Instalación del servidor SnapCenter

SnapCenter Software 4.6

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-46/install/install_workflow.html on September 29, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

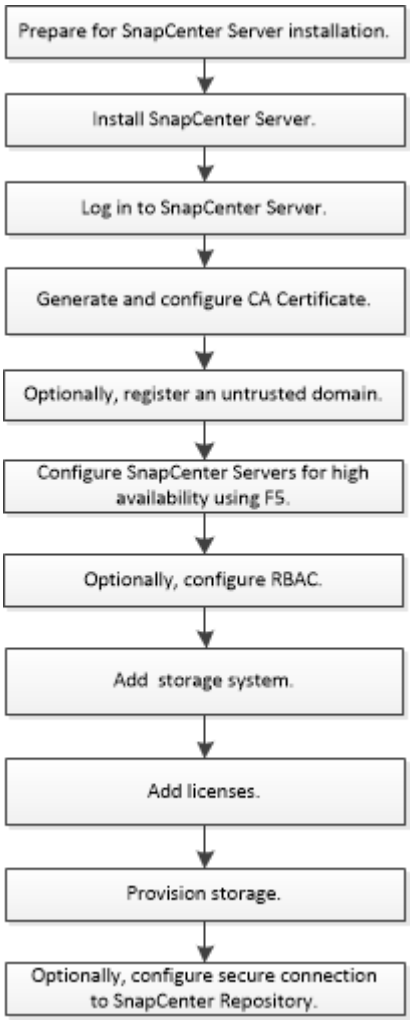
Instalación del servidor SnapCenter . . . 1
- Flujo de trabajo de instalación . . . 1
- Prepare la instalación del servidor SnapCenter . . . 1
  - Requisitos de dominio y grupo de trabajo . . . 1
  - Requisitos de espacio y de tamaño . . . 2
  - Requisitos del host SAN . . . 3
  - Sistemas de almacenamiento y aplicaciones compatibles . . . 3
  - Exploradores compatibles . . . 4
  - Requisitos de conexión y puerto . . . 4
  - Licencias SnapCenter . . . 8
  - Métodos de autenticación para las credenciales . . . 11
  - Conexiones de almacenamiento y credenciales . . . 12
- Instale el servidor SnapCenter . . . 13
- Inicie sesión en SnapCenter . . . 14
  - Modifique el tiempo de espera de sesión de interfaz gráfica de usuario predeterminada de SnapCenter . . . 16
  - Proteja el servidor web de SnapCenter mediante la desactivación de SSL 3.0 . . . 16
- Configurar certificado de CA . . . 16
  - Genere un archivo CSR de certificado de CA . . . 16
  - Importar certificados de CA . . . 17
  - Obtenga la huella digital del certificado de CA . . . 18
  - Configure el certificado de CA con servicios de plugins de host de Windows . . . 18
  - Configurar el certificado de CA con el sitio SnapCenter . . . 19
  - Habilite los certificados de CA para SnapCenter . . . 20
- Configure Active Directory, LDAP y LDAPS . . . 20
  - Registrar dominios de Active Directory que no son de confianza . . . 20
  - Configure el certificado de cliente de CA para LDAPS . . . 22
- Configuración de la alta disponibilidad . . . 23
  - Configurar servidores SnapCenter para alta disponibilidad mediante F5 . . . 23
  - Configure el balanceador de carga de red de Microsoft manualmente . . . 24
  - Cambie de NLB a F5 para ofrecer alta disponibilidad . . . 25
  - Alta disponibilidad del repositorio MySQL de SnapCenter . . . 25
  - Exportar certificados SnapCenter . . . 26
- Configurar el control de acceso basado en roles (RBAC) . . . 27
  - Añada un usuario o grupo y asigne roles y activos . . . 27
  - Crear un rol . . . 30
  - Añadir un rol de RBAC de ONTAP mediante comandos de inicio de sesión de seguridad . . . 31
  - Cree roles de SVM con privilegios mínimos . . . 32
  - Cree roles de clúster ONTAP con privilegios mínimos . . . 37
  - Configure los grupos de aplicaciones de IIS para habilitar los permisos de lectura de Active Directory . . . 42
- Añadir sistemas de almacenamiento . . . 43
- Añada licencias estándar basadas en controladora de SnapCenter . . . 47
  - Requisitos previos para añadir una licencia basada en controladora . . . 47

Añada una licencia basada en controladora . . . 51
Añada licencias basadas en capacidad estándar de SnapCenter . . . 52
Requisitos previos para añadir licencias basadas en capacidad . . . 53
Añada una licencia basada en capacidad . . . 55
Aprovisione su sistema de almacenamiento . . . 57
Aprovisionar almacenamiento en hosts Windows . . . 57
Aprovisione almacenamiento en entornos VMware . . . 73
Configure las conexiones MySQL protegidas con SnapCenter Server . . . 75
Configure conexiones MySQL protegidas para configuraciones de servidor SnapCenter independientes . . . 75
Configure conexiones MySQL protegidas para configuraciones de alta disponibilidad . . . 78
Funciones habilitadas en su host de Windows durante la instalación . . . 82

Instalación del servidor SnapCenter

Flujo de trabajo de instalación

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



Prepare la instalación del servidor SnapCenter

Requisitos de dominio y grupo de trabajo

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

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

- **Dominio de Active Directory**

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

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

- **Grupos de trabajo**

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

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

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

Requisitos de espacio y de tamaño

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

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

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

Requisitos del host SAN

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

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

- Utilidades de host

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

- Microsoft DSM para Windows MPIO

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

  Se requiere un DSM para configuraciones de alta disponibilidad.

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

Sistemas de almacenamiento y aplicaciones compatibles

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

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

de revisión P1 del software SnapCenter 4.5.

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

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

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

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

Exploradores compatibles

El software SnapCenter se puede usar en diversos exploradores.

- Cromo

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

- Internet Explorer

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

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

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

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

- Microsoft Edge

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

Requisitos de conexión y puerto

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

- Las aplicaciones no pueden compartir los puertos.

  Cada puerto debe ser dedicado a la aplicación adecuada.

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

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

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

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

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

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

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

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

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

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

Licencias SnapCenter

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

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

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

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

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

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

Licencias de Single Mailbox Recovery (SMBR)

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

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

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

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

Métodos de autenticación para las credenciales

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

Autenticación de Windows

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

Autenticación de dominio que no es de confianza

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

Autenticación de grupo de trabajo local

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

Autenticación de SQL Server

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

Autenticación de Linux

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

Autenticación AIX

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

Autenticación de base de datos de Oracle

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

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

Autenticación de Oracle ASM

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

Autenticación de catálogo de RMAN

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

Conexiones de almacenamiento y credenciales

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

- **Conexiones de almacenamiento**

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

- **Credenciales**

  - Administrador de dominio o cualquier miembro del grupo de administradores

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

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

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

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

  - Credenciales para grupos de recursos individuales

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

backup al nombre de usuario.

Instale el servidor SnapCenter

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

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

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

Lo que necesitará

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

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

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

- Pasos*

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

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

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

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

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

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

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

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

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

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

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

Inicie sesión en SnapCenter

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

Lo que necesitará

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

Acerca de esta tarea

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

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

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

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

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

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

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

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

- Pasos*

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

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

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

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

Resultados

Aparecerá la página Dashboard.

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

Después de terminar

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

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

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

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

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

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

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

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

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

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

Configurar certificado de CA

Genere un archivo CSR de certificado de CA

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

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

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

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

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

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

Importar certificados de CA

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

- Pasos*

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

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

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

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

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

Obtenga la huella digital del certificado de CA

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

- Pasos*

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

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

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

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie la huella digital.

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

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

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

- Pasos*

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

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

Por ejemplo:

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

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

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

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

Por ejemplo:

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

Configurar el certificado de CA con el sitio SnapCenter

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

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

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

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

Habilite los certificados de CA para SnapCenter

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

Lo que necesitará

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

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

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

Después de terminar

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

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

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

Configure Active Directory, LDAP y LDAPS

Registrar dominios de Active Directory que no son de confianza

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

Lo que necesitará

Protocolo LDAP y LDAPS

- Puede registrar los dominios de directorio activo que no son de confianza mediante los protocolos LDAP o LDAPS.
- Debe haber habilitado la comunicación bidireccional entre los hosts del plugin y SnapCenter Server.

- La resolución de DNS se debe configurar desde el servidor de SnapCenter a los hosts del plugin y viceversa.

Protocolo LDAP

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

  Puede registrar un dominio no confiable con el FQDN. Si el FQDN no se puede resolver desde el servidor SnapCenter, puede registrarse con una dirección IP de una controladora de dominio y esto debe poder resolverse desde el servidor SnapCenter.

Protocolo LDAPS

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

  "Configure el certificado de cliente de CA para LDAPS"

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

Acerca de esta tarea

- Puede utilizar la interfaz de usuario de SnapCenter, los cmdlets de PowerShell o la API DE REST para registrar un dominio que no es de confianza.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Configuración global**.
  3. En la página Global Settings (Configuración global), haga clic en **Configuración de dominio**.
  4. Haga clic en + para registrar un nuevo dominio.
  5. En la página Registrar nuevo dominio, seleccione **LDAP** o **LDAPS**.
     a. Si selecciona **LDAP**, especifique la información necesaria para registrar el dominio que no es de confianza para LDAP:

Para este campo…	Realice lo siguiente…
Nombre de dominio	Especifique el nombre NetBIOS para el dominio.
Dominio FQDN	Especifique el FQDN y haga clic en **resolver**.

Para este campo…	Realice lo siguiente…
Direcciones IP del controlador de dominio	Si el dominio FQDN no se puede resolver desde el servidor SnapCenter, especifique una o más direcciones IP de las controladoras de dominio. Para obtener más información, consulte "Agregue la IP del controlador de dominio para dominios que no sean de confianza desde la interfaz gráfica de usuario".

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

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

6. Haga clic en **Aceptar**.

Configure el certificado de cliente de CA para LDAPS

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

- Pasos*

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

6. Complete el asistente de la siguiente manera:

En esta ventana del asistente…	Haga lo siguiente…
En la segunda página del asistente	Haga clic en **examinar**, seleccione el *Root Certificate* y haga clic en **Siguiente**.
Finalización del Asistente para importación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación.

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

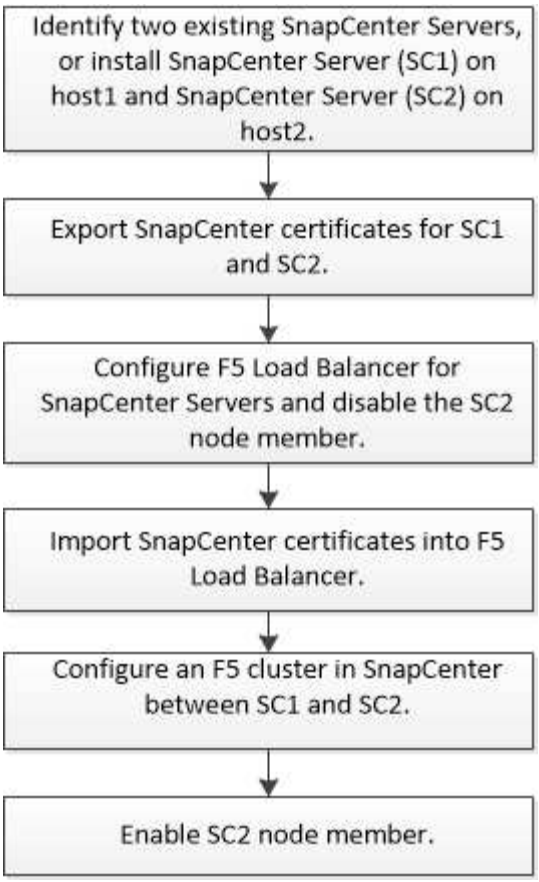
Configuración de la alta disponibilidad

Configurar servidores SnapCenter para alta disponibilidad mediante F5

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

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

La imagen del flujo de trabajo enumera los pasos para configurar SnapCenter Server para una alta disponibilidad utilizando el equilibrador de carga F5. Para obtener instrucciones detalladas, consulte "Cómo configurar instancias de SnapCenter Server para obtener una alta disponibilidad mediante el balanceador de carga F5".



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

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

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

Información de configuración adicional de F5

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

Configure el balanceador de carga de red de Microsoft manualmente

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

manualmente NLB fuera de la instalación de SnapCenter para obtener alta disponibilidad.

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

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

Cambie de NLB a F5 para ofrecer alta disponibilidad

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

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

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

Alta disponibilidad del repositorio MySQL de SnapCenter

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

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

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

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

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

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

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

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

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

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

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

Exportar certificados SnapCenter

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

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

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

Resultados

Los certificados se exportan en formato .pfx.

Configurar el control de acceso basado en roles (RBAC)

Añada un usuario o grupo y asigne roles y activos

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

Lo que necesitará

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

  Desde SnapCenter 4.5, sólo puede incluir los siguientes caracteres especiales en nombres de usuario y nombres de grupos: Espacio ( ), guión (-), guión bajo (_) y dos puntos (:). Si desea utilizar una función que ha creado en una versión anterior de SnapCenter con estos caracteres especiales, puede deshabilitar la validación del nombre de la función cambiando el valor del parámetro 'DisableSQLInjtionValidation' a TRUE en el archivo web.config ubicado en el que está instalado SnapCenter WebApp. Después de modificar el valor, no es necesario reiniciar el servicio.

- SnapCenter incluye varios roles predefinidos.

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

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

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

- Es necesario asignar un rol al usuario o grupo en algún momento para aprovechar los permisos y las eficiencias de RBAC.

- Puede asignar activos como host, grupos de recursos, políticas, conexión de almacenamiento, plugin, y las credenciales para el usuario mientras crea el usuario o el grupo.
- Los activos mínimos que debe asignar un usuario para realizar ciertas operaciones son los siguientes:

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

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

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

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

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

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

- Pasos*

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

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

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

b. En la tabla Asset, seleccione el activo.

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

c. Repita este procedimiento para todos los activos necesarios.

d. Haga clic en **Guardar**.

5. Haga clic en **Enviar**.

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

Crear un rol

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

Inició sesión con el rol de administrador de SnapCenter.

- Pasos*

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

   Desde SnapCenter 4.5, sólo puede incluir los siguientes caracteres especiales en nombres de usuario y nombres de grupos: Espacio ( ), guión (-), guión bajo (_) y dos puntos (:). Si desea utilizar una función que ha creado en una versión anterior de SnapCenter con estos caracteres especiales, puede deshabilitar la validación del nombre de la función cambiando el valor del parámetro 'DisableSQLInjtionValidation' a TRUE en el archivo web.config ubicado en el que está instalado SnapCenter WebApp. Después de modificar el valor, no es necesario reiniciar el servicio.

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

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

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

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

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

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

Lo que necesitará

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

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

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

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

Acerca de esta tarea

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

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

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

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

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

- Pasos*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cree roles de SVM con privilegios mínimos

Hay varios comandos de la CLI de ONTAP que debe ejecutar cuando crea un rol para un usuario de SVM nuevo en ONTAP. Este rol es obligatorio si configura SVM en ONTAP

para su uso con SnapCenter y no desea utilizar el rol vsadmin.

- Pasos*

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

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

   Debe repetir este comando para cada permiso.

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

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

2. Desbloquee el usuario.

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

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

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

- `security login role create -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -vserver SVM_Name -access all`
- `security login role create -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -vserver SVM_Name -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 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 update" -access all

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

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_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
```

Cree roles de clúster ONTAP con privilegios mínimos

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

- Pasos*

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

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

Debe repetir este comando para cada permiso.

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

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

2. Desbloquee el usuario.

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

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

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

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

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

"lun resize" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all

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

"volume online" -access all

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

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

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

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

- Pasos*

1. Abra el Administrador de IIS en el servidor de Windows donde está instalado SnapCenter.

2. En el panel de navegación izquierdo, haga clic en **grupos de aplicaciones**.
3. Seleccione SnapCenter en la lista grupos de aplicaciones y, a continuación, haga clic en **Configuración avanzada** en el panel acciones.
4. Seleccione identidad y, a continuación, haga clic en **…** para editar la identidad del grupo de aplicaciones SnapCenter.
5. En el campo cuenta personalizada, introduzca un nombre de usuario de dominio o de administrador de dominio con permiso de lectura de Active Directory.
6. Haga clic en Aceptar.

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

Añadir sistemas de almacenamiento

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

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

Lo que necesitará

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

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

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

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

Acerca de esta tarea

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

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

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

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

- Pasos*

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

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

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

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

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

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

      El puerto 443 predeterminado normalmente funciona.

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

      El valor predeterminado es 60 segundos.

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

Resultados

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

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

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

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

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

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

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

Después de terminar

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

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

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

Añada licencias estándar basadas en controladora de SnapCenter

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

La licencia basada en controladora tiene las siguientes características:

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

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

- Se bloqueó en el número de serie de la controladora

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

Requisitos previos para añadir una licencia basada en controladora

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

Comprobar si se ha instalado la licencia de SnapManager Suite

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

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

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

       Cuando hace clic en el nombre del clúster, todas las SVM que forman parte del clúster se muestran en la sección Storage Virtual Machines.
  3. En la lista Storage Connections, localice la columna Controller License.

     La columna Controller License muestra el siguiente estado:

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

Identifique las licencias instaladas en la controladora

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

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

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

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

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

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

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

Recupere el número de serie de la controladora

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

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

```
cluster1::> system show -instance

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

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

3. Registre los números de serie.

Recupere el número de serie de la licencia basada en controladora

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

Lo que necesitará

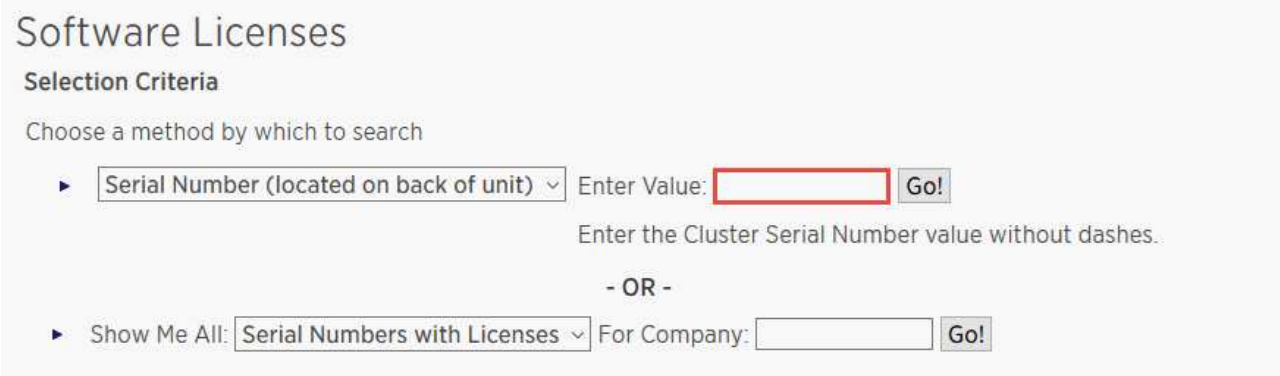
- Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.

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

- Debe tener el número de serie de la controladora.

- Pasos*

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



Se muestra una lista de licencias para la controladora especificada.

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

Añada una licencia basada en controladora

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

Lo que necesitará

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

Acerca de esta tarea

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

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

- Pasos*

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

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

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

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

```
license show
```

Elimine la licencia de prueba

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

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

- Pasos*

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

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

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

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

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

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

Añada licencias basadas en capacidad estándar de SnapCenter

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

La licencia tiene las siguientes características:

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

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

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

- Disponible por terabytes

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

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

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

Requisitos previos para añadir licencias basadas en capacidad

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

Calcular los requisitos de capacidad

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

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

Acerca de esta tarea

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

- Pasos*

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

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

     2   entries were displayed.
     ```

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

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

Recupere el número de serie de licencia basada en capacidad

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

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

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

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

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

  5. Registre el número de serie.

Genere un archivo de licencia de NetApp

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

Lo que necesitará

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

Añada una licencia basada en capacidad

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

Lo que necesitará

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

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

Acerca de esta tarea

Puede realizar las siguientes tareas en la página Settings:

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

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

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

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

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

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

   El umbral predeterminado es de 90 %.

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

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

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

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

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

Cómo calcula SnapCenter el uso de la capacidad

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

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

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

Aprovisione su sistema de almacenamiento

Aprovisionar almacenamiento en hosts Windows

Configurar el almacenamiento de LUN

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

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

Establecer una sesión iSCSI

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

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

   Se mostrará el asistente Establish Session.

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

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

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

   SnapCenter establecerá la sesión iSCSI.

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

Desconecte una sesión iSCSI

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

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

     SnapCenter desconectará la sesión iSCSI.

Cree y gestione grupos

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

Cree un igroup

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

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

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

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

     SnapCenter creará el igroup en el sistema de almacenamiento.

Cambiar el nombre de un igroup

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

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

Modificar un igroup

Es posible usar SnapCenter para añadir iniciadores de igroups a un grupo existente. Durante la creación de

un igroup, puede añadir un solo host. Si desea crear un igroup para un clúster, puede modificar el igroup a fin de añadir nodos a ese igroup.

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

Eliminar un igroup

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

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

     SnapCenter eliminará el igroup.

Crear y gestionar discos

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

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

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

Ver los discos en un host

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

- Pasos*

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

   Se muestra una lista de los discos.

Vea los discos en clúster

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

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

     Se muestra una lista de los discos.

Crear LUN o discos conectados mediante FC o iSCSI

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

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

Lo que necesitará

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

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

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

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

Acerca de esta tarea

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

2. En la página hosts, haga clic en **Disks**.
3. Seleccione el host en la lista desplegable **Host**.
4. Haga clic en **Nuevo**.

   Se abrirá el asistente Create Disk.

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

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

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

Seleccione…	Si…
Disco dedicado	Solo un host puede acceder al LUN. Ignore el campo **Grupo de recursos**.
Disco compartido	El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server. Introduzca el nombre del grupo de recursos del clúster en el campo **Grupo de recursos**. Es necesario crear el disco en un solo host del clúster de conmutación al nodo de respaldo.

Seleccione…	Si…
Volumen compartido de clúster (CSV)	El LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server donde se utilizan volúmenes compartidos de clúster. Introduzca el nombre del grupo de recursos del clúster en el campo **Grupo de recursos**. Asegúrese de que el host en el que se crea el disco sea el propietario del grupo de clústeres.

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

Propiedad	Descripción
Asignación automática del punto de montaje	SnapCenter asigna de forma automática un punto de montaje de volumen según la unidad del sistema. Por ejemplo, si la unidad del sistema es C:, la asignación automática crea un punto de montaje de volumen debajo de la unidad C: (C:\scmnpt\). La asignación automática no es compatible con los discos compartidos.
Asignar letra de unidad	Monte el disco en la unidad seleccionada en la lista desplegable adyacente.
Utilice punto de montaje de volumen	Monte el disco en la ruta de unidad especificada en el campo adyacente. La raíz del punto de montaje de volumen debe ser propiedad del host en el que se crea el disco.
No asigne la letra de unidad ni el punto de montaje de volumen	Seleccione esta opción si prefiere montar el disco manualmente en Windows.
Tamaño de LUN	Especifique el tamaño del LUN; el valor mínimo es 150 MB. Seleccione MB, GB o TB en la lista desplegable contigua.

Propiedad	Descripción
Use thin provisioning para el volumen que aloja este LUN	Aprovisione con thin provisioning el LUN. Thin provisioning solo asigna la cantidad de espacio de almacenamiento que se necesita en un momento. Esto permite que el LUN se expanda de forma eficiente hasta la capacidad máxima disponible. Asegúrese de que el espacio disponible en el volumen sea suficiente para acomodar todo el almacenamiento de LUN que considere necesario.
Elija el tipo de partición	Seleccione una partición GPT para una tabla de particiones GUID o una partición MBR para un registro de arranque maestro. Las particiones MBR pueden generar problemas de desalineación en los clústeres de conmutación al nodo de respaldo de Windows Server. No se admiten los discos de partición de firmware extensible unificado (UEFI).

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

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

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

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

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

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

Cambiar el tamaño de un disco

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

Acerca de esta tarea

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

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

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

     Se muestra una lista de los discos.

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

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

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

   SnapCenter cambiará el tamaño del disco.

Conectar un disco

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

Lo que necesitará

- Inició el servicio iSCSI o FC en el sistema de almacenamiento.
- Si utiliza iSCSI, debe haber establecido una sesión iSCSI con el sistema de almacenamiento.
- No se puede conectar un LUN a más de un host a menos que el LUN se comparta entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.
- Si el LUN se comparte entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server donde se utilizan volúmenes compartidos de clúster (CSV), es necesario conectar el disco en el host propietario del grupo de clústeres.
- Se debe instalar el plugin para Windows únicamente en el host donde se conecta el disco.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Disks**.
  3. Seleccione el host en la lista desplegable **Host**.
  4. Haga clic en **conectar**.

     Se abrirá el asistente Connect Disk.

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

En este campo…	Realice lo siguiente…
Sistema de almacenamiento	Seleccione la máquina virtual de almacenamiento SVM para el LUN.
Ruta de LUN	Haga clic en **examinar** para seleccionar la ruta completa del volumen que contiene el LUN.
Nombre de LUN	Introduzca el nombre del LUN.
Tamaño del clúster	Seleccione el tamaño de la asignación de bloques LUN para el clúster. El tamaño del clúster varía según el sistema operativo y las aplicaciones.

En este campo…	Realice lo siguiente…
Etiqueta de LUN	De forma opcional, puede introducir un texto descriptivo para el LUN.

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

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

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

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

Propiedad	Descripción
No asigne la letra de unidad ni el punto de montaje de volumen	Seleccione esta opción si prefiere montar el disco manualmente en Windows.

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

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

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

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

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

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

Desconectar un disco

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

Lo que necesitará

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

Acerca de esta tarea

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

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

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

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

     SnapCenter desconectará el disco.

Eliminar un disco

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

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

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

     SnapCenter eliminará el disco.

Cree y gestione recursos compartidos de SMB

Para configurar un recurso compartido de SMB3 en una máquina virtual de

almacenamiento (SVM), se puede usar la interfaz de usuario de SnapCenter o cmdlets de PowerShell.

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

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

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

Cree un recurso compartido de SMB

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

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

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

     Se abrirá el cuadro de diálogo New Share.

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

En este campo…	Realice lo siguiente…
Descripción	Introduzca un texto descriptivo para el recurso compartido.

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

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

   SnapCenter creará el recurso compartido de SMB en la SVM.

Eliminar un recurso compartido de SMB

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

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

     SnapCenter eliminará el recurso compartido de SMB de la SVM.

Recupere espacio en el sistema de almacenamiento

Si bien NTFS hace un seguimiento del espacio disponible en un LUN cuando se modifican o se eliminan archivos, no provee la nueva información al sistema de

almacenamiento. Es posible ejecutar la recuperación de espacio mediante el cmdlet de PowerShell en el host del plugin para Windows a fin de garantizar que los bloques recién liberados se marquen como disponibles en el almacenamiento.

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

Lo que necesitará

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

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

Acerca de esta tarea

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

  Ya que al hacerlo se ralentiza el proceso de recuperación.

Paso

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

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

Drive_path es la ruta de la unidad asignada al LUN.

Aprovisionar el almacenamiento mediante cmdlets de PowerShell

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

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

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

Aprovisione almacenamiento en entornos VMware

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

Plataformas de sistemas operativos invitados compatibles con VMware

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

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

- LUN de RDM

  Compatible con un máximo de 56 LUN de RDM con cuatro controladoras SCSI LSI Logic para RDMS normales, o 42 LUN de RDM con tres controladoras SCSI LSI Logic en una configuración del plugin para Windows de buzón a buzón MSCS para máquinas virtuales VMware

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

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

Limitaciones relacionadas con el servidor ESXi de VMware

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

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

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

Privilegios mínimos de vCenter requeridos para operaciones de RDM en SnapCenter

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

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

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

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

Gestione LUN de RDM FC en un clúster de Microsoft

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

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

Requisitos

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

- Las máquinas virtuales (VM) deben ejecutar la misma versión de Windows Server.
- Las versiones del servidor ESX o ESXi deben ser las mismas para cada host primario de VMware.
- Cada host primario debe tener al menos dos adaptadores de red.
- Debe haber al menos un almacén de datos de VMware Virtual Machine File System (VMFS) compartido entre los dos servidores ESX o ESXi.
- VMware recomienda que el almacén de datos compartido se cree en una FC SAN.

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

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

  No se pueden usar discos virtuales para almacenamiento compartido.

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

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

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

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

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

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

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

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

Limitaciones

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

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

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

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

- No se admiten los iniciadores de ESX iSCSI y los adaptadores de bus de host en los discos compartidos de un clúster de Microsoft.
- El plugin para Windows no admite la migración de máquinas virtuales con vMotion si las máquinas virtuales forman parte de un clúster de Microsoft.
- El plugin para Windows no admite MPIO en máquinas virtuales de un clúster de Microsoft.

Cree un LUN de RDM FC compartido

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

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

Configure las conexiones MySQL protegidas con SnapCenter Server

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

Configure conexiones MySQL protegidas para configuraciones de servidor SnapCenter independientes

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

Se generan los siguientes certificados:

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

- Pasos*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Detenga la aplicación web del servidor SnapCenter en el servidor de información de Internet (IIS).
5. Reinicie el servicio MySQL.
6. Actualice el valor de la clave MySQLProtocol en el archivo web.config.

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

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

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

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

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

+

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

+

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

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

Configure conexiones MySQL protegidas para configuraciones de alta disponibilidad

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

Se generan los siguientes certificados:

- Certificado de CA

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

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

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

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

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

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

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

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

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

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

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

   Debe especificar las rutas del certificado de CA, del certificado público de cliente y de la clave privada

de cliente en la sección [client] el archivo de configuración del servidor MySQL (my.ini).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

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

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

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

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

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

+

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

+

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

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

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

Funciones habilitadas en su host de Windows durante la instalación

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

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

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

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.