
2. Localice el mosaico Resumen de protección más reciente en el Panel de control y utilice el menú desplegable para seleccionar un complemento.

El panel muestra un gráfico de anillos para los recursos respaldados en el almacenamiento principal y, si corresponde al complemento, un gráfico de anillos para los recursos respaldados en el almacenamiento secundario.



Los informes de protección de datos solo están disponibles para tipos de complementos específicos. No se admite la especificación de **Todos los complementos**.

3. Haga clic en el segmento de dona que representa el estado para el que desea un informe.

Al hacer clic en el gráfico de anillos, se le redirige de la página del Panel a los Informes y, luego, a la página del Complemento. El informe muestra solo el estado del complemento que seleccionó. Puede revisar el informe o descargarlo a su sistema local.



No se admite la redirección a la página Informes para el gráfico de anillos de SnapMirror ni para la copia de seguridad de SAP HANA basada en archivos.

Administrar RBAC

SnapCenter le permite modificar roles, usuarios y grupos.

Modificar un rol

Puede modificar una función de SnapCenter para eliminar usuarios o grupos y cambiar los permisos asociados con la función. Es especialmente útil modificar roles cuando desea cambiar o eliminar los permisos utilizados por un rol completo.

Antes de empezar

Debe haber iniciado sesión como rol "SnapCenterAdmin".



No puede modificar ni eliminar permisos para la función SnapCenterAdmin.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Roles**.
3. Desde el campo Nombre del rol, haga clic en el rol que desea modificar.
4. Seleccione **Todos los miembros de este rol pueden ver los objetos de otros miembros** para permitir que otros miembros del rol 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 de este rol vean los objetos a los que están asignados otros miembros.



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

5. En la página Detalles del rol, modifique los permisos o cancele la asignación de los miembros según sea necesario.
6. Haga clic en **Enviar**.

Modificar usuarios y grupos

Puede modificar usuarios o grupos de SnapCenter para cambiar sus roles y activos.

Antes de empezar

Debe iniciar sesión como administrador de SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Usuarios y acceso**.
3. Desde la lista de nombres de usuario o grupo, haga clic en el usuario o grupo que desee modificar.
4. En la página de detalles de Usuario o Grupo, modifique los roles y activos.
5. Haga clic en **Enviar**.

Administrar hosts

Puede agregar hosts e instalar paquetes de complementos de SnapCenter , agregar un servidor de verificación, eliminar hosts, migrar trabajos de respaldo y actualizar hosts para actualizar paquetes de complementos o agregar nuevos paquetes de complementos. Según el complemento que utilice, también puede aprovisionar discos, administrar recursos compartidos SMB, administrar grupos de iniciadores (igroups), administrar sesiones iSCSI y migrar datos.

Puedes realizar estas tareas...	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para la base de datos Oracle	Para la base de datos SAP HANA	Para complementos compatibles con NetApp	Para Db2	Para PostgreSQL	Para MySQL
Agregar hosts e instalar el paquete de complemento	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
Suspender programaciones y colocar hosts en modo de mantenimiento	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Puedes realizar estas tareas...	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para la base de datos Oracle	Para la base de datos SAP HANA	Para complementos compatibles con NetApp	Para Db2	Para PostgreSQL	Para MySQL
Modificar hosts agregando, actualizando o eliminando complementos	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Eliminar hosts de SnapCenter	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Iniciar servicios de complemento (solo aplicable para complementos que se ejecutan en el host de Windows)	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Discos de aprovisionamiento	No	No	Sí	No	No	No	No	No	No
Administrar recursos compartidos de SMB	No	No	Sí	No	No	No	No	No	No

Puedes realizar estas tareas...	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para la base de datos Oracle	Para la base de datos SAP HANA	Para complementos compatibles con NetApp	Para Db2	Para PostgreSQL	Para MySQL
Administrar iGroups	No	No	Sí	No	No	No	No	No	No
Administrar sesiones iSCSI	No	No	Sí	No	No	No	No	No	No

Actualizar la información de la máquina virtual

Debe actualizar la información de su máquina virtual cuando cambien las credenciales de VMware vCenter o cuando se reinicie el host del sistema de archivos o de la base de datos. Al actualizar la información de su máquina virtual en SnapCenter, se inicia la comunicación con VMware vSphere vCenter y se obtienen las credenciales de vCenter.



Los discos basados en RDM son administrados por el complemento SnapCenter para Microsoft Windows, que está instalado en el host de la base de datos. Para administrar RDM, el complemento SnapCenter para Microsoft Windows se comunica con el servidor vCenter que administra 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 **Hosts administrados**.
3. En la página Hosts administrados, seleccione el host que desea actualizar.
4. Haga clic en **Actualizar VM**.

Modificar los hosts de los complementos

Después de instalar un complemento, puede modificar los detalles de los hosts del complemento si es necesario. Puede modificar las credenciales, la ruta de instalación, los complementos, los detalles del directorio de registro del complemento de SnapCenter para Microsoft SQL Server, la cuenta de servicio administrada de grupo (gMSA) y el puerto del complemento.



Asegúrese de que la versión del complemento sea la misma que la versión de SnapCenter Server.

Acerca de esta tarea

- Puedes modificar un puerto de complemento solo después de instalar el complemento.

No es posible modificar el puerto del complemento mientras se realizan operaciones de actualización.

- Al modificar un puerto de complemento, debe tener en cuenta los siguientes escenarios de reversión de puerto:
 - En una configuración independiente, si SnapCenter no logra cambiar el puerto de uno de los componentes, la operación falla y el puerto antiguo se conserva para todos los componentes.

Si se cambió el puerto para todos los componentes pero uno de los componentes no puede iniciarse con el nuevo puerto, entonces el puerto antiguo se conserva para todos los componentes. Por ejemplo, si desea cambiar el puerto de dos complementos en el host independiente y SnapCenter no logra aplicar el nuevo puerto a uno de los complementos, la operación falla (con un mensaje de error apropiado) y el puerto antiguo se conserva para ambos complementos.

 - En una configuración en clúster, si SnapCenter no logra cambiar el puerto del complemento que está instalado en uno de los nodos, la operación falla y el puerto antiguo se conserva para todos los nodos.
- Por ejemplo, si el complemento está instalado en cuatro nodos en una configuración en clúster y no se cambia el puerto para uno de los nodos, el puerto antiguo se conserva para todos los nodos.

Cuando se instalan complementos con gMSA, puedes modificarlos en la ventana **Más opciones**. Cuando se instalan complementos sin gMSA, puede especificar la cuenta gMSA para utilizarla como cuenta de servicio del complemento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que **Hosts administrados** esté seleccionado en la parte superior.
3. Seleccione el host que desea modificar y modifique cualquier campo.

Sólo se puede modificar un campo a la vez.

4. Haga clic en **Enviar**.

Resultado

El host se valida y se agrega al servidor SnapCenter .

Iniciar o reiniciar los servicios del complemento

Al iniciar los servicios del complemento SnapCenter , podrá iniciar servicios si no se están ejecutando o reiniciarlos si se están ejecutando. Es posible que desee reiniciar los servicios después de realizar el mantenimiento.

Debe asegurarse de que no haya ningún trabajo en ejecución al reiniciar los servicios.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. En la página Hosts administrados, seleccione el host que desea iniciar.
4. Hacer clic  icono y haga clic en **Iniciar servicio** o **Reiniciar servicio**.

Puede iniciar o reiniciar el servicio de varios hosts simultáneamente.

Suspender programaciones para mantenimiento del host

Cuando desee evitar que el host ejecute cualquier trabajo programado de SnapCenter , puede colocarlo en modo de mantenimiento. Debe hacer esto antes de actualizar los complementos o si está realizando tareas de mantenimiento en los hosts.



No se pueden suspender las programaciones en un host que está inactivo porque SnapCenter no puede comunicarse con ese host.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. En la página Hosts administrados, 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 complemento en modo de mantenimiento.

Puede suspender la programación de varios hosts simultáneamente.



No es necesario detener primero el servicio de complemento. El servicio de complemento puede estar en estado de ejecución o detenido.

Resultado

Después de suspender las programaciones en el host, la página Hosts administrados muestra **Suspendido** en el campo Estado general del host.

Después de completar el mantenimiento del host, puede sacarlo del modo de mantenimiento haciendo clic en **Activar programación**. Puede activar la programación de varios hosts simultáneamente.

Operaciones respaldadas desde la página de Recursos

Puede descubrir recursos y realizar operaciones de protección de datos desde la página Recursos. Las operaciones que puedes realizar varían según el complemento que estés utilizando para administrar tus recursos.

Desde la página Recursos, puede realizar las siguientes tareas:

Puedes realizar estas tareas...	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para la base de datos Oracle	Para la base de datos SAP HANA
Determinar si hay recursos disponibles para realizar copias de seguridad	Sí	Sí	Sí	Sí	Sí

Puedes realizar estas tareas...	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para la base de datos Oracle	Para la base de datos SAP HANA
Realizar una copia de seguridad a pedido de un recurso	Sí	Sí	Sí	Sí	Sí
Restaurar desde copias de seguridad	Sí	Sí	Sí	Sí	Sí
Copias de seguridad clonadas	No	Sí	Sí	Sí	Sí
Administrar copias de seguridad	Sí	Sí	Sí	Sí	Sí
Administrar clones	No	Sí	Sí	Sí	Sí
Administrar políticas	Sí	Sí	Sí	Sí	Sí
Administrar conexiones de almacenamiento	Sí	Sí	Sí	Sí	Sí
Montar copias de seguridad	No	No	No	Sí	No
Desmontar copias de seguridad	No	No	No	Sí	No
Ver detalles	Sí	Sí	Sí	Sí	Sí

Administrar políticas

Puede separar políticas de un recurso o grupo de recursos, modificarlas, eliminarlas, verlas y copiarlas.

Modificar políticas

Puede modificar las opciones de replicación, la configuración de retención de instantáneas, el recuento de reintentos de error o la información de los scripts mientras una política está asociada a un recurso o grupo de recursos. Puede modificar el tipo de programación (frecuencia) solo después de separar una política.

Acerca de esta tarea

Modificar el tipo de programación en una política requiere pasos adicionales porque SnapCenter Server registra el tipo de programación solo en el momento en que la política se adjunta a un recurso o grupo de recursos.

Si quieres...	Entonces...
Agregar un tipo de programación adicional	Cree una nueva política y adjúntela a los recursos o grupos de recursos necesarios. Por ejemplo, si una política de grupo de recursos especifica solo copias de seguridad cada hora y desea agregar también copias de seguridad diarias, puede crear una política con un tipo de programación diaria y agregarla al grupo de recursos. El grupo de recursos tendría entonces dos políticas: horaria y diaria.
Eliminar o cambiar un tipo de programación	Realice lo siguiente: 1. Separe la política de cada recurso y grupo de recursos que utilice esa política. 2. Modificar el tipo de programación. 3. Adjunte la política nuevamente a todos los recursos y grupos de recursos. Por ejemplo, si una política especifica copias de seguridad cada hora y desea cambiarlas a copias de seguridad diarias, primero debe separar la política.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Seleccione la política y luego haga clic en **Modificar**.
4. Modifique la información y luego haga clic en **Finalizar**.

Desvincular políticas

Puede separar políticas de un recurso o grupo de recursos en cualquier momento si ya no desea que esas políticas rijan la protección de datos de los recursos. Debes separar una política antes de poder eliminarla o antes de modificar el tipo de programación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
3. Seleccione el grupo de recursos y luego haga clic en **Modificar grupo de recursos**.
4. En la página Políticas del asistente Modificar grupo de recursos, en la lista desplegable, desmarque la marca de verificación junto a las políticas que desea separar.
5. Realice cualquier modificación adicional al grupo de recursos en el resto del asistente y luego haga clic en **Finalizar**.

Eliminar políticas

Si ya no necesita las políticas, es posible que desee eliminarlas.

Antes de empezar

Debe separar la política del recurso o del grupo de recursos si la política está asociada con algún recurso o grupo de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Políticas**.
3. Seleccione la política y luego haga clic en **Eliminar**.
4. Haga clic en **Sí**.

Administrar grupos de recursos

Puede realizar varias operaciones en grupos de recursos.

Puede realizar las siguientes tareas relacionadas con los grupos de recursos:

- Modifique un grupo de recursos seleccionándolo y haciendo clic en **Modificar grupo de recursos** para editar la información que proporcionó al crear el grupo de recursos.



Puede cambiar la programación mientras modifica el grupo de recursos. Sin embargo, para cambiar el tipo de programación es necesario modificar la política.



Si elimina recursos de un grupo de recursos, las configuraciones de retención de copias de seguridad definidas en las políticas actualmente asociadas al grupo de recursos seguirán aplicándose a los recursos eliminados.

- Crear una copia de seguridad de un grupo de recursos.
- Crear un clon de una copia de seguridad.

Puede clonar desde las copias de seguridad existentes de SQL, Oracle, sistemas de archivos de Windows, aplicaciones personalizadas y recursos de bases de datos o grupos de recursos de SAP HANA.

- Crear un clon de un grupo de recursos.

Esta operación solo se admite 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 la clonación).

- Evitar que se inicien operaciones programadas en grupos de recursos.
- Eliminar un grupo de recursos.

Detener y reanudar operaciones en grupos de recursos

Puede deshabilitar temporalmente el inicio de operaciones programadas en un grupo de recursos. Más tarde, cuando lo desees, podrás habilitar esas operaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
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 había puesto en modo de mantenimiento, seleccione el grupo de recursos y haga clic en **Producción**.

Eliminar grupos de recursos

Puede eliminar un grupo de recursos si ya no necesita proteger los recursos del grupo de recursos. Debe asegurarse de que los grupos de recursos se eliminen antes de quitar complementos de SnapCenter.

Acerca de esta tarea

Debe eliminar manualmente todos los clones creados para cualquiera de los recursos del grupo de recursos. Opcionalmente, puede forzar la eliminación de todas las copias de seguridad, metadatos, políticas e instantáneas asociadas con el grupo de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione **Grupo de recursos** de la lista **Ver**.
3. Seleccione el grupo de recursos y haga clic en **Eliminar**.
4. Opcional: seleccione la casilla de verificación **Eliminar copias de seguridad y separar 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**.

Administrar copias de seguridad

Puede cambiar el nombre y eliminar copias de seguridad. También puedes eliminar varias copias de seguridad simultáneamente.

Cambiar el nombre de las copias de seguridad

Puede cambiar el nombre de las copias de seguridad si desea proporcionar un nombre mejor para mejorar la capacidad de búsqueda.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso o grupo de recursos de la lista.

Se muestra la página de topología de recursos o grupos de recursos. Si el recurso o el grupo de recursos no está configurado para la protección de datos, se muestra el asistente de protección en lugar de la página de topología.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento principales.

No se puede cambiar el nombre de las copias de seguridad que están en el sistema de almacenamiento secundario.

Si ha catalogado las copias de seguridad de las bases de datos Oracle mediante Oracle Recovery Manager (RMAN), no podrá cambiar el nombre de esas copias de seguridad catalogadas.

5. Seleccione la copia de seguridad y luego haga clic en .
6. En el campo **Cambiar nombre de copia de seguridad como**, ingrese un nuevo nombre y haga clic en **Aceptar**.

Eliminar copias de seguridad

Puede eliminar copias de seguridad si ya no las necesita para otras operaciones de protección de datos.

Antes de empezar

Debe haber eliminado los clones asociados antes de eliminar un backup.



Si una copia de seguridad está asociada a un recurso clonado, no podrás eliminarla.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso o grupo de recursos de la lista.

Se muestra la página de topología de recursos o grupos de recursos.

4. Desde la vista Administrar copias, seleccione **Copias de seguridad** de los sistemas de almacenamiento principales.

No se pueden eliminar las copias de seguridad que están en el sistema de almacenamiento secundario.

5. Seleccione la copia de seguridad y luego haga clic en  .

Si elimina una copia de seguridad de la base de datos de SAP HANA, los catálogos de SAP HANA asociados a la copia de seguridad también se eliminan.



Si se elimina la última copia de seguridad restante, no se podrán eliminar las entradas del catálogo de HANA asociadas.

6. Haga clic en **Aceptar**.



Si tiene algunas copias de seguridad de bases de datos obsoletas en SnapCenter que no tienen copias de seguridad correspondientes en el sistema de almacenamiento, debe usar el comando `remove-smbbackup` para limpiar estas entradas de copia de seguridad obsoletas. Si se catalogaron las copias de seguridad obsoletas, se descatalogarán de la base de datos del catálogo de recuperación.

Quitar la protección

Eliminar protección elimina todas las copias de seguridad y separa todas las políticas. Antes de eliminar la protección, debe asegurarse de que las copias de seguridad no estén montadas y que no haya clones asociados con la copia de seguridad.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
3. Seleccione el recurso o grupo de recursos de la lista.

Se muestra la página de topología de recursos o grupos de recursos.

4. Seleccione la copia de seguridad y haga clic en **Eliminar protección**.

Eliminar clones

Puedes eliminar clones si consideras que ya no son necesarios.

Acerca de esta tarea

No puedes eliminar clones que actúen como fuente para otros clones.

Por ejemplo, si la base de datos de producción es db1, la base de datos clone1 se clona desde la copia de seguridad de db1 y, posteriormente, se protege el clone1. La base de datos clone2 se clona a partir de la copia de seguridad de clone1. Si decide eliminar clone1, primero debe eliminar clone2 y luego eliminar clone1.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de la lista.
2. En la página Recursos, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.

3. Seleccione el recurso o grupo de recursos de la lista.

Se muestra la página de topología del recurso o del grupo de recursos.

4. Desde la vista Administrar copias, seleccione **Clones** de los sistemas de almacenamiento primario o secundario (duplicados o reflejados).

5. Seleccione el clon y luego haga clic  .

Si está eliminando clones de bases de datos de SAP HANA, en la página Eliminar clon, realice las siguientes acciones:

- En el campo **Eliminar antes del clon**, ingrese los comandos que deben ejecutarse antes de eliminar el clon.
- En el campo **Desmontar**, ingrese 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 se deben esperar después de completar la eliminación del clon de la aplicación y antes de iniciar la eliminación del sistema de archivos.

Después de modificar el valor del parámetro, reinicie el servicio SnapCenter Plug-in Loader (SPL).

Supervisar trabajos, programaciones, eventos y registros

Puede supervisar el progreso de sus trabajos, obtener información sobre trabajos programados y revisar eventos y registros desde la página Monitor.

Monitorear trabajos

Puede ver información sobre trabajos de copia de seguridad, clonación, restauración y verificación de SnapCenter . Puede filtrar esta vista según la fecha de inicio y finalización, el tipo de trabajo, el grupo de recursos, la política o el complemento de SnapCenter . También puede obtener detalles adicionales y archivos de registro de trabajos específicos.

También puede supervisar trabajos relacionados con las operaciones de SnapMirror y SnapVault .



Puede supervisar únicamente los trabajos que usted creó y que son relevantes para usted, a menos que se le asigne el rol de administrador de SnapCenter u otro rol de superusuario.

Puede realizar las siguientes tareas relacionadas con la supervisión de trabajos:

- Supervisar operaciones de copia de seguridad, clonación, restauración y verificación.
- Ver detalles del trabajo e informes.
- Detener un trabajo programado.

Administrar trabajos de copia de seguridad programados

A partir de la versión 6.0.1 de SnapCenter, se introdujo un nuevo parámetro **JobConcurrencyThreshold** que establece un umbral para la cantidad de trabajos programados que se pueden ejecutar en un momento determinado. Esto le permite controlar la cantidad de copias de seguridad que desea ejecutar en función de la configuración del hardware de sus sistemas.

El valor predeterminado asignado a **JobConcurrencyThreshold** es 0 y está deshabilitado. Puede habilitarlo asignando un valor si observa una degradación del rendimiento durante la ventana de copia de seguridad programada.



Si habilita **JobConcurrencyThreshold** para administrar trabajos simultáneos, SnapCenter no le permitirá controlar el orden de las copias de seguridad y es posible que estas no se activen a la misma hora especificada en la programación.

Pasos

1. Establezca el valor del parámetro *JobConcurrencyThreshold* ubicado en *C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config*.
2. Recicle el grupo de aplicaciones de SnapCenter haciendo clic en IIS > Grupos de aplicaciones > SnapCenter > Reiniciar.
3. Reinicie el servicio web SnapCenter haciendo clic en IIS > Sitios > SnapCenter > Reiniciar.

Gestionar trabajos obsoletos

Los trabajos obsoletos se crean debido a interrupciones en SnapCenter o actualizaciones de trabajos incorrectas. A partir del lanzamiento de SnapCenter 6.0.1, se introduce un cronograma predefinido para limpiar estos trabajos obsoletos que permanecen bloqueados durante más de 72 horas. Puede cambiar la frecuencia de programación editando el parámetro configurable **CleanUpStaleJobsIntervalHours**.

Puede activar la limpieza a pedido ejecutando la programación desde **Monitor > Programaciones > SnapCenter_StaleJobCleanUp**.

Pasos

1. Establezca el valor del parámetro *CleanUpStaleJobsIntervalHours* ubicado en *C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config*.
2. Recicle el grupo de aplicaciones de SnapCenter haciendo clic en IIS > Grupos de aplicaciones > SnapCenter > Reiniciar.
3. Reinicie el servicio web SnapCenter haciendo clic en IIS > Sitios > SnapCenter > Reiniciar.

Monitorear horarios

Es posible que desee ver los cronogramas actuales para determinar cuándo comienza la operación, cuándo se ejecutó por última vez y cuándo se ejecutará la próxima vez. También puede determinar el host en el que se ejecuta la operación, junto con el grupo de recursos de la operación y la información de políticas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Horarios**.
3. Seleccione el grupo de recursos y el tipo de programación.

4. Ver la lista de operaciones programadas.

Monitorear eventos

Puede 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, como la creación de una copia de seguridad programada. Es posible que desee ver eventos para determinar si una operación, como una copia de seguridad o una restauración, está actualmente en curso.

Acerca de esta tarea

Toda la información del trabajo aparece en la página Eventos. Por ejemplo, cuando se inicia un trabajo de copia de seguridad, aparece un evento “inicio de copia de seguridad”. Cuando se completa la copia de seguridad, aparece un evento “copia de seguridad completa”.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Eventos**.
3. (Opcional) En el cuadro Filtro, ingrese la fecha de inicio o finalización, la categoría del evento (como copia de seguridad, grupo de recursos o política) y el nivel de gravedad, y haga clic en **Aplicar**. Alternativamente, ingrese caracteres en el cuadro de búsqueda.
4. Ver la lista de eventos.

Monitorear registros

Puede ver y descargar registros del servidor SnapCenter, registros del agente de host SnapCenter y registros de complementos. Es posible que desees ver los registros para ayudar con la solución de problemas.

Acerca de esta tarea

Puede filtrar los registros para mostrar solo un nivel de gravedad de registro específico:

- Depurar
- Información
- Advertir
- Error
- Fatal

También puede obtener registros a nivel de trabajo, por ejemplo, registros que le ayudan a solucionar el motivo de una falla en un trabajo de respaldo. Para los registros de nivel de trabajo, utilice la opción **Monitor > Trabajos**.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página Trabajos, seleccione un trabajo y haga clic en Descargar registros.

La carpeta comprimida descargada contiene los registros de trabajo y los registros comunes. El nombre de la carpeta comprimida contiene el ID del trabajo y el tipo de trabajo seleccionado.

3. En la página Monitor, haga clic en **Registros**.
4. Seleccione el tipo de registro, el host y la instancia.

Si selecciona el tipo de registro **plugin**, puede seleccionar un host o un complemento de SnapCenter . No puede hacerlo si el tipo de registro es **servidor**.

5. Para filtrar los registros por una fuente, mensaje o nivel de registro específico, haga clic en el ícono de filtro en la parte superior del encabezado de la columna.

Para mostrar todos los registros, elija **Mayor o igual a** como Debug nivel.

6. Haga clic en **Actualizar**.
7. Ver la lista de registros.
8. Haga clic en **Descargar** para descargar los registros.

La carpeta comprimida descargada contiene los registros de trabajo y los registros comunes. El nombre de la carpeta comprimida contiene el ID del trabajo y el tipo de trabajo seleccionado.

En configuraciones grandes para lograr un rendimiento óptimo, debe establecer la configuración de registro de SnapCenter al 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 configuración después de que finalice un trabajo de conmutación por error, ejecute el cmdlet `Get-SmRepositoryConfig`.

Eliminar trabajos y registros de SnapCenter

Puede eliminar trabajos y registros de copia de seguridad, restauración, clonación y verificación de SnapCenter. SnapCenter almacena registros de trabajos exitosos y fallidos indefinidamente a menos que los elimine. Es posible que quieras eliminarlos para reponer el almacenamiento.

Acerca de esta tarea

No debe haber ningún puesto de trabajo en funcionamiento actualmente. Puede eliminar un trabajo específico proporcionando un ID de trabajo o puede eliminar trabajos dentro de un período específico.

No es necesario colocar el host en modo de mantenimiento para eliminar trabajos.

Pasos

1. Inicie PowerShell.
2. Desde el símbolo del sistema, ingrese: `Open-SMConnection`
3. Desde el símbolo del sistema, ingrese: `Remove-SmJobs`
4. En el panel de navegación izquierdo, haga clic en **Monitor**.
5. En la página Monitor, haga clic en **Trabajos**.
6. En la página Trabajos, revise el estado del trabajo.

Información relacionada

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Descripción general de las capacidades de generación de informes de SnapCenter

SnapCenter ofrece una variedad de opciones de informes que le permiten supervisar y administrar el estado del sistema y el éxito operativo.

Tipo de informe	Descripción
Informe de respaldo	El Informe de copia de seguridad proporciona datos generales sobre las tendencias de copia de seguridad para su entorno de SnapCenter , la tasa de éxito de la copia de seguridad y cierta información sobre cada copia de seguridad realizada durante el tiempo especificado. Si se elimina una copia de seguridad, el informe no muestra ninguna información sobre el estado de la copia de seguridad eliminada. El Informe detallado de copia de seguridad proporciona información detallada sobre un trabajo de copia de seguridad específico y enumera los recursos respaldados exitosamente y aquellos que fallaron.
Informe de clonación	El informe de clonación proporciona datos generales sobre las tendencias de clonación para su entorno de SnapCenter , la tasa de éxito de clonación y cierta información sobre cada trabajo de clonación realizado durante el tiempo especificado. Si se elimina un clon, el informe no muestra ninguna información sobre el estado del clon eliminado. El Informe detallado de clonación proporciona detalles sobre el clon especificado, el host de clonación y el estado de la tarea del trabajo de clonación. Si una tarea falla, el Informe detallado de clonación muestra información sobre la falla.
Informe de restauración	El informe de restauración proporciona información general sobre los trabajos de restauración. El Informe detallado de restauración proporciona detalles sobre un trabajo de restauración específico, incluido el nombre del host, el nombre de la copia de seguridad, el inicio y la duración del trabajo y el estado de las tareas de trabajo individuales. Si una tarea falla, el Informe detallado de restauración muestra información sobre la falla.

Tipo de informe	Descripción
Informe de protección	Estos informes proporcionan detalles de protección para los recursos administrados por todas las instancias del complemento SnapCenter . Este informe proporciona detalles de protección para los recursos administrados por todas las instancias del complemento. Puede ver una descripción general, detalles de los recursos no protegidos, recursos que no se respaldaron cuando se generó el informe, recursos de un grupo de recursos para los cuales fallaron las operaciones de respaldo y el estado de SnapVault .
Informe programado	Estos informes están programados para ejecutarse periódicamente, como diariamente, semanalmente o mensualmente. Los informes se generan automáticamente en la fecha y hora especificadas y se envían a las personas respectivas por correo electrónico. Puede habilitar, deshabilitar, modificar o eliminar los horarios. La programación habilitada se puede ejecutar a pedido 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 Administrador podrá ver o modificar la programación según su permiso. Si la opción Todos los miembros de este rol pueden ver los objetos de otros miembros está seleccionada en la página Agregar rol, entonces otros miembros del rol podrán ver y modificar.

Informes de acceso

Puede utilizar el panel de control de SnapCenter para obtener una descripción general rápida del estado de su sistema. Desde el Panel de Control puedes obtener más detalles. Alternativamente, puede acceder directamente a los informes detallados.

Puede acceder a los informes mediante uno de los siguientes métodos:

- En el panel de navegación izquierdo, haga clic en **Panel de control** y, a continuación, haga clic en el gráfico circular **Resumen de la última protección** para ver más detalles en la página Informes.
- En el panel de navegación izquierdo, haga clic en **Informes**.

Filtrar su informe

Es posible que desee filtrar los datos de su informe según una variedad de parámetros, dependiendo del nivel de detalle y el período de tiempo de la información que necesita.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Informes**.
2. Si no se muestra la vista de Parámetros, haga clic en el ícono **Alternar área de parámetros** en la barra de herramientas del informe.
3. Especifique el rango de tiempo para el cual desea ejecutar su informe. + Si omite la fecha de finalización, recupera toda la información disponible.
4. Filtre la información de su informe según cualquiera de los siguientes criterios:
 - Grupo de recursos
 - Host
 - Política
 - Recurso
 - Estado
 - Nombre del complemento
5. Haga clic en **Aplicar**.

Exportar o imprimir informes

La exportación de informes de SnapCenter le permite ver el informe en una variedad de formatos alternativos. También puede imprimir informes.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Informes**.
2. Desde la barra de herramientas de informes, realice una de las siguientes acciones:
 - Haga clic en el ícono **Alternar vista previa de impresión** para obtener una vista previa de un informe imprimible.
 - Seleccione un formato de la lista desplegable del ícono **Exportar** para exportar un informe a un formato alternativo.
3. Para imprimir un informe, haga clic en el ícono **Imprimir**.
4. Para ver un resumen de un informe específico, desplácese hasta la sección correspondiente del informe.

Configurar el servidor SMTP para notificaciones por correo electrónico

Puede especificar el servidor SMTP que se utilizará para enviar informes de trabajos de protección de datos a usted mismo o a otras personas. También puede enviar un correo electrónico de prueba para verificar la configuración. La configuración se aplica globalmente para cualquier trabajo de SnapCenter para el que configure la notificación por correo electrónico.

Esta opción configura el servidor SMTP para enviar todos los informes de trabajos de protección de datos. Sin embargo, si desea recibir actualizaciones periódicas de trabajos de protección de datos de SnapCenter para un recurso en particular enviadas a usted o a otras personas para poder supervisar el estado de 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 izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Configuración global**.
3. Ingrese el servidor SMTP y haga clic en **Guardar**.
4. Para enviar un correo electrónico de prueba, ingrese la dirección de correo electrónico desde y hacia la cual enviará el correo electrónico, ingrese el asunto y haga clic en **Enviar**.

Configurar la opción de enviar informes por correo electrónico

Si desea que se le envíen actualizaciones periódicas de trabajos de protección de datos de SnapCenter a usted o a otras personas para poder supervisar el estado de dichas actualizaciones, puede configurar la opción para enviar por correo electrónico los informes de SnapCenter cuando crea un grupo de recursos.

Antes de empezar

Debes haber configurado tu servidor SMTP en la página de Configuración global en Configuración.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y luego seleccione el complemento apropiado de 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 de notificaciones del asistente para nuevo grupo de recursos, seleccione en el menú desplegable si desea recibir informes siempre, en caso de error o en caso de error o advertencia.
4. Introduzca la dirección desde donde se envía el correo electrónico, la dirección a la que se envía el correo electrónico y el asunto del correo electrónico.

Administrar el repositorio de SnapCenter Server

La información relacionada con diversas operaciones realizadas desde SnapCenter se almacena en el repositorio de base de datos del servidor SnapCenter . Debe crear copias de seguridad del repositorio para proteger el servidor SnapCenter contra la pérdida de datos.

El repositorio del servidor SnapCenter a veces se denomina base de datos NSM.

Requisitos previos para proteger el repositorio de SnapCenter

Su entorno debe cumplir ciertos requisitos previos para proteger el repositorio de SnapCenter .

- Administrar conexiones de máquinas virtuales de almacenamiento (SVM)

Debes configurar las credenciales de almacenamiento.

- Aprovisionamiento de hosts

Debe haber al menos un disco de almacenamiento NetApp en el host del repositorio de SnapCenter . Si no hay un disco NetApp presente en el host del repositorio de SnapCenter , debe crear uno.

Para obtener detalles sobre cómo agregar hosts, configurar conexiones SVM y aprovisionar hosts,

consulte las instrucciones de instalación.

- Aprovisionamiento de LUN iSCSI o VMDK

Para una configuración de alta disponibilidad (HA), puede aprovisionar un LUN iSCSI o un VMDK en uno de los servidores SnapCenter .

Realice una copia de seguridad del repositorio de SnapCenter

Realizar una copia de seguridad del repositorio de SnapCenter Server ayuda a protegerlo contra la pérdida de datos. Puede realizar una copia de seguridad del repositorio ejecutando 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 copias de seguridad para el repositorio de SnapCenter

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet *Open-SmConnection* y luego ingrese sus credenciales.
3. Realice una copia de seguridad del repositorio utilizando el cmdlet *Protect-SmRepository* y los parámetros necesarios.

Ver copias de seguridad del repositorio de SnapCenter

Puede mostrar una lista de copias de seguridad del repositorio de base de datos de SnapCenter Server ejecutando el cmdlet *Get-SmRepositoryBackups*.

Las copias de seguridad del repositorio se crean según la programación especificada en el cmdlet *Protect-SmRepository*.

Pasos

1. Inicie PowerShell.
2. Desde el símbolo del sistema, ingrese el siguiente cmdlet y proporcione las credenciales para conectarse al servidor SnapCenter : *Open-SMConnection*
3. Enumere todas las copias de seguridad de bases de datos de SnapCenter disponibles mediante el cmdlet *Get-SmRepositoryBackups*.

Restaurar el repositorio de la base de datos de SnapCenter

Puede restaurar el repositorio de SnapCenter ejecutando el cmdlet *Restore-SmRepositoryBackup*.

Al restaurar el repositorio de SnapCenter , otras operaciones de SnapCenter que se estén ejecutando se verán afectadas porque durante la operación de restauración la base de datos del repositorio no será accesible.

Pasos

1. Inicie PowerShell.
2. Desde el símbolo del sistema, ingrese el siguiente cmdlet y proporcione las credenciales para conectarse al servidor SnapCenter : *Open-SMConnection*
3. Restaure la copia de seguridad del repositorio mediante el cmdlet *Restore-SmRepositoryBackup*.

El siguiente cmdlet restaura el repositorio de base de datos MySQL de SnapCenter a partir de las copias de seguridad existentes en iSCSI LUN 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 los archivos de respaldo se eliminan accidentalmente en el LUN iSCSI. Para VMDK, restaure manualmente la copia de seguridad desde las instantáneas de ONTAP .

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```



La copia de seguridad que se utilizó para realizar la operación de restauración del repositorio no aparecerá en la lista cuando se recuperen las copias de seguridad del repositorio después de realizar la operación de restauración.

Migrar el repositorio de SnapCenter

Puede migrar el repositorio de base de datos de SnapCenter Server desde la ubicación predeterminada a otro disco. Puedes migrar el repositorio cuando quieras reubicarlo en un disco con más espacio.

Pasos

1. Detener el servicio MYSQL57 en Windows.
2. Localice el directorio de datos MySQL.

Generalmente, puede encontrar el directorio de datos en C:\ProgramData\MySQL\MySQL Server 5.7\Data.

3. Copie el directorio de datos MySQL a la nueva ubicación, por ejemplo, E:\Data\msm.
4. Haga clic derecho en el nuevo directorio y luego seleccione **Propiedades > Seguridad** para agregar la cuenta del servidor local del Servicio de red al nuevo directorio y luego asigne control total a la cuenta.
5. Cambie el nombre del directorio de la base de datos original, por ejemplo, msm_copy.
6. Desde un símbolo del sistema de Windows, cree un enlace de directorio simbólico utilizando el comando *mklink*.

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\msm" "E:\Data\msm" "
```

7. Inicie el servicio MYSQL57 en Windows.
8. Verifique que el cambio de ubicación de la base de datos sea exitoso iniciando sesión en SnapCenter y verificando las entradas del repositorio, o iniciando sesión en la utilidad MySQL y conectándose al nuevo

repositorio.

9. Eliminar el directorio del repositorio de base de datos original, renombrado (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 en ningún momento esta contraseña generada automáticamente. Si desea acceder a la base de datos del repositorio, deberá restablecer la contraseña.

Antes de empezar

Debe tener privilegios de administrador de SnapCenter para restablecer la contraseña.

Pasos

1. Inicie PowerShell.
2. Desde el símbolo del sistema, ingrese el siguiente comando y luego proporcione las credenciales para conectarse al servidor SnapCenter : *Open-SMConnection*
3. Restablecer la contraseña del repositorio: *Set-SmRepositoryPassword*

El siguiente comando restablece la contraseña del 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 sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Administrar recursos de dominios no confiables

Además de administrar hosts en dominios confiables de Active Directory (AD), SnapCenter también administra hosts en múltiples dominios no confiables de AD. Los dominios de AD que no son de confianza deben registrarse en el servidor SnapCenter . SnapCenter admite usuarios y grupos de múltiples dominios de AD que no son de confianza.

Puede instalar SnapCenter Server en una máquina que esté en un dominio o en un grupo de trabajo. Para instalar SnapCenter Server, debe especificar las credenciales del dominio si la máquina está en un dominio o las credenciales del administrador local si la máquina está en un grupo de trabajo.

No se admiten los grupos de Active Directory (AD) que pertenecen a dominios no registrados en el servidor SnapCenter . Si bien puede crear roles de SnapCenter con estos grupos de AD, el inicio de sesión en SnapCenter Server falla con el siguiente mensaje de error: El usuario con el que intenta iniciar sesión no

pertenece a ningún rol. Por favor, póngase en contacto con su administrador.

Modificar dominios no confiables

Puede modificar un dominio no confiable cuando desee actualizar las direcciones IP del controlador de dominio o el nombre de dominio completo (FQDN).

Acerca de esta tarea

Después de modificar el FQDN, es posible que los activos asociados (hosts, usuarios y grupos) no funcionen como se espera.

Para modificar un dominio que no es de confianza, puede utilizar la interfaz de usuario de SnapCenter o los cmdlets de PowerShell.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Configuración global**.
3. En la página Configuración global, haga clic en **Configuración de dominio**.

4.  , y luego proporcione los siguientes detalles:

Para este campo...	Haz esto...
FQDN del dominio	Especifique el FQDN y haga clic en Resolver .
Direcciones IP del controlador de dominio	Si el FQDN del dominio no se puede resolver, especifique una o más direcciones IP de controlador de dominio.

5. Haga clic en **Aceptar**.

Anular el registro de dominios de Active Directory que no sean de confianza

Puede anular el registro de un dominio de Active Directory que no sea de confianza si no desea utilizar los activos asociados con ese dominio.

Antes de empezar

Deberías haber eliminado los hosts, usuarios, grupos y credenciales asociados con el dominio no confiable.

Acerca de esta tarea

- Una vez que se cancela el registro del dominio en SnapCenter Server, los usuarios de ese dominio no pueden acceder a SnapCenter Server.
- Si hay activos asociados (hosts, usuarios y grupos), después de anular el registro del dominio, los activos no estarán operativos.
- Para anular el registro de un dominio que no es de confianza, puede utilizar la interfaz de usuario de SnapCenter o los cmdlets de PowerShell.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Configuración global**.
3. En la página Configuración global, haga clic en **Configuración de dominio**.
4. De la lista de dominios, seleccione el dominio cuyo registro desea cancelar.
5. Hacer clic  , y luego haga clic en **Aceptar**.

Administrar el sistema de almacenamiento

Después de agregar el sistema de almacenamiento, puede modificar la configuración y las conexiones del sistema de almacenamiento o eliminarlo.

Modificar la configuración del sistema de almacenamiento

Puede utilizar SnapCenter para modificar la configuración de su sistema de almacenamiento si desea cambiar el nombre de usuario, la contraseña, la plataforma, el puerto, el protocolo, el período de espera, la dirección IP preferida o las opciones de mensajería.

Acerca de esta tarea

Puede modificar las conexiones de almacenamiento para un usuario individual o para un grupo. Si pertenece a uno o más grupos con permiso para el 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 para el sistema de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Sistemas de almacenamiento**.
2. En la página Sistemas de almacenamiento, desde el menú desplegable **Tipo**, realice una de las siguientes acciones:

Seleccionar...	Pasos...
SVM de ONTAP	Para ver todas las máquinas virtuales de almacenamiento (SVM) que se agregaron y modificar la configuración de SVM requerida. - En la página Conexiones de almacenamiento, haga clic en el nombre de SVM apropiado. - Ejecute una de las siguientes acciones: - Si el SVM no es parte de ningún clúster, en la página Modificar sistema de almacenamiento, modifique las configuraciones como nombre de usuario, contraseña, configuración de EMS y AutoSupport , plataforma, protocolo, puerto, tiempo de espera e IP preferida. - Si el SVM es parte de un clúster, en la página Modificar sistema de almacenamiento, seleccione Administrar SVM de forma independiente y modifique las configuraciones como nombre de usuario, contraseña, configuración de EMS y AutoSupport , plataforma, protocolo, puerto, tiempo de espera e IP preferida. Después de modificar el SVM para que se administre de forma independiente, si decide administrarlo a través del clúster, debe eliminar el SVM y luego hacer clic en Redescubrir. El SVM se agregará al clúster ONTAP .  Cuando se actualiza una contraseña del sistema de almacenamiento en la GUI de SnapCenter , debe reiniciar los servicios SMCORE del complemento correspondiente o el host del servidor porque la contraseña actualizada no se refleja en SMCORE y los trabajos de respaldo fallarán con un error de credencial incorrecta.

Seleccionar...	Pasos...
Clústeres ONTAP	Para ver todos los clústeres que se agregaron y modificar la configuración del clúster requerida. - En la página Conexiones de almacenamiento, haga clic en el nombre del clúster. - En la página Modificar sistema de almacenamiento, haga clic en el ícono de edición junto a Nombre de usuario y modifique el nombre de usuario y la contraseña. - Seleccione o borre las configuraciones de EMS y AutoSupport . - Haga clic en Más opciones y modifique otras configuraciones como plataforma, protocolo, puerto, tiempo de espera e IP preferida.

3. Haga clic en **Enviar**.

Eliminar el sistema de almacenamiento

Puede utilizar SnapCenter para eliminar cualquier sistema de almacenamiento no utilizado.

Acerca de esta tarea

Puede eliminar conexiones de almacenamiento para un usuario individual o para un grupo. Si pertenece a uno o más grupos con permiso para el 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 para el sistema de almacenamiento.



Al eliminar un sistema de almacenamiento, todas las operaciones que se estén realizando en ese sistema de almacenamiento fallarán.

Pasos

- En el panel de navegación izquierdo, haga clic en **Sistemas de almacenamiento**.
- En la página Sistemas de almacenamiento, en el menú desplegable **Tipo**, seleccione * ONTAP SVMs* o * ONTAP Clusters*.
- En la página Conexiones de almacenamiento, seleccione la casilla de verificación junto a la SVM o el clúster que desea eliminar.



No puede seleccionar el SVM que forma parte de un clúster.

- Haga clic en **Eliminar**.
- En la página Eliminar configuración de conexión del sistema de almacenamiento, haga clic en **Aceptar**.



Si se elimina un SVM del clúster ONTAP mediante la GUI de ONTAP , en la GUI de SnapCenter , haga clic en **Redescubrir** para actualizar la lista de SVM.

Compatibilidad con 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 falso.

- `MinOntapVersionToUseREST`

El valor predeterminado es 9.13.1.

Habilitar la conexión a través de la API REST

1. Establezca `IsRestEnabledForStorageConnection` en verdadero.
2. Agregue la clave en `SMCoreServiceHost.dll.config` y `SnapDriveService.dll.config` tanto en el servidor como en los hosts del complemento de Windows.

```
<add key="IsRestEnabledForStorageConnection" value="true" />
```

Limitar la conexión a través de la API REST a una versión específica de ONTAP

1. Establezca el parámetro de configuración `MinOntapVersionToUseREST` en verdadero.
2. Agregue la clave en `SMCoreServiceHost.dll.config` y `SnapDriveService.dll.config` tanto en el servidor como en los hosts del complemento de Windows.

```
<add key="MinOntapVersionToUseREST" value="9.13.1" />
```

3. Reinicie el servicio para `SmCore` en el servidor y el complemento y el servicio `SnapDrive` en la máquina del complemento.

Gestionar la recopilación de datos de EMS

Puede programar y administrar la recopilación de datos del Sistema de gestión de eventos (EMS) mediante cmdlets de PowerShell. La recopilación de datos de EMS implica reunir detalles sobre el servidor SnapCenter , los paquetes de complementos de SnapCenter instalados, los hosts e información similar, y luego enviarlos a una máquina virtual de almacenamiento ONTAP (SVM) específica.



La utilización de la CPU del sistema es alta cuando la tarea de recopilación de datos está en curso. La utilización de la CPU sigue siendo alta mientras la operación avanza, independientemente del tamaño de los datos.

Detener la recopilación de datos de EMS

La recopilación de datos EMS está habilitada de forma predeterminada y se ejecuta cada siete días después

de la fecha de instalación. Puede deshabilitar la recopilación de datos en cualquier momento mediante el cmdlet de PowerShell *Disable-SmDataCollectionEMS*.

Pasos

1. Desde una línea de comandos de PowerShell, establezca una sesión con SnapCenter ingresando *Open-SmConnection*.
2. Deshabilite la recopilación de datos EMS ingresando *Disable-SmDataCollectionEms*.

Iniciar la recopilación de datos EMS

La recopilación de datos EMS está habilitada de forma predeterminada y está programada para ejecutarse cada siete días a partir de la fecha de instalación. Si lo ha deshabilitado, puede iniciar nuevamente la recopilación de datos EMS utilizando el cmdlet *Enable-SmDataCollectionEMS*.

Se ha otorgado el permiso de generación de registro de soporte automático de eventos 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 ingresando *Open-SmConnection*.
2. Habilite la recopilación de datos EMS ingresando *Enable-SmDataCollectionEMS*.

Cambiar el cronograma de recopilación de datos de EMS y el SVM objetivo

Puede utilizar cmdlets de PowerShell para cambiar la programación de recopilación de datos de EMS o la máquina virtual de almacenamiento de destino (SVM).

Pasos

1. Desde una línea de comandos de PowerShell, para establecer una sesión con SnapCenter, ingrese el cmdlet *Open-SmConnection*.
2. Para cambiar el destino de recopilación de datos de EMS, ingrese el cmdlet *Set-SmDataCollectionEmsTarget*.
3. Para cambiar el programa de recopilación de datos de EMS, ingrese el cmdlet *Set-SmDataCollectionEmsSchedule*.

Supervisar el estado de la recopilación de datos de EMS

Puede supervisar el estado de su recopilación de datos EMS mediante varios cmdlets de PowerShell. Puede obtener información sobre la programación, el destino de la máquina virtual de almacenamiento (SVM) y el estado.

Pasos

1. Desde una línea de comandos de PowerShell, establezca una sesión con SnapCenter ingresando *Open-SmConnection*.
2. Recupere información sobre el programa de recopilación de datos de EMS ingresando *Get-SmDataCollectionEmsSchedule*.
3. Recupere información sobre el estado de recopilación de datos EMS ingresando *Get-SmDataCollectionEmsStatus*.
4. Recupere información sobre el objetivo de recopilación de datos EMS ingresando *Get-SmDataCollectionEmsTarget*.

Información relacionada

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Actualizar SnapCenter Server y los complementos

Configurar SnapCenter para buscar actualizaciones disponibles

SnapCenter se comunica periódicamente con el sitio de soporte de NetApp para notificarle sobre las actualizaciones de software disponibles. También puede crear una programación para especificar el intervalo en el que desea recibir información sobre las actualizaciones disponibles.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página **Configuración**, haga clic en **Software**.

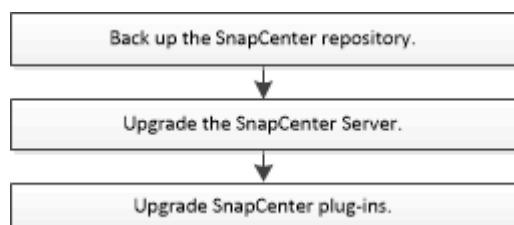
La página Software disponible muestra los paquetes de complementos disponibles, las versiones disponibles y su estado de instalación.

3. Haga clic en **Buscar actualizaciones** para ver si hay versiones más nuevas de los paquetes de complementos disponibles.
4. Haga clic en **Programar actualizaciones** para crear un programa para especificar el intervalo en el que desea recibir información sobre las actualizaciones disponibles:
 - a. Seleccione el intervalo en **Buscar actualizaciones**.
 - b. Seleccione la credencial de Windows de administrador del servidor SnapCenter y haga clic en **Aceptar**.

Actualizar el flujo de trabajo

Cada versión de SnapCenter contiene un paquete de complementos y servidor de SnapCenter actualizado. Las actualizaciones de los paquetes de complementos se distribuyen con el instalador de SnapCenter . Puede configurar SnapCenter para buscar actualizaciones disponibles.

El flujo de trabajo muestra las diferentes tareas necesarias para actualizar el servidor SnapCenter y los paquetes de complementos.



Rutas de actualización admitidas

La ruta de actualización le ayuda a comprender desde qué versiones anteriores de SnapCenter puede actualizar a las últimas versiones de SnapCenter y qué versiones de los complementos son compatibles.

Si está en la versión SnapCenter Server...	Puede actualizar directamente SnapCenter Server a...	Versiones de complementos compatibles
5,0	6,0	• 5,0 • 6,0
	6.0.1	• 6.0.1
	6,1	• 6,1
6,0	6.0.1	• 6,0 • 6.0.1
	6,1	• 6,1
6.0.1	6,1	• 6.0.1 • 6,1

Para obtener información sobre cómo actualizar el SnapCenter Plug-in for VMware vSphere, consulte ["Actualizar el SnapCenter Plug-in for VMware vSphere"](#) .

Actualizar 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 una copia de seguridad 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 los programas de copia de seguridad y verificación existentes con prescripts y posscripts habilitados en la política, las operaciones de copia de seguridad continuarán funcionando después de la actualización.

En la página **Detalles del trabajo**, un mensaje de advertencia recomienda que el cliente copie los scripts en `SCRIPTS_PATH` y edite la política para proporcionar una ruta relativa a `SCRIPTS_PATH`. Para el trabajo del ciclo de vida de clonación, el mensaje de advertencia aparece en el nivel de subtrabajo.

Pasos

1. Descargue el paquete de instalación de SnapCenter Server 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` ubicado en `C:\Archivos de programa\ 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 base de datos MySQL de SnapCenter si la copia de seguridad del repositorio no está configurada.

```
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, ingrese 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 complemento se instala mediante 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`.
- Deberías realizar un nuevo descubrimiento de recursos 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 complementos antes de agregar cualquier sistema de almacenamiento.

Actualizar el servidor SnapCenter en el host Linux

Puede utilizar el archivo de instalación de SnapCenter Server para actualizar SnapCenter Server.

Pasos

1. Realice una de las acciones para actualizar SnapCenter Server.

Si quieres realizar...	Haz esto...
Actualización no interactiva	<pre>sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename></pre> Ejemplo: <code>sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log</code> Los registros se almacenarán en <i>/var/opt/snapcenter/logs</i>. Parámetros a pasar 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 distinto de 0 para actualizar el servidor SnapCenter .
Instalación interactiva	<pre>./snapcenter-linux-server- (e18/e19/sles15).bin</pre> Se le solicitará que confirme la actualización. Introduzca cualquier valor distinto de 0 para confirmar la actualización de SnapCenter Server.



Debe cerrar la sesión y luego iniciar sesión en SnapCenter, o cerrar y luego abrir un nuevo navegador para acceder a la GUI de SnapCenter .

Actualice sus paquetes de complementos

Los paquetes de complementos se distribuyen como parte de la actualización de SnapCenter .

No es necesario colocar manualmente cada host de complemento que desea actualizar en modo de mantenimiento porque el procedimiento de actualización coloca sus hosts de complemento de Windows, Linux o AIX en modo de mantenimiento. El modo de mantenimiento evita que se ejecuten trabajos programados en el host del complemento durante la actualización.

Antes de empezar

- Si es un usuario no root con acceso a las máquinas Linux, debe actualizar el archivo */etc/sudoers* con los últimos valores de suma de comprobación antes de realizar la operación de actualización.
- De forma predeterminada, SnapCenter detecta JAVA_HOME del entorno. Si desea utilizar un JAVA_HOME fijo y está actualizando los complementos en un host Linux, debe agregar 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 complemento o cuando se reinicia el servicio del cargador de complementos de SnapCenter (SPL). Antes de actualizar o reiniciar el SPL, si agrega el parámetro SKIP_JAVAHOME_UPDATE y establece el valor en TRUE, el valor de JAVA_HOME no se actualiza.

- Deberías haber realizado una copia de seguridad de todos los archivos de configuración de SnapCenter que hayas modificado, ya sea 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.

Acerca de esta tarea

- Para el complemento SnapCenter para Microsoft SQL Server, el complemento SnapCenter para Microsoft Exchange Server y el complemento SnapCenter para Microsoft Windows, se recomienda actualizar tanto el servidor como los hosts del complemento a la última versión para que se ejecute SCRIPTS_PATH.

Para los programas de copia de seguridad y verificación existentes con prescripts y posscripts habilitados en la política, las operaciones de copia de seguridad continuarán funcionando después de la actualización.

En la página **Detalles del trabajo**, un mensaje de advertencia recomienda que el cliente copie los scripts en SCRIPTS_PATH y edite la política para proporcionar una ruta relativa a SCRIPTS_PATH. Para el trabajo del ciclo de vida de clonación, el mensaje de advertencia aparece en el nivel de subtrabajo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts > Hosts administrados**.
2. Actualice los hosts realizando una de las siguientes tareas:
 - Si la columna Estado general muestra "Actualización disponible" para uno de los hosts del complemento, 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 complemento cumple con los requisitos para actualizar el complemento.
 - iii. Haga clic en **Actualizar**.
 - Si desea actualizar varios hosts, seleccione todos los hosts y haga clic en  y luego haga clic en **Actualizar > Aceptar**.

Todos los servicios relacionados se reinician durante la actualización del complemento.



Se seleccionan todos los complementos del paquete, pero solo se actualizan los complementos que se instalaron con la versión anterior de SnapCenter y los complementos restantes no se instalan. Debe utilizar la opción **Agregar complementos** para instalar cualquier complemento nuevo.

Si no ha seleccionado la casilla **Omitir comprobaciones previas**, se validará el host del complemento para comprobar si cumple los requisitos para instalarlo. Si no se cumplen los requisitos mínimos, se mostrarán los mensajes de error o advertencia correspondientes. Después de solucionar el problema, haga clic en **Actualizar**.



Si el error está relacionado con el espacio en disco o 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.

Actualización tecnológica

Actualización tecnológica del host del servidor SnapCenter

Cuando sea necesario actualizar el host de SnapCenter Server, puede instalar la misma versión de SnapCenter Server en el nuevo host y luego ejecutar las API para realizar una copia de seguridad de 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 de SnapCenter Server.
 - b. (Opcional) Configure los certificados CA y habilite SSL bidireccional. Para obtener más información, consulte ["Configurar el certificado de CA"](#) y ["Configurar y habilitar SSL bidireccional"](#) .
 - c. (Opcional) Configure la autenticación multifactor. Para más información, consulte ["Habilitar la autenticación multifactor"](#) .
2. Inicie sesión como usuario administrador de SnapCenter .
3. Cree una copia de seguridad del servidor SnapCenter en el host antiguo utilizando la API:
`/<snapcenter_version>/server/backup` o el cmdlet: *New-SmServerBackup*.



Antes de realizar la copia de seguridad, suspenda todos los trabajos programados y asegúrese de que no haya ningún trabajo en ejecución.



Si desea restaurar la copia de seguridad en el servidor SnapCenter que se ejecuta en un nuevo dominio, antes de realizar una copia de seguridad debe agregar el nuevo usuario del dominio en el antiguo host SnapCenter y asignarle el rol de administrador de SnapCenter .

4. Copie la copia de seguridad del host antiguo al nuevo.
5. Restaure la copia de seguridad del servidor SnapCenter en el nuevo host mediante la API:
`/<snapcenter_version>/server/restore` o el cmdlet: *Restore-SmServerBackup*.

Restaurar actualizará la nueva URL del servidor SnapCenter en todos los hosts de forma predeterminada. Si desea omitir la actualización, utilice el atributo `-SkipSMSURLInHosts` y actualice por separado la URL del servidor ejecutando la API: `/<snapcenter_version>/server/configureurl` o el cmdlet: *Set-SmServerConfig*.



Si el host del complemento no puede resolver el nombre de host del servidor, inicie sesión en cada uno de los host del complemento y agregue la entrada `etc/host` para la nueva IP en el formato `<New IP> SC_Server_Name`.



Las entradas del servidor `etc/host` no se restaurarán. Puedes 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 desea continuar utilizando los usuarios del dominio antiguo, debe registrar el dominio antiguo en el nuevo servidor SnapCenter .



Si ha actualizado manualmente el archivo web.config en el antiguo host de SnapCenter , las actualizaciones no se copiarán al nuevo host. Debes realizar manualmente los mismos cambios en el archivo web.config del nuevo host.

6. Si omitió la actualización de la URL del servidor SnapCenter o alguno de los hosts estuvo inactivo durante el proceso de restauración, actualice el nuevo nombre del servidor en todos los hosts o en los hosts específicos administrados por 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 SnapCenter .

Actualización tecnológica de un nodo en el clúster F5

Puede realizar una actualización técnica de cualquier nodo en el clúster F5 eliminando el nodo y agregando el nuevo. Si el nodo que necesita actualizarse está activo, haga que otro nodo del clúster esté activo y luego elimine el nodo.

Para obtener información sobre cómo agregar un nodo al clúster F5, consulte ["Configurar servidores SnapCenter para alta disponibilidad mediante F5"](#) .



Si la URL del clúster F5 cambia, la URL se puede actualizar en todos los hosts mediante la API: /<snapcenter_version>/server/configureurl o el cmdlet: *Set-SmServerConfig*.

Desactivación del antiguo host del servidor SnapCenter

Puede eliminar el antiguo host de SnapCenter Server después de verificar que el nuevo SnapCenter Server esté en funcionamiento y que todos los hosts de complementos puedan comunicarse con el nuevo host de SnapCenter Server.

Revertir al antiguo host de SnapCenter Server

En caso de cualquier problema, puede recuperar el antiguo host de SnapCenter Server actualizando la URL de SnapCenter Server en todos los hosts mediante la API:

/<snapcenter_version>/server/configureurl o el cmdlet: *Set-SmServerConfig*.

Recuperación ante desastres

Recuperación ante desastres del host independiente de SnapCenter

Puede realizar la recuperación ante desastres restaurando la copia de seguridad 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 de SnapCenter Server.
 - b. Configurar certificados CA y habilitar SSL bidireccional. Para obtener más información, consulte ["Configurar el certificado de CA"](#) y ["Configurar y habilitar SSL bidireccional"](#) .

2. Copie la copia de seguridad del antiguo servidor SnapCenter al nuevo host.
3. Inicie sesión como usuario administrador de SnapCenter .
4. Restaure la copia de seguridad del servidor SnapCenter en el nuevo host mediante la API: `/<snapcenter_version>/server/restore` o el cmdlet: *Restore-SmServerBackup*.

Restaurar actualizará la nueva URL del servidor SnapCenter en todos los hosts de forma predeterminada. Si desea omitir la actualización, utilice 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 complemento no puede resolver el nombre de host del servidor, inicie sesión en cada uno de los host del complemento y agregue la entrada *etc/host* para la nueva IP en el formato `<New IP> SC_Server_Name`.



Las entradas del servidor *etc/host* no se restaurarán. Puedes restaurarlo manualmente desde el servidor antiguo.

5. Si omitió la actualización de la URL o alguno de los hosts estuvo inactivo durante el proceso de restauración, actualice el nuevo nombre del servidor en todos los hosts o en los hosts específicos administrados por SnapCenter mediante la API: `/<snapcenter_version>/server/configureurl` o el cmdlet: *Set-SmServerConfig*.

Recuperación ante desastres del clúster SnapCenter F5

Puede realizar una recuperación ante desastres restaurando la copia de seguridad del servidor en el nuevo host y luego 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 de SnapCenter Server.
 - b. Configurar certificados CA y habilitar SSL bidireccional. Para obtener más información, consulte ["Configurar el certificado de CA"](#) y ["Configurar y habilitar SSL bidireccional"](#) .
2. Copie la copia de seguridad del antiguo servidor SnapCenter al nuevo host.
3. Inicie sesión como usuario administrador de SnapCenter .
4. Restaure la copia de seguridad del servidor SnapCenter en el nuevo host mediante la API: `/<snapcenter_version>/server/restore` o el cmdlet: *Restore-SmServerBackup*.

Restaurar actualizará la nueva URL del servidor SnapCenter en todos los hosts de forma predeterminada. Si desea omitir la actualización, utilice 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 complemento no puede resolver el nombre de host del servidor, inicie sesión en cada uno de los host del complemento y agregue la entrada *etc/host* para la nueva IP en el formato `<New IP> SC_Server_Name`.



Las entradas del servidor *etc/host* no se restaurarán. Puedes restaurarlo manualmente desde el servidor antiguo.

5. Si omitió la actualización de la URL o alguno de los hosts estuvo inactivo durante el proceso de restauración, actualice el nuevo nombre del servidor en todos los hosts o en los hosts específicos administrados por SnapCenter mediante la API: `/<snapcenter_version>/server/configureurl` o el cmdlet: `Set-SmServerConfig`.
6. Convierta el host independiente en un clúster 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, debe acceder a la página de Swagger. ver ["Cómo acceder a las API REST mediante la página web de la API de Swagger"](#).

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar el ["Guía de referencia de cmdlets del software SnapCenter"](#).

Actualización tecnológica de los hosts de complementos de SnapCenter

Cuando sea necesario actualizar los hosts del complemento SnapCenter, deberá mover los recursos del host antiguo al nuevo. Cuando se agrega el nuevo host a SnapCenter, descubrirá todos los recursos, pero se tratará como recursos nuevos.

Acerca de esta tarea

Debe ejecutar la API o el cmdlet que tomará el nombre del host antiguo y el nombre del host nuevo como entrada, comparará los recursos por nombre y volverá a vincular los objetos de los recursos coincidentes del host antiguo al host nuevo. Los recursos coincidentes se marcarán como protegidos.

- El parámetro *IsDryRun* se establece en Verdadero de manera predeterminada e identifica los recursos coincidentes del host antiguo y el 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 antiguo al nuevo host.

- El parámetro *AutoMigrateManuallyAddedResources* se establece en Verdadero de manera predeterminada y copia automáticamente los recursos agregados manualmente del host antiguo al nuevo host.

El parámetro *AutoMigrateManuallyAddedResources* solo se aplica a los recursos de Oracle y SAP HANA.

- El parámetro *SQLInstanceMapping* debe usarse si el nombre de la instancia es diferente entre el host antiguo y el nuevo. Si es una instancia predeterminada, utilice *default_instance* como nombre de instancia.

La actualización tecnológica es compatible con los siguientes complementos de SnapCenter :

- Complemento de SnapCenter para Microsoft SQL Server

- Si las bases de datos SQL están protegidas a nivel de instancia y, como parte de la actualización tecnológica del host, solo se mueven recursos parciales al nuevo host, entonces la protección a nivel de instancia existente se convertirá en protección de grupo de recursos y las instancias de ambos hosts se agregarán al grupo de recursos.
- Si se utiliza un host SQL (por ejemplo, host1) como programador o servidor de verificación para recursos de otro host (por ejemplo, host2), mientras se realiza una actualización técnica en el host1, la programación o los detalles de verificación no se migrarán y continuarán ejecutándose en el host1. Si tiene que modificarlo, deberá hacerlo manualmente en los hosts respectivos.
- Si está utilizando la configuración de instancias de clúster de conmutación por error de SQL (FCI), puede realizar la actualización técnica agregando el nuevo nodo al clúster FCI y actualizando el host del complemento en SnapCenter.
- Si está utilizando la configuración del grupo de disponibilidad (AG) de SQL, no es necesaria la actualización tecnológica. Puede agregar el nuevo nodo a AG y actualizar el host en SnapCenter.
- Complemento de SnapCenter para Windows
- Complemento de SnapCenter para bases de datos Oracle

Si está utilizando la configuración de Oracle Real Application Cluster (RAC), puede realizar la actualización técnica agregando el nuevo nodo al clúster RAC y actualizando el host del complemento en SnapCenter.

- Complemento de SnapCenter para la base de datos SAP HANA

Los casos de uso admitidos son:

- Migrar recursos de un host a otro host.
- Migrar recursos de varios hosts a uno o menos hosts.
- Migrar recursos de un host a varios hosts.

Los escenarios soportados son:

- El nuevo host tiene un nombre diferente al del host anterior
- El host existente ha cambiado de nombre

Antes de empezar

Como este flujo de trabajo modifica los datos en el 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 se puede revertir al estado anterior mediante la copia de seguridad.

Para más información, consulte ["Realice una copia de seguridad del repositorio de SnapCenter"](#).

Pasos

1. Implemente el nuevo host e instale la aplicación.
2. Suspender los horarios del antiguo host.
3. Mueva los recursos necesarios del host antiguo al nuevo host.
 - a. Abra 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 la misma ruta de montaje que el host anterior. Si el almacenamiento no está asignado correctamente, las copias de seguridad creadas en el host antiguo no se podrán usar para la restauración.



De forma predeterminada, Windows asigna automáticamente la siguiente unidad disponible.

- Si la recuperación ante desastres de almacenamiento está habilitada, el almacenamiento respectivo debe montarse en el nuevo host.
- b. Verifique la compatibilidad si hay un cambio en la versión de la aplicación.
- c. Solo para el host del complemento Oracle, asegúrese de que los UID y GID de Oracle y sus usuarios de grupo sean los mismos que los del host anterior.

Para obtener información, consulte:

- ["Cómo migrar una base de datos SQL de un host antiguo a un host nuevo"](#)
- ["Cómo migrar una base de datos Oracle de un host antiguo a un host nuevo"](#)
- ["Cómo instalar la base de datos SAP HANA en un nuevo host"](#)

4. Agregue el nuevo host a SnapCenter.
5. Verificar si se descubrieron 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 habilitada de forma predeterminada y se identifican los recursos coincidentes que se deben volver a vincular. Puede verificar los recursos ejecutando 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 en el nuevo host no es la misma que la del host anterior, las siguientes operaciones de restauración fallarán:

- La restauración local de SQL fallará. Sin embargo, se puede aprovechar la función RTAL.
- La restauración de las bases de datos de Oracle y SAP HANA fallará.

Si desea migrar a varios hosts, debe realizar todos los pasos desde el paso 1 para todos los hosts.



Puede ejecutar la API o el cmdlet en el mismo host varias veces; se volverá a vincular solo si se identifica un nuevo recurso.

7. (Opcional) Elimine el o los hosts antiguos de SnapCenter.

Información relacionada

Para obtener información sobre las API, debe acceder a la página de Swagger. ver ["Cómo acceder a las API REST mediante la página web de la API de Swagger"](#) .

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar el ["Guía de referencia de cmdlets del software SnapCenter"](#) .

Actualización tecnológica del sistema de almacenamiento

Cuando se actualiza tecnológicamente el almacenamiento, los datos se migran al nuevo

almacenamiento y los hosts de la aplicación se montan con el nuevo almacenamiento. El flujo de trabajo de respaldo de SnapCenter identifica el nuevo almacenamiento y crea la instantánea si el nuevo almacenamiento está registrado en SnapCenter.

Puede realizar restauraciones, montajes y clonaciones en las nuevas copias de seguridad creadas después de la actualización del almacenamiento. Sin embargo, estas operaciones fallarán cuando se realicen en las copias de seguridad que se crearon antes de la actualización del almacenamiento porque las copias de seguridad tienen los detalles de almacenamiento antiguos. Debe ejecutar la API o el cmdlet de actualización de tecnología de almacenamiento para actualizar las copias de seguridad antiguas en SnapCenter con los nuevos detalles de almacenamiento.

La actualización tecnológica es compatible con los siguientes complementos de SnapCenter :

- Complemento de SnapCenter para Microsoft SQL Server
- Complemento de SnapCenter para Windows
- Complemento de SnapCenter para bases de datos Oracle
- Complemento de SnapCenter para la base de datos SAP HANA
- Complemento de SnapCenter para Microsoft Exchange Server

Los casos de uso admitidos son:

- Actualización del almacenamiento principal

La actualización de la tecnología de almacenamiento permite reemplazar el almacenamiento principal por almacenamiento nuevo. No es posible convertir el almacenamiento secundario existente en un almacenamiento primario.

- Actualización del almacenamiento secundario

Actualizar las copias de seguridad del almacenamiento principal

Cuando se actualiza tecnológicamente el almacenamiento, debe ejecutar la API o el cmdlet de actualización tecnológica de almacenamiento para actualizar las copias de seguridad antiguas en SnapCenter con los nuevos detalles de almacenamiento.

Antes de empezar

Como este flujo de trabajo modifica los datos en el 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 se puede revertir al estado anterior mediante la copia de seguridad.

Para más información, consulte ["Realice una copia de seguridad del repositorio de SnapCenter"](#) .

Pasos

1. Migrar los datos del almacenamiento antiguo al nuevo.

Para obtener información sobre cómo migrar, consulte:

- ["Cómo migrar los datos a un nuevo almacenamiento"](#)
- ["¿Cómo puedo copiar un volumen y conservar todas las copias instantáneas?"](#)

2. Ponga el host en modo de mantenimiento.

3. Monte el nuevo almacenamiento en los hosts respectivos y active las bases de datos.

El nuevo almacenamiento debe conectarse al host de la misma manera que antes. Por ejemplo, si se conectó como SAN, debe 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 en funcionamiento.
5. Agregue el nuevo almacenamiento en SnapCenter.

Asegúrese de tener un nombre SVM único en todos los clústeres en SnapCenter. Si está utilizando el mismo nombre de SVM en el nuevo almacenamiento y si todos los volúmenes de SVM se pueden migrar antes de ejecutar la actualización del almacenamiento, se recomienda eliminar la SVM en el clúster antiguo y redescubrir el clúster antiguo en SnapCenter, lo que eliminará la SVM de la memoria caché.

6. Ponga el host en modo de producción.
7. En SnapCenter, cree una copia de seguridad de los recursos cuyo almacenamiento se migra. SnapCenter necesita una nueva copia de seguridad para identificar la última huella de almacenamiento, y se utilizará para actualizar los metadatos de las copias de seguridad antiguas existentes.



Cada vez que se conecta 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 un recurso nuevo. Durante la actualización de la tecnología de almacenamiento, cuando el LUN del nuevo almacenamiento se conecta al host con la misma letra de unidad o ruta, la detección del sistema de archivos de Windows en SnapCenter marcará el recurso existente como eliminado incluso si está montado con la misma letra de unidad o ruta y mostrará el nuevo LUN como nuevo recurso. Como el recurso está marcado como eliminado, no se considerará para la actualización de tecnología de almacenamiento en SnapCenter y se perderán todas las copias de seguridad del recurso antiguo. Siempre que se produce una actualización de almacenamiento, para los recursos del sistema de archivos de Windows, no se debe realizar el descubrimiento de recursos antes de ejecutar la API o el cmdlet de actualización de almacenamiento.

8. Ejecute la API de actualización de almacenamiento:

`/<snapcenter_version>/techrefresh/primarystorage` o el cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.



Si el recurso está configurado con una política de replicación habilitada, la última copia de seguridad después de la actualización del almacenamiento debe tener detalles del almacenamiento secundario.

- a. Si utiliza la configuración de instancias de clúster de conmutación por error de SQL (FCI), las copias de seguridad se mantienen a nivel de clúster. Debe proporcionar el nombre del clúster como entrada para la actualización de la tecnología de almacenamiento.
- b. Si utiliza la configuración del grupo de disponibilidad (AG) de SQL, las copias de seguridad se mantienen en el nivel de nodo. Debe proporcionar el nombre del nodo como entrada para la actualización de la tecnología de almacenamiento.
- c. Si está utilizando la configuración de Oracle Real Application Clusters (RAC), puede realizar una actualización de la tecnología de almacenamiento en cualquier nodo.

El atributo *IsDryRun* está establecido en Verdadero de forma predeterminada. Identificará los recursos para los cuales se actualiza el almacenamiento. Puede ver el recurso y los detalles de

almacenamiento modificados ejecutando la API: '<snapcenter_version>/jobs/{jobid}' o el cmdlet *Get-SmJobSummaryReport*.

- Después de verificar los detalles de almacenamiento, configure el atributo *IsDryRun* en Falso y ejecute la API de actualización de almacenamiento:

/<snapcenter_version>/techrefresh/primarystorage o el cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

Esto actualizará los detalles de almacenamiento en las copias de seguridad más antiguas.

Puede ejecutar la API o el cmdlet en el mismo host varias veces; actualizará los detalles de almacenamiento en las copias de seguridad más antiguas solo si se actualiza el almacenamiento.



La jerarquía de clones no se puede migrar en ONTAP. Si el almacenamiento que se está migrando tiene metadatos clonados en SnapCenter, entonces el recurso clonado se marcará como recurso independiente. Los clones de metadatos de clones se eliminarán de forma recursiva.

- (Opcional) Si no se mueven todas las instantáneas del antiguo almacenamiento principal al nuevo, ejecute la siguiente API: /<snapcenter_version>/hosts/primarybackupsexistencecheck o el cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

Esto realizará la verificación de existencia de la instantánea en el nuevo almacenamiento principal y marcará las copias de seguridad respectivas como no disponibles para ninguna operación en SnapCenter.

Actualizar las copias de seguridad del almacenamiento secundario

Cuando se actualiza tecnológicamente el almacenamiento, debe ejecutar la API o el cmdlet de actualización tecnológica de almacenamiento para actualizar las copias de seguridad antiguas en SnapCenter con los nuevos detalles de almacenamiento.

Antes de empezar

Como este flujo de trabajo modifica los datos en el 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 se puede revertir al estado anterior mediante la copia de seguridad.

Para más información, consulte ["Realice una copia de seguridad del repositorio de SnapCenter"](#).

Pasos

- Migrar los datos del almacenamiento antiguo al nuevo.

Para obtener información sobre cómo migrar, consulte:

- ["Cómo migrar los datos a un nuevo almacenamiento"](#)
- ["¿Cómo puedo copiar un volumen y conservar todas las copias instantáneas?"](#)

- Establezca la relación SnapMirror entre el almacenamiento principal y el nuevo almacenamiento secundario, y asegúrese de que el estado de la relación sea saludable.
- En SnapCenter, cree una copia de seguridad de los recursos cuyo almacenamiento se migra.

SnapCenter necesita una nueva copia de seguridad para identificar la última huella de almacenamiento y se utilizará para actualizar los metadatos de las copias de seguridad antiguas existentes.



Debes esperar hasta que se complete esta operación. Si continúa con el siguiente paso antes de completarlo, SnapCenter perderá por completo los metadatos de las instantáneas secundarias antiguas.

4. Después de crear con éxito una copia de seguridad de todos los recursos en un host, ejecute la API de actualización de almacenamiento secundario:

`/<snapcenter_version>/techrefresh/secondarystorage` o el cmdlet: *Invoke-SmTechRefreshSecondaryStorage*.

Esto actualizará los detalles de almacenamiento secundario de las copias de seguridad más antiguas en el host determinado.

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 con éxito las copias de seguridad más antiguas, puede romper la antigua relación de almacenamiento secundario con el principal.

Desinstalar SnapCenter Server y sus complementos

Desinstalar los paquetes de complementos de SnapCenter

Requisitos previos para eliminar un host

Puede eliminar hosts y desinstalar complementos individuales o paquetes de complementos mediante la GUI de SnapCenter . También puede desinstalar complementos individuales o paquetes de complementos en hosts remotos mediante la interfaz de línea de comandos (CLI) en su host de SnapCenter Server o mediante la opción **Desinstalar un programa** de Windows localmente en cualquier host.

Antes de eliminar un host de SnapCenter Server, debe completar los requisitos previos.

- Debes iniciar sesión como administrador.
- Debe asegurarse de que no se estén ejecutando trabajos de descubrimiento en el host.
- Se le debe asignar 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 agregar el host a SnapCenter.
- Debe confirmar la huella digital si el host de SnapCenter se actualiza a una versión posterior de SnapCenter pero el host del complemento aún ejecuta una versión anterior del complemento.

Requisitos previos para eliminar un host mediante el control de acceso basado en roles

- Debería haber iniciado sesión utilizando un rol RBAC que tenga permisos de lectura, eliminación de host, instalación, desinstalación de complementos y eliminación de objetos.

Los objetos pueden ser clones, copias de seguridad, grupos de recursos, sistemas de almacenamiento, etc.

- Debería haber agregado el usuario RBAC al rol RBAC.
- Debe asignar el usuario RBAC al host, al complemento, a las credenciales, a los grupos de recursos y al sistema de almacenamiento (para clones) que desea eliminar.
- Debería haber iniciado sesión en SnapCenter como usuario RBAC.

Requisitos previos para eliminar un host con clones creados a partir de la operación del ciclo de vida de clonación

- Deberías haber creado trabajos de clonación utilizando la gestión del ciclo de vida de clonación para bases de datos SQL.
- Debería haber creado una función RBAC con permisos de 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 complementos y lectura y eliminación de host.
- Debería haber asignado el usuario RBAC al rol RBAC.
- Debería haber asignado el usuario RBAC al host, al complemento de SnapCenter para Microsoft SQL

Server, a las credenciales, al grupo de recursos del ciclo de vida de clones y al sistema de almacenamiento.

- Debería haber iniciado sesión en SnapCenter como usuario RBAC.

Para obtener información sobre cómo desinstalar el SnapCenter Plug-in for VMware vSphere, consulte ["Eliminar el SnapCenter Plug-in for VMware vSphere"](#).

Eliminar un host

Cuando SnapCenter Server elimina un host, primero elimina las copias de seguridad, los clones, los trabajos de clonación, los grupos de recursos y los recursos enumerados para ese host en la página Recursos de SnapCenter y, luego, desinstala los paquetes de complementos en el host.

Acerca de esta tarea

- Si elimina un host, las copias de seguridad, los clones y los grupos de recursos asociados con el host también se eliminan.
- Al eliminar los grupos de recursos, también se eliminan todas las programaciones asociadas.
- Si el host tiene un grupo de recursos compartido con otro host y usted elimina el host, el grupo de recursos también se elimina.
- Debe utilizar el cmdlet *Remove-SmHost* para eliminar los hosts de complementos fuera de servicio o inaccesibles.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#)

- El tiempo necesario para eliminar un host depende de la cantidad de copias de seguridad y de la configuración de retención. Esto se debe a que las instantáneas se eliminan de cada uno de los controladores y se limpian los metadatos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página **Hosts**, haga clic en **Hosts administrados**.
3. Seleccione el host que desea eliminar y luego haga clic en **Eliminar**.
4. Para los clústeres Oracle RAC, para eliminar el SnapCenter software de todos los hosts del clúster, seleccione **Incluir todos los hosts del clúster**.

También puedes eliminar un nodo de un clúster y de esa manera eliminar todos los nodos uno por uno.

5. Haga clic en **Aceptar**.



Cuando desinstala y reinstala complementos de host en un clúster, los recursos del clúster no se detectan automáticamente. Seleccione el nombre de host del clúster y luego haga clic en **Actualizar recursos** para descubrir automáticamente los recursos del clúster.

Desinstalar complementos mediante la GUI de SnapCenter

Cuando decida que ya no necesita un complemento individual o un paquete de complementos, puede desinstalarlo mediante la interfaz de SnapCenter .

Antes de empezar

- Deberías haber eliminado los grupos de recursos del paquete de complemento que estás desinstalando.
- Deberías haber separado las políticas asociadas con los grupos de recursos para el paquete de complemento que estás desinstalando.

Acerca de esta tarea

Puede desinstalar un complemento individual. Por ejemplo, podría necesitar desinstalar el complemento de SnapCenter para Microsoft SQL Server porque un host se está quedando sin recursos y desea migrarlo a un host más potente. También puede desinstalar un paquete de complemento completo. Por ejemplo, es posible que necesite desinstalar el paquete de complementos de SnapCenter para Linux, que incluye el complemento de SnapCenter para Oracle Database y el complemento de SnapCenter para UNIX.

- Eliminar un host incluye desinstalar todos los complementos.

Cuando se elimina un host de SnapCenter, SnapCenter desinstala todos los paquetes de complementos en el host antes de eliminarlo.

- La GUI de SnapCenter elimina complementos de un host a la vez.

Cuando utiliza la GUI de SnapCenter , puede desinstalar complementos solo en un host a la vez. Sin embargo, es posible que tenga varias operaciones de desinstalación ejecutándose al mismo tiempo.

También puede desinstalar un complemento de varios hosts utilizando el cmdlet *Uninstall-SmHostPackage* y los parámetros necesarios. La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets del software SnapCenter"](#) .



Desinstalar el paquete de complementos de SnapCenter para Windows de un host en el que está instalado SnapCenter Server dañará la instalación de SnapCenter Server. No desinstale el paquete de complementos de SnapCenter para Windows a menos que esté seguro de que ya no necesita el servidor SnapCenter .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. En la página Hosts administrados, seleccione el host del que desea desinstalar el complemento o el paquete de complementos.
4. Junto al complemento que desea eliminar, haga clic en **Eliminar** > **Enviar**.

Después de terminar

Debe esperar 5 minutos antes de reinstalar el complemento en ese host. Este período de tiempo es suficiente para que la GUI de SnapCenter actualice el estado del host administrado. La instalación fallará si reinstala inmediatamente el complemento.

Si está desinstalando el paquete de complementos de SnapCenter para Linux, los archivos de registro específicos de la desinstalación están disponibles en: */custom_location/snapcenter/log*.

Desinstalar complementos de Windows mediante el cmdlet de PowerShell

Puede desinstalar complementos individuales o desinstalar paquetes de complementos de uno o más hosts mediante el cmdlet *Uninstall-SmHostPackage* en la interfaz de línea de comandos del host de SnapCenter Server.

Debería haber iniciado sesión en SnapCenter como un usuario de dominio con derechos de administrador local en cada host en el que desee desinstalar los complementos.

Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , ingrese el comando *Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME* y luego ingrese sus credenciales.
3. Desinstale los complementos de Windows mediante el cmdlet *Uninstall-SmHostPackage* y los parámetros necesarios.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar el "[Guía de referencia de cmdlets del software SnapCenter](#)".

Desinstalar complementos localmente en un host

Puede desinstalar los complementos de SnapCenter localmente en un host si no puede acceder al host desde el servidor de SnapCenter .

Acerca de esta tarea

La mejor práctica para desinstalar complementos individuales o paquetes de complementos es utilizar la GUI de SnapCenter o utilizar el cmdlet *Uninstall-SmHostPackage* en la interfaz de línea de comandos del host del servidor SnapCenter . Estos procedimientos ayudan a que el servidor SnapCenter se mantenga actualizado con cualquier cambio.

Sin embargo, es posible que en ocasiones necesites desinstalar complementos localmente. Por ejemplo, es posible que haya ejecutado un trabajo de desinstalación desde SnapCenter Server pero el trabajo falló, o que haya desinstalado SnapCenter Server y queden complementos huérfanos en un host.



Desinstalar un paquete de complemento localmente en un host no elimina los datos asociados con el host; por ejemplo, trabajos programados y metadatos de respaldo.



No intente desinstalar el paquete de complementos de SnapCenter para Windows localmente desde el Panel de control. Debe utilizar la GUI de SnapCenter para asegurarse de que el complemento de SnapCenter para Microsoft Windows se desinstale correctamente.

Pasos

1. En el sistema host, navegue hasta el Panel de control y haga clic en **Desinstalar un programa**.
2. En la lista de programas, seleccione el complemento o paquete de complementos de SnapCenter que desea desinstalar y haga clic en **Desinstalar**.

Windows desinstala todos los complementos del paquete seleccionado.

Desinstalar el paquete de complementos para Linux o AIX mediante CLI

Puede desinstalar el paquete de complementos de SnapCenter para Linux o el paquete de complementos de SnapCenter para AIX mediante la interfaz de línea de comandos.

Antes de empezar

- Asegúrese de haber eliminado los trabajos programados
- Asegúrese de que todos los trabajos en ejecución se hayan completado.

Paso

Ejecute `/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall` para desinstalar.

Desinstalar el servidor SnapCenter en el host de Windows

Si ya no desea utilizar SnapCenter Server para administrar trabajos de protección de datos, puede desinstalar SnapCenter Server mediante el Panel de control de programas y características en el host de SnapCenter Server. Al desinstalar SnapCenter Server se eliminan todos sus componentes.

Antes de empezar

- Asegúrese de tener al menos 2 GB de espacio libre en la unidad donde está instalado SnapCenter Server.
- Asegúrese de que el dominio en el que está instalado SnapCenter Server no se elimine.

Si elimina el dominio donde se instaló SnapCenter Server y luego intenta desinstalarlo, la operación falla.

- Deberías haber realizado una copia de seguridad de la base de datos del repositorio porque esta se limpiará y desinstalará.

Pasos

1. En el host del servidor SnapCenter , navegue hasta el Panel de control.
2. Asegúrate de estar en la vista **Categoría**.
3. En Programas, haga clic en **Desinstalar un programa**.

Se abre la ventana Programas y características.

4. Seleccione NetApp SnapCenter Server y haga clic en **Desinstalar**.

A partir de SnapCenter 4.2, cuando desinstala SnapCenter Server, se desinstalan todos sus componentes, incluida la base de datos del repositorio de MySQL Server.

- Para eliminar el nodo NLB de un clúster NLB es necesario reiniciar el host del servidor SnapCenter . Si no reinicia el host, es posible que experimente una falla si intenta reinstalar SnapCenter Server.
- Debe desinstalar manualmente .NET Framework que no se elimina durante la desinstalación.

Desinstalar el servidor SnapCenter en el host Linux

Si ya no desea utilizar SnapCenter Server para administrar trabajos de protección de datos, puede desinstalar SnapCenter Server. Al desinstalar SnapCenter Server se

eliminan todos sus componentes.

Pasos

- 1. Realice una de las acciones para desinstalar SnapCenter Server.

Si quieres realizar...	Haz esto...
Desinstalación no interactiva	<pre>\$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1</pre> Ejemplo: sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall
Desinstalación interactiva	<pre>\$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</pre> Introduzca cualquier valor distinto de 0 en la entrada de confirmación para confirmar la desinstalación.

Automatizar mediante API REST

Automatización de SnapCenter mediante API REST

Puede utilizar las API REST para realizar varias operaciones de administración de SnapCenter . Las API REST se exponen a través de la página web Swagger. Puede acceder a la página web de Swagger disponible en *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* para mostrar la documentación de la API REST, así como para emitir manualmente una llamada API.

Los complementos que admiten las API REST son:

- Complemento para Microsoft SQL Server
- Complemento para la base de datos SAP HANA
- Complemento para base de datos Oracle

Para obtener información sobre el SnapCenter Plug-in for VMware vSphere , consulte ["SnapCenter Plug-in for VMware vSphere"](#)

Cómo acceder a la API REST de SnapCenter de forma nativa

Puede acceder a la API REST de SnapCenter directamente utilizando cualquier lenguaje de programación que admita un cliente REST. Las opciones de lenguaje más populares incluyen Python, PowerShell y Java.

Fundación de servicios web REST

La Transferencia de Estado Representacional (REST) es un estilo para crear aplicaciones web distribuidas. Al aplicarla al diseño de una API de servicios web, establece un conjunto de tecnologías y mejores prácticas para exponer recursos basados en servidor y gestionar sus estados. Utiliza protocolos y estándares convencionales para proporcionar una base flexible para la gestión de SnapCenter.

Recursos y representación estatal

Los recursos son los componentes básicos de un sistema web. Al crear una aplicación de servicios web REST, las primeras tareas de diseño incluyen:

Identificación de recursos del sistema o del servidor

Cada sistema utiliza y mantiene recursos. Un recurso puede ser un archivo, una transacción comercial, un proceso o una entidad administrativa. Una de las primeras tareas al diseñar una aplicación basada en servicios web REST es identificar los recursos.

Definición de estados de recursos y operaciones estatales asociadas

Los recursos siempre están en uno de un número finito de estados. Los estados, así como las operaciones asociadas utilizadas para efectuar los cambios de estado, deben estar claramente definidos.

Puntos finales URI

Cada recurso REST debe definirse y estar disponible mediante un esquema de direccionamiento bien definido. Los puntos finales donde se ubican 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 en la red. El Localizador Uniforme de Recursos (URL) es un tipo de URI que se utiliza con servicios web para identificar y acceder a los recursos. Los recursos suelen exponerse en una estructura jerárquica similar a la de un directorio de archivos.

Mensajes HTTP

El Protocolo de Transferencia de Hipertexto (HTTP) es el protocolo que utilizan el cliente y el 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 las acciones de gestión de estado correspondientes. 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 que acompañan a los flujos de datos de solicitud y respuesta.

Formato JSON

Si bien la información se puede estructurar y transferir entre un cliente y un servidor de servicios web de varias maneras, la opción más popular es la Notación de Objetos JavaScript (JSON).

JSON es un estándar de la industria para representar estructuras de datos simples en texto plano y se utiliza para transferir información de estado que describe los recursos. La API REST de SnapCenter utiliza JSON para dar formato a los datos incluidos en el cuerpo de cada solicitud y respuesta HTTP.

Características operativas básicas

Si bien REST establece un conjunto común de tecnologías y mejores prácticas, los detalles de cada API pueden variar según las opciones de diseño.

Transacción de API de solicitud y respuesta

Cada llamada a la API REST se realiza como una solicitud HTTP al sistema SnapCenter Server que genera una respuesta asociada para el cliente. Este par de solicitud y respuesta se considera una transacción API.

Antes de utilizar la API, debe familiarizarse con las variables de entrada disponibles para controlar una solicitud y el contenido de la salida de respuesta.

Soporte para operaciones CRUD

A cada uno de los recursos disponibles a través de la API REST de SnapCenter se accede según el modelo CRUD:

- Crear
- Leer
- Actualizar
- Borrar

Para algunos de los recursos, solo se admite un subconjunto de las operaciones.

Identificadores de objetos

A cada instancia u objeto de recurso se le asigna un identificador único al crearse. 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 al llamador una URL con el ID asociado en el encabezado de ubicación de la respuesta HTTP. Puede extraer el identificador y usarlo en llamadas posteriores al hacer referencia a la instancia del recurso.



El contenido y la estructura interna de los identificadores de objeto pueden cambiar en cualquier momento. Solo debe usar los identificadores en las llamadas a la API correspondientes según sea necesario al referirse a los objetos asociados.

Instancias y colecciones de objetos

Dependiendo de la ruta del recurso y del método HTTP, una llamada API puede aplicarse a una instancia de objeto específica o a una colección de objetos.

Operaciones sincrónicas y asincrónicas

SnapCenter ejecuta una solicitud HTTP recibida de un cliente de forma sincrónica o asincrónica.

Procesamiento sincrónico

SnapCenter ejecuta la solicitud inmediatamente y responde con un código de estado HTTP de 200 o 201 si es exitosa.

Cada solicitud que utiliza el método GET siempre se realiza de forma sincrónica. Además, las solicitudes que utilizan POST están diseñadas para ejecutarse sincrónicamente si se espera que se completen en menos de dos segundos.

Procesamiento asincrónico

Si una solicitud asincrónica 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 llamador junto con el objeto de trabajo. Debes recuperar el estado del trabajo para determinar el éxito o el fracaso.

Las solicitudes que utilizan los métodos POST y DELETE están diseñadas para ejecutarse de forma asincrónica si se espera que demoren más de dos segundos en completarse.

Seguridad

La seguridad proporcionada con la API 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 a través de la red entre el servidor SnapCenter y el cliente normalmente se cifra mediante TLS, según la configuración de SnapCenter .

Autenticación HTTP

A nivel HTTP, se utiliza autenticación básica para las transacciones 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 de API

Puede controlar cómo se procesa una llamada API a través de parámetros y variables establecidos en la solicitud HTTP.

Métodos HTTP

Los métodos HTTP compatibles con la API REST de SnapCenter se muestran en la siguiente tabla.



No todos los métodos HTTP están disponibles en cada uno de los puntos finales REST.

Método HTTP	Descripción
CONSEGUIR	Recupera propiedades de objeto en una instancia o colección de recursos.
CORREO	Crea una nueva instancia de recurso basada en la entrada proporcionada.
BORRAR	Elimina una instancia de recurso existente.
PONER	Modifica una instancia de recurso existente.

Encabezados de solicitud

Debes incluir varios encabezados en la solicitud HTTP.

Tipo de contenido

Si el cuerpo de la solicitud incluye JSON, este encabezado debe establecerse como *application/json*.

Aceptar

Este encabezado debe establecerse en *application/json*.

Autorización

La autenticación básica debe configurarse con el nombre de usuario y la contraseña codificados como una cadena base64.

Cuerpo de la solicitud

El contenido del cuerpo de la solicitud varía según la llamada específica. El cuerpo de la solicitud HTTP

consta de uno de los siguientes elementos:

- Objeto JSON con variables de entrada
- Vacío

Filtrado de objetos

Al ejecutar una llamada a la API que usa GET, puede limitar o filtrar los objetos devueltos según 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 en un rango de valores. La API REST de SnapCenter admite los operadores de filtrado que se muestran en la siguiente tabla.

Operador	Descripción
=	Igual a
<	Menos que
>	Más que
≤	Menor o igual a
≥	Mayor o igual que
ACTUALIZAR	O
!	No es igual a
*	Comodín codicioso

También puede devolver una colección de objetos en función de si un campo específico está configurado o no utilizando la palabra clave **null** o su negación **!null** como parte de la consulta.



Cualquier campo que no esté configurado generalmente se excluye de las consultas coincidentes.

Solicitar campos de objeto específicos

De forma predeterminada, al ejecutar una llamada a la API mediante GET, solo se devuelven los atributos que identifican de forma única 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 utilizando el `fields` parámetro de consulta de las siguientes maneras:

Campos comunes o estándar

Especifique **campos=*** 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 a ellos. Estas son las mismas propiedades devueltas para un objeto después de usar GET con una clave de ruta URL (UUID).

Todos los campos

Especifique **fields=*** para recuperar todos los campos del objeto, incluidos aquellos que requieren procesamiento adicional del servidor para acceder.

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 y sin espacios.



Como práctica recomendada, siempre debe identificar los campos específicos que desea. Solo 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 mediante *fields=** basándose en un análisis de rendimiento interno. La clasificación de un campo podría cambiar en futuras versiones.

Ordenar objetos en el conjunto de salida

Los registros de una colección de recursos se devuelven en el orden predeterminado definido por el objeto. Puedes cambiar el orden usando el `order_by` parámetro de consulta con el nombre del campo y dirección de clasificación 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.
- Al incluir varios parámetros, debe separar los campos con una coma.

Paginación al recuperar objetos de una colección

Al emitir una llamada API utilizando GET para acceder a una colección de objetos del mismo tipo, SnapCenter intenta devolver tantos objetos como sea posible en función de 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 finaliza la solicitud y, por lo tanto, limita la cantidad de registros devueltos.



Si una solicitud finaliza antes de iterar sobre todos los objetos, la respuesta contiene el enlace 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
```

La cantidad de objetos realmente devueltos puede ser menor que el máximo vigente, en función de la restricción de tiempo relacionada, así como de la cantidad total de objetos en el sistema.

Limitar el tiempo empleado 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 de 15 segundos. Puede cambiar este límite utilizando el parámetro de consulta *return_timeout*. Por ejemplo:

```
return_timeout=5
```

La cantidad de objetos realmente devueltos puede ser menor que el máximo vigente, en función de la restricción relacionada con la cantidad de objetos, así como de la cantidad total de objetos en el sistema.

Limitar el conjunto de resultados

Si es necesario, puede combinar estos dos parámetros con parámetros de consulta adicionales para limitar el conjunto de resultados. Por ejemplo, lo siguiente devuelve hasta 10 eventos EMS generados después del tiempo especificado:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Puede emitir varias solicitudes para navegar por los objetos. Cada llamada a la API posterior debe usar 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 número entero en bytes, puede utilizar opcionalmente un sufijo como se muestra en la siguiente tabla.

Sufijo	Descripción
KB	KB Kilobytes (1024 bytes) o kibibytes
MEGABYTE	MB Megabytes (KB x 1024 bytes) o mebibytes
GB	GB Gigabytes (MB x 1024 bytes) o gibibytes
tuberculosis	TB Terabytes (GB x 1024 bytes) o tebibytes
PB	PB Petabytes (TB x 1024 bytes) o pebibytes

Interpretación de una respuesta de API

Cada solicitud de API genera una respuesta para el cliente. Debe examinar la respuesta para determinar si fue exitosa y recuperar datos adicionales según sea necesario.

Código de estado HTTP

A continuación se describen los códigos de estado HTTP utilizados por la API REST de SnapCenter .

Código	Descripción
200	OK Indica éxito para llamadas que no crean un nuevo objeto.

Código	Descripción
201	Creado Se ha creado un objeto correctamente. El encabezado de ubicación en la respuesta incluye el identificador único del objeto.
202	Aceptado Se ha iniciado un trabajo en segundo plano para ejecutar la solicitud, pero aún no se ha completado.
400	Solicitud incorrecta La entrada de la solicitud no se reconoce o es inadecuada.
401	La autenticación de usuario no autorizado ha fallado.
403	Acceso prohibido denegado debido a un error de autorización (RBAC).
404	No encontrado El recurso al que se refiere la solicitud no existe.
405	Método no permitido El método HTTP en la solicitud no es compatible con el recurso.
409	Conflicto Un intento de crear un objeto falló porque primero se debe crear un objeto diferente o el objeto solicitado ya existe.
500	Error interno Se produjo 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 URL completa del nuevo objeto, incluido el identificador único asignado al objeto.

Tipo de contenido

Normalmente esto será `application/json`.

Cuerpo de la respuesta

El contenido del cuerpo de respuesta resultante de una solicitud de API difiere según el objeto, el tipo de procesamiento y el éxito o fracaso de la solicitud. La respuesta siempre se representa en JSON.

Objeto único

Se puede devolver un solo objeto con un conjunto de campos según la solicitud. Por ejemplo, se puede usar GET para recuperar propiedades seleccionadas de un clúster mediante el identificador único.

Múltiples objetos

Se pueden devolver varios objetos de una colección de recursos. En todos los casos, se utiliza un formato consistente, con `num_records` Indica el número de registros y los registros que contienen una matriz de 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 asincrónica, se devuelve un objeto Job que ancla la tarea en segundo plano. Por ejemplo, la solicitud PATCH utilizada para actualizar la configuración del clúster se procesa de forma asincrónica y devuelve un objeto Job.

Objeto de error

Si ocurre 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 la respuesta incluye un objeto JSON vacío.

Errores

Si ocurre un error, se devuelve un objeto de error en el cuerpo de la 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 categoría de error general, y el mensaje para determinar el error específico. Cuando está disponible, el campo de destino incluye la entrada de usuario específica asociada con el 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.

Código	Descripción
409	Ya existe un objeto con el mismo identificador.
400	El valor de un campo tiene un valor no válido o falta, o se proporcionó un campo adicional.
400	La operación no está soportada.

Código	Descripción
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 REST compatibles con SnapCenter Server y complementos

Los recursos disponibles a través de la API REST de SnapCenter están organizados en categorías, como se muestra en la página de documentación de la API de SnapCenter . A continuación se presenta una breve descripción de cada uno de los recursos con las rutas de recursos base, junto con consideraciones de uso adicionales cuando corresponda.

Autorización

Puede utilizar 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 utilizar API para realizar diferentes operaciones.

- recuperar todos los dominios en SnapCenter
- recuperar detalles de un dominio específico
- registrar o anular el registro de un dominio
- modificar un dominio

Empleos

Puede utilizar API para realizar diferentes operaciones.

- recuperar todos los trabajos en SnapCenter
- recuperar el estado de un trabajo
- cancelar o detener un trabajo

Configuración

Puede utilizar API para realizar diferentes operaciones.

- registrar, modificar o eliminar 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 autenticación multifactor (MFA) del inicio de sesión del servidor SnapCenter
- Habilitar o deshabilitar y configurar MFA para el inicio de sesión del servidor SnapCenter
- Crea el archivo de configuración necesario para configurar MFA

Anfitriones

Puede utilizar API para realizar diferentes operaciones.

- Consultar todos los hosts de SnapCenter
- eliminar uno o más hosts de SnapCenter
- recuperar un host por nombre
- recuperar todos los recursos en un host
- recuperar un recurso utilizando el ID del recurso
- recuperar los detalles de configuración del complemento
- configurar el host del complemento
- recuperar todos los recursos del complemento para el host de Microsoft SQL Server
- recuperar todos los recursos del complemento para el host de la base de datos Oracle
- recuperar todos los recursos del complemento para el host de la aplicación personalizada
- recuperar todos los recursos del complemento para el host SAP HANA
- recuperar los complementos instalados
- Instalar complementos en un host existente
- actualizar el paquete de host
- eliminar complementos de un host existente
- Agregar complemento en un host
- agregar o modificar host
- obtener la firma del host Linux
- Registrar la firma del host Linux
- Poner el host en modo de mantenimiento o producción
- Iniciar o reiniciar los servicios del complemento en el host
- cambiar el nombre de un host

Recursos

Puede utilizar API para realizar diferentes operaciones.

- recuperar todos los recursos
- recuperar un recurso utilizando el ID del recurso
- recuperar todos los recursos del complemento para el host de Microsoft SQL Server
- recuperar todos los recursos del complemento para el host de la base de datos Oracle

- recuperar todos los recursos del complemento para el host de la aplicación personalizada
- recuperar todos los recursos del complemento para el host SAP HANA
- recuperar un recurso de Microsoft SQL Server usando una clave
- recuperar un recurso personalizado usando una clave
- modificar un recurso del complemento para el host de la aplicación personalizada
- Eliminar un recurso del complemento para el host de la aplicación personalizada mediante una clave
- recuperar un recurso de SAP HANA usando una clave
- modificar un recurso del complemento para el host de SAP HANA
- Eliminar un recurso del complemento para el host SAP HANA mediante una clave
- recuperar un recurso de Oracle usando una clave
- crear un recurso de volumen de aplicación de Oracle
- modificar un recurso de volumen de aplicación de Oracle
- Eliminar un recurso de volumen de aplicación de Oracle mediante una clave
- recuperar los detalles secundarios del recurso de Oracle
- Realice una copia de seguridad del recurso de Microsoft SQL Server mediante el complemento para Microsoft SQL Server
- Realice una copia de seguridad del recurso Oracle mediante el complemento para la base de datos Oracle
- Realice una copia de seguridad del recurso personalizado mediante un complemento para una aplicación personalizada
- configurar la base de datos SAP HANA
- configurar la base de datos Oracle
- restaurar una copia de seguridad de una base de datos SQL
- restaurar una copia de seguridad de una base de datos Oracle
- restaurar una copia de seguridad de una aplicación personalizada
- crear un recurso de SAP HANA
- Proteger un recurso personalizado mediante un complemento para una aplicación personalizada
- Proteger un recurso de Microsoft SQL Server mediante un complemento para Microsoft SQL Server
- modificar un recurso protegido de Microsoft SQL Server
- eliminar la protección del recurso de Microsoft SQL Server
- Proteger un recurso de Oracle mediante un complemento para la base de datos de Oracle
- modificar un recurso protegido de Oracle
- eliminar la protección del recurso de Oracle
- Clonar un recurso desde la copia de seguridad mediante un complemento para una aplicación personalizada
- Clonar un volumen de aplicación Oracle desde la copia de seguridad mediante un complemento para la base de datos Oracle
- Clonar un recurso de Microsoft SQL Server desde la copia de seguridad mediante el complemento para Microsoft SQL Server
- Crear un ciclo de vida de clonación de un recurso de Microsoft SQL Server

- Modificar el ciclo de vida de los clones de un recurso de Microsoft SQL Server
- Eliminar el ciclo de vida del clon de un recurso de Microsoft SQL Server
- mover una base de datos existente de Microsoft SQL Server desde un disco local a un LUN de NetApp
- crear un archivo de especificación de clonación para una base de datos Oracle
- Iniciar un trabajo de actualización de clonación a pedido de un recurso de Oracle
- Cree un recurso de Oracle a partir de la copia de seguridad utilizando el archivo de especificación de clonación
- restaura la base de datos a la réplica secundaria y vuelve a unir la base de datos al grupo de disponibilidad
- crear un recurso de volumen de aplicación de Oracle

Copias de seguridad

Puede utilizar API para realizar diferentes operaciones.

- recuperar detalles de la copia de seguridad por nombre de copia de seguridad, tipo, complemento, recurso o fecha
- recuperar todas las copias de seguridad
- recuperar detalles de la copia de seguridad
- cambiar el nombre o eliminar copias de seguridad
- montar una copia de seguridad de Oracle
- desmontar una copia de seguridad de Oracle
- catalogar una copia de seguridad de Oracle
- Descatalogar una copia de seguridad de Oracle
- Obtenga todas las copias de seguridad necesarias para montarlas y realizar la recuperación en un punto determinado del tiempo

Clones

Puede utilizar API para realizar diferentes operaciones.

- crear, mostrar, modificar y eliminar el archivo de especificación de clonación de base de datos de Oracle
- mostrar la jerarquía de clones de la base de datos Oracle
- recuperar detalles del clon
- recuperar todos los clones
- eliminar clones
- recuperar detalles del clon por ID
- Iniciar un trabajo de actualización de clonación a pedido de un recurso de Oracle
- Clonar un recurso de Oracle desde la copia de seguridad utilizando el archivo de especificación de clonación

División de clones

Puede utilizar API para realizar diferentes operaciones.

- Estimar la operación de división de clones del recurso clonado
- recuperar el estado de una operación de división de clonación
- iniciar o detener una operación de división de clonación

Grupos de recursos

Puede utilizar API para realizar diferentes operaciones.

- recuperar detalles de todos los grupos de recursos
- recuperar el grupo de recursos por nombre
- Crear un grupo de recursos para el complemento de una aplicación personalizada
- Crear un grupo de recursos para el complemento de Microsoft SQL Server
- Crear un grupo de recursos para el complemento de la base de datos Oracle
- Modificar un grupo de recursos para un complemento para una aplicación personalizada
- Modificar un grupo de recursos para el complemento de Microsoft SQL Server
- Modificar un grupo de recursos para el complemento de la base de datos Oracle
- Crear, modificar o eliminar el ciclo de vida de un clon de un grupo de recursos para el complemento de Microsoft SQL Server
- realizar una copia de seguridad de un grupo de recursos
- Poner el grupo de recursos en modo de mantenimiento o producción
- eliminar un grupo de recursos

Políticas

Puede utilizar API para realizar diferentes operaciones.

- recuperar detalles de la póliza
- recuperar detalles de la póliza por nombre
- eliminar una política
- crear una copia de una política existente
- Crear o modificar la política para el complemento de una aplicación personalizada
- Crear o modificar la política para el complemento de Microsoft SQL Server
- Crear o modificar la política para el complemento de la base de datos Oracle
- Crear o modificar la política para el complemento de la base de datos SAP HANA

Almacenamiento

Puede utilizar API para realizar diferentes operaciones.

- recuperar todas las acciones

- recuperar una acción por nombre
- crear o eliminar un recurso compartido
- recuperar detalles de almacenamiento
- recuperar detalles de almacenamiento por nombre
- crear, modificar o eliminar un almacenamiento
- descubrir recursos en un clúster de almacenamiento
- recuperar recursos en un clúster de almacenamiento

Compartir

Puede utilizar API para realizar diferentes operaciones.

- recuperar los detalles de una acción
- recuperar detalles de todas las acciones
- crear o eliminar un recurso compartido en el almacenamiento
- recuperar una acción por nombre

Complementos

Puede utilizar API para realizar diferentes operaciones.

- enumerar todos los complementos para un host
- recuperar un recurso de Microsoft SQL Server usando una clave
- modificar un recurso personalizado usando una clave
- eliminar un recurso personalizado usando una clave
- recuperar un recurso de SAP HANA usando una clave
- modificar un recurso de SAP HANA usando una clave
- eliminar un recurso de SAP HANA usando una clave
- recuperar un recurso de Oracle usando una clave
- modificar un recurso de volumen de aplicación de Oracle utilizando una clave
- Eliminar un recurso de volumen de aplicación de Oracle mediante una clave
- Realice una copia de seguridad del recurso Microsoft SQL Server mediante un complemento para Microsoft SQL Server y una clave
- Realice una copia de seguridad del recurso Oracle mediante un complemento para la base de datos Oracle y una clave
- Realice una copia de seguridad del recurso de la aplicación personalizada mediante un complemento para la aplicación personalizada y una clave
- Configurar la base de datos SAP HANA usando una clave
- configurar la base de datos Oracle usando una clave
- restaurar una copia de seguridad de una aplicación personalizada usando una clave
- crear un recurso de SAP HANA
- crear un recurso de volumen de aplicación de Oracle

- Proteger un recurso personalizado mediante un complemento para una aplicación personalizada
- Proteger un recurso de Microsoft SQL Server mediante un complemento para Microsoft SQL Server
- modificar un recurso protegido de Microsoft SQL Server
- eliminar la protección del recurso de Microsoft SQL Server
- Proteger un recurso de Oracle mediante un complemento para la base de datos de Oracle
- modificar un recurso protegido de Oracle
- eliminar la protección del recurso de Oracle
- Clonar un recurso desde la copia de seguridad mediante un complemento para una aplicación personalizada
- Clonar un volumen de aplicación Oracle desde la copia de seguridad mediante un complemento para la base de datos Oracle
- Clonar un recurso de Microsoft SQL Server desde la copia de seguridad mediante el complemento para Microsoft SQL Server
- Crear un ciclo de vida de clonación de un recurso de Microsoft SQL Server
- Modificar el ciclo de vida de los clones de un recurso de Microsoft SQL Server
- Eliminar el ciclo de vida del clon de un recurso de Microsoft SQL Server
- crear un archivo de especificación de clonación para una base de datos Oracle
- Iniciar un ciclo de vida de clonación a pedido de un recurso de Oracle
- Clonar un recurso de Oracle desde la copia de seguridad utilizando el archivo de especificación de clonación

Informes

Puede utilizar API para realizar diferentes operaciones.

- recuperar informes de operaciones de copia de seguridad, restauración y clonación para los complementos respectivos
- agregar, ejecutar, eliminar o modificar programaciones
- recuperar datos para los informes programados

Alertas

Puede utilizar API para realizar diferentes operaciones.

- recuperar todas las alertas
- recuperar alertas por ID
- eliminar múltiples alertas o eliminar una alerta por ID

Rbac

Puede utilizar API para realizar diferentes operaciones.

- recuperar detalles de usuarios, grupos y roles
- agregar o eliminar usuarios

- asignar usuario a rol
- desasignar usuario de rol
- crear, modificar o eliminar roles
- asignar grupo a un rol
- desasignar un grupo de un rol
- agregar o eliminar grupos
- crear una copia de un rol existente
- Asignar o desasignar recursos a un usuario o grupo

Configuración

Puede utilizar API para realizar diferentes operaciones.

- ver los ajustes de configuración
- modificar los ajustes de configuración

Configuración del certificado

Puede utilizar API para realizar diferentes operaciones.

- Ver el estado del certificado para el servidor SnapCenter o el host del complemento
- modificar la configuración del certificado para el servidor SnapCenter o el host del complemento

Repositorio

Puede utilizar API para realizar diferentes operaciones.

- recuperar las copias de seguridad del repositorio
- ver la información de configuración sobre el repositorio
- proteger y restaurar el repositorio de SnapCenter
- desproteger el repositorio de SnapCenter
- Reconstruir y conmutar por error el repositorio

Versión

Puede utilizar esta API para ver la versión de SnapCenter .

Cómo acceder a las API REST mediante la página web de la API de Swagger

Las API REST se exponen a través de la página web Swagger. Puede acceder a la página web de Swagger para mostrar las API REST de SnapCenter Server, así como para emitir manualmente una llamada API. Puede utilizar las API REST para ayudar a administrar su servidor SnapCenter o para realizar operaciones de protección de datos.

Debe conocer la dirección IP de administración o el nombre de dominio del servidor SnapCenter en el que

desea ejecutar las API REST.

No necesita permisos especiales para ejecutar el cliente API REST. Cualquier usuario puede acceder a la página web de Swagger. Los permisos respectivos sobre los objetos a los que se accede a través de la API REST se basan en el usuario que genera el token para iniciar sesión en la API REST.

Pasos

1. Desde un navegador, ingrese la URL para acceder a la página web de Swagger en el formato `https://<dirección_IP_o_nombre_de_SnapCenter>:<puerto_de_SnapCenter>/swagger/`.



Asegúrese de que la URL de la API REST no tenga los siguientes caracteres: +, ., %, y &.

2. En el campo **Swagger Explore**, si la documentación de la 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 tipos o categorías de recursos de API.

4. Haga clic en un tipo de recurso de API para mostrar las API en ese tipo de recurso.

Si encuentra un comportamiento inesperado al ejecutar las API REST de SnapCenter, puede usar los archivos de registro para identificar la causa y resolver el problema. Puede descargar los archivos de registro desde la interfaz de usuario de SnapCenter haciendo clic en **Monitor > Registros > Descargar**.

Comience a utilizar la API REST

Puede comenzar a utilizar rápidamente la API REST de SnapCenter. Acceder a la API proporciona cierta perspectiva antes de comenzar a usarla con los procesos de flujo de trabajo más complejos en una configuración en vivo.

Hola Mundo

Puede ejecutar un comando simple en su sistema para comenzar a utilizar la API REST de SnapCenter y confirmar su disponibilidad.

Antes de empezar

- Asegúrese de que la utilidad Curl esté disponible en su sistema.
- Dirección IP o nombre de host del servidor SnapCenter
- Nombre de usuario y contraseña de una cuenta con autoridad para acceder a la API REST de SnapCenter



Si sus credenciales incluyen caracteres especiales, debe formatearlas de una manera que sea aceptable para Curl según el shell que esté utilizando. Por ejemplo, puede insertar una barra invertida antes de cada carácter especial o envolver todo el texto. `username:password` cadena entre comillas simples.

Paso

En la interfaz de la línea de comandos, ejecute lo siguiente para recuperar la información del complemento:

```
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 declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](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. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Puede encontrar una lista actualizada 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/"](https://www.netapp.com/company/legal/privacy-policy/)

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

["Aviso para SnapCenter 6.1"](#)

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.