Instalar y configurar SnapCenter Server

SnapCenter software

NetApp
January 09, 2026

Tabla de contenidos

Instalar y configurar SnapCenter Server

Prepare la instalación del servidor SnapCenter

Requisitos para instalar el servidor SnapCenter

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

Requisitos del dominio y grupos de trabajo para el host Windows

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

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

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

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

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

Requisitos de espacio y de tamaño

Debería estar familiarizado con los requisitos de espacio y tamaño.

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

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

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

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

Requisitos del host SAN

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

- Utilidades de host: Las utilidades de host son compatibles con FC e iSCSI, y le permiten usar MPIO en sus servidores Windows. "Más información".
- Microsoft DSM para Windows MPIO: Este software funciona con controladores Windows MPIO para gestionar varias rutas entre equipos host de Windows y NetApp. Se requiere un DSM para configuraciones de alta disponibilidad.

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

Requisitos de navegador

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

Requisitos de puertos

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

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

instalación si no quiere usar el predeterminado.

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

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

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

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

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

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

Nombre de puerto	Números de puerto	Protocolo	Dirección	Descripción
Plugin de SnapCenter para base de datos SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidireccional	Para un tenant único de un contenedor de base de datos multitenant (MDC), el número del puerto termina en 13; para los que no son MDC, el número de puerto termina en 15. Puede personalizar el número de puerto.
Complemento de SnapCenter para PostgreSQL	5432			Este puerto es el puerto PostgreSQL predeterminado utilizado para la comunicación del plugin para PostgreSQL con el clúster PostgreSQL. Puede personalizar el número de puerto.

Regístrese para acceder al software de SnapCenter

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

Antes de empezar

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

Acerca de esta tarea

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

Pasos

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

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

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

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

Autenticación multifactor (MFA)

Gestionar la autenticación multifactor (MFA)

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

Habilitar la autenticación multifactor (MFA)

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

Acerca de esta tarea

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

Antes de empezar

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

  El certificado DE CA es obligatorio por los siguientes motivos:

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

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

Pasos

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

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

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

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

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

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

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

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

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

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

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

Actualizar metadatos de MFA de AD FS

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

Pasos

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

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

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

Actualice los metadatos de MFA de SnapCenter

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

desastres, etc.

Pasos

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

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

   c. Habilite la autenticación multifactor (MFA).

      Consulte "Active la autenticación multifactor".

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

Deshabilitar la autenticación multifactor (MFA)

Pasos

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

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

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

Configure AD FS como OAuth/OIDC

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

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

  4. Selecciona **Generar secreto compartido**.

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

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

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

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

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

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

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

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

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

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

c. Haga clic en **Finalizar**.

Crear grupo de aplicaciones con comandos de PowerShell

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

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

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

   `ClientRoleIdentifier` nombre del grupo de aplicaciones

   `redirectURL` URL válida para redirección después de la autorización

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

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

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

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

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

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

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

   ```
   "client_id = $identifier"

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

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

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

   $transformrule = @"

   @RuleTemplate = "LdapClaims"

   @RuleName = "AD User properties and Groups"

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

```
"AD AUTHORITY"]

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

"@
```

6. Escriba el archivo de reglas de transformación.

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

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

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Actualizar tiempo de caducidad del token de acceso

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

Acerca de esta tarea

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

Paso

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

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

Obtenga el token portador de AD FS

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

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

Campo	Valor

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

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

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

Autenticación CLI MFA de SnapCenter

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

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

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

Autenticación de la API de REST MFA de SnapCenter

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

Flujo de trabajo de la API de REST de MFA

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

Acerca de esta tarea

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

Para autenticarse a través de AD FS MFA

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

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

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

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

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

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

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

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

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

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

GUI

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

Interfaz PowerShell

- Pasos*

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

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

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

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

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

Interfaz SCCLI

- Pasos*

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

API REST

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

Parámetro	Valor
Dirección URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Publicación
Cuerpo de la solicitud	{ «IsGuiMFAEnabled»: Falso, «IsRestApiMFAEnabled»: Verdadero, «IsCliMFAEnabled»: Falso, ADFSConfigFilePath: C:\\ADFS_metadata\\abc.xml }
Cuerpo de respuesta	{ «MFAConfiguration»: { «IsGuiMFAEnabled»: Falso, «ADFSConfigFilePath»: «C:\\ADFS_metadata\\abc.xml», «SCConfigFilePath»: Null, «IsRestApiMFAEnabled»: Verdadero, «IsCliMFAEnabled»: Falso, «ADFSHostName»: «win-adfs-sc49.winscedom2.com» } }

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

Parámetro	Valor
Dirección URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Obtenga
Cuerpo de respuesta	{ «MFAConfiguration»: { «IsGuiMFAEnabled»: Falso, «ADFSConfigFilePath»: «C:\\ADFS_metadata\\abc.xml», «SCConfigFilePath»: Null, «IsRestApiMFAEnabled»: Verdadero, «IsCliMFAEnabled»: Falso, «ADFSHostName»: «win-adfs-sc49.winscedom2.com» } }

Instale el servidor SnapCenter

Instale el servidor de SnapCenter en el host de Windows

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

De forma opcional, puede ejecutar diversos procedimientos de instalación y configuración mediante cmdlets de PowerShell. Debe utilizar PowerShell 7.4.2 o posterior.

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

Antes de empezar

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

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

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

Pasos

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

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

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

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

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

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

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

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

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

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

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

Funciones habilitadas en el host de Windows durante la instalación

El instalador de SnapCenter Server habilita las funciones de Windows y los roles en el host de Windows durante la instalación Estos podrían ser de interés para solucionar problemas y realizar mantenimiento al sistema host.

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

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

Instale el servidor SnapCenter en el host Linux

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

Antes de empezar

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

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

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

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

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

- La ruta de acceso utilizada para el directorio PID de MySQL es */var/opt/mysqld*. Ejecute los siguientes comandos para establecer los permisos para la instalación de MySQL.
  - `mkdir /var/opt/mysqld`
  - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
  - `sudo restorecon -Rv /var/opt/mysqld`
- La ruta utilizada para el directorio Data de MySQL es */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Ejecute los siguientes comandos para establecer los permisos para el directorio de datos de MySQL.
  - `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
  - `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
  - `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

Acerca de esta tarea

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

Pasos

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

`(el8/el9/sles15).bin`

5. Realice una de las acciones para instalar el servidor SnapCenter.

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

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

El futuro

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

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

Funciones habilitadas en el host Linux durante la instalación

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

- RabbitMQ
- Erlang

Registre SnapCenter

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

Pasos

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

Inicie sesión en SnapCenter mediante la autorización de RBAC

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

Antes de empezar

- Debe habilitar el servicio de activación de procesos de Windows (WAS) en Windows Server Manager.
- Si desea utilizar Internet Explorer como explorador para iniciar sesión en el servidor SnapCenter, debe asegurarse de que el modo protegido de Internet Explorer está deshabilitado.
- Si el servidor SnapCenter está instalado en el host Linux, debe iniciar sesión mediante la cuenta de usuario que se utilizó para instalar el servidor de SnapCenter.

Acerca de esta tarea

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

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

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

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

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

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

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

- Pasos*

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

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

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

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

resultado

Aparecerá la página Dashboard.

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

Después de terminar

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

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

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

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

Inicie sesión en SnapCenter con la autenticación multifactor (MFA)

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

Antes de empezar

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

Acerca de esta tarea

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

1. Inicie SnapCenter desde el acceso directo creado en el escritorio de host local, o desde la URL provista al final de la instalación o desde la URL que proporcionó el administrador de SnapCenter.
2. En la página de inicio de sesión de AD FS, introduzca Username y Password.

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

   - Si el nombre de usuario o la contraseña son válidos

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

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

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

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

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

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

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

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

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

- Pasos*
  1. Para iniciar el Editor del Registro en el host del servidor web SnapCenter, haga clic en **Inicio** > **Ejecutar** y, a continuación, escriba regedit.
  2. En el Editor del Registro, desplácese hasta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
     - Si la clave del servidor ya existe:
       i. Seleccione el DWORD activado y, a continuación, haga clic en **Editar** > **Modificar**.
       ii. Cambie el valor a 0 y, a continuación, haga clic en **Aceptar**.
     - Si la clave del servidor no existe:

i. Haga clic en **Editar** > **Nuevo** > **clave** y, a continuación, asigne un nombre al servidor de claves.

ii. Con la nueva clave de servidor seleccionada, haga clic en **Edición** > **Nuevo** > **DWORD**.

iii. Asigne un nombre al nuevo DWORD activado y, a continuación, introduzca 0 como el valor.

3. Cierre el Editor del Registro.

Configurar el servidor SnapCenter

Agregar y aprovisionar el sistema de almacenamiento

Añadir sistemas de almacenamiento

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

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

Antes de empezar

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

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

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

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

Acerca de esta tarea

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

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

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

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

- Pasos*

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

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

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

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

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

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

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

   El puerto 443 predeterminado normalmente funciona.

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

   El valor predeterminado es 60 segundos.

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

resultado

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

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

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

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

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

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

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

Después de terminar

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

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

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

Conexiones de almacenamiento y credenciales

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

Conexiones de almacenamiento

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

Credenciales

- Administrador de dominio o cualquier miembro del grupo de administradores

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

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

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

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

- Credenciales para grupos de recursos individuales

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

Aprovisionar almacenamiento en hosts Windows

Cree y gestione grupos

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

Cree un igroup

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

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

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

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

SnapCenter creará el igroup en el sistema de almacenamiento.

Cambiar el nombre de un igroup

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

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

Modificar un igroup

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

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

Eliminar un igroup

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

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

     SnapCenter eliminará el igroup.

Crear y gestionar discos

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

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

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

Ver los discos en un host

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

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

     Se muestra una lista de los discos.

Vea los discos en clúster

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

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

     Se muestra una lista de los discos.

Establecer una sesión iSCSI

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

     Se mostrará el asistente Establish Session.

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

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

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

     SnapCenter establecerá la sesión iSCSI.

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

Crear LUN o discos conectados mediante FC o iSCSI

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

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

Antes de empezar

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

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

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

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

Acerca de esta tarea

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

     Se abrirá el asistente Create Disk.

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

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

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

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

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

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

Propiedad	Descripción
Asignación automática del punto de montaje	SnapCenter asigna de forma automática un punto de montaje de volumen según la unidad del sistema. Por ejemplo, si la unidad del sistema es C:, la asignación automática crea un punto de montaje de volumen debajo de la unidad C: (C:\scmnpt\). La asignación automática no es compatible con los discos compartidos.
Asignar letra de unidad	Monte el disco en la unidad seleccionada en la lista desplegable adyacente.

Propiedad	Descripción
Utilice punto de montaje de volumen	Monte el disco en la ruta de unidad especificada en el campo adyacente. La raíz del punto de montaje de volumen debe ser propiedad del host en el que se crea el disco.
No asigne la letra de unidad ni el punto de montaje de volumen	Seleccione esta opción si prefiere montar el disco manualmente en Windows.
Tamaño de LUN	Especifique el tamaño del LUN; el valor mínimo es 150 MB. Seleccione MB, GB o TB en la lista desplegable contigua.
Use thin provisioning para el volumen que aloja este LUN	Aprovisione con thin provisioning el LUN. Thin provisioning solo asigna la cantidad de espacio de almacenamiento que se necesita en un momento. Esto permite que el LUN se expanda de forma eficiente hasta la capacidad máxima disponible. Asegúrese de que el espacio disponible en el volumen sea suficiente para acomodar todo el almacenamiento de LUN que considere necesario.
Elija el tipo de partición	Seleccione una partición GPT para una tabla de particiones GUID o una partición MBR para un registro de arranque maestro. Las particiones MBR pueden generar problemas de desalineación en los clústeres de conmutación al nodo de respaldo de Windows Server. No se admiten los discos de partición de firmware extensible unificado (UEFI).

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

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

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

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

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

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

Cambiar el tamaño de un disco

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

Acerca de esta tarea

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

- Los LUN con particiones tipo GPT tienen un límite de tamaño del sistema de almacenamiento de 16 TB.
- Se recomienda realizar una snapshot antes de cambiar el tamaño de un LUN.
- Si se necesita restaurar un LUN de una snapshot realizada antes de cambiar el tamaño de la LUN, SnapCenter cambia automáticamente el tamaño del LUN al tamaño de la snapshot.

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

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

     Se muestra una lista de los discos.

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

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

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

     SnapCenter cambiará el tamaño del disco.

Conectar un disco

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

Antes de empezar

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

Se abrirá el asistente Connect Disk.

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

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

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

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

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

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

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

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

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

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

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

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

Desconectar un disco

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

     Se muestra una lista de los discos.

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

SnapCenter desconectará el disco.

Eliminar un disco

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

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

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

     SnapCenter eliminará el disco.

Cree y gestione recursos compartidos de SMB

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

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

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

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

Cree un recurso compartido de SMB

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

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

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

Se abrirá el cuadro de diálogo New Share.

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

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

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

   SnapCenter creará el recurso compartido de SMB en la SVM.

Eliminar un recurso compartido de SMB

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

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

SnapCenter eliminará el recurso compartido de SMB de la SVM.

Recupere espacio en el sistema de almacenamiento

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

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

Antes de empezar

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

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

Acerca de esta tarea

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

  Ya que al hacerlo se ralentiza el proceso de recuperación.

Paso

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

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

Drive_path es la ruta de la unidad asignada al LUN.

Aprovisionar el almacenamiento mediante cmdlets de PowerShell

Si no desea utilizar la GUI de SnapCenter para realizar trabajos de aprovisionamiento de host y recuperación de espacio, puede usar los cmdlets de PowerShell. Puede usar los cmdlets directamente o añadirlos a scripts.

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

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

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

Aprovisione almacenamiento en entornos VMware

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

Plataformas de sistemas operativos invitados compatibles con VMware

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

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

- LUN de RDM

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

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

Limitaciones relacionadas con el servidor ESXi de VMware

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

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

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

Privilegios mínimos de vCenter requeridos para operaciones de RDM en SnapCenter

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

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

- Máquina virtual: Configuración

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

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

Gestione LUN de RDM FC en un clúster de Microsoft

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

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

Requisitos

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

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

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

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

  No se pueden usar discos virtuales para almacenamiento compartido.

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

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

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

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

- Los clústeres de máquinas virtuales de Microsoft no pueden formar parte de un clúster de VMware.
- Es necesario utilizar credenciales de vCenter, no de ESX o ESXi al instalar el plugin para Windows en máquinas virtuales que pertenecen a un clúster de Microsoft.

- El plugin para Windows no puede crear un iGroup individual con iniciadores de varios hosts.

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

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

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

Limitaciones

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

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

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

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

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

Cree un LUN de RDM FC compartido

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

El disco compartido no se crea 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".

Añada licencias estándar basadas en controladora de SnapCenter

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

La licencia basada en controladora tiene las siguientes características:

- Autorización para licencia estándar de SnapCenter incluida con la compra de los paquetes Premium o Flash Bundle (no con el paquete básico)
- Uso de almacenamiento ilimitado
- Se agrega directamente al controlador de almacenamiento FAS, AFF o ASA mediante el Administrador del sistema ONTAP o la CLI de ONTAP .

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

- Se bloqueó en el número de serie de la controladora

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

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

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

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

Pasos

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

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

   La columna Controller License muestra el siguiente estado:

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

Paso 2: Identificar las licencias instaladas en la controladora

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

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

Pasos

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

   Resultado de ejemplo

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

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

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

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

Paso 3: Recupere el número de serie de la controladora

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

Pasos

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

Resultado de ejemplo

```
cluster1::> system show -instance

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

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

3. Registre los números de serie.

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

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

Antes de empezar

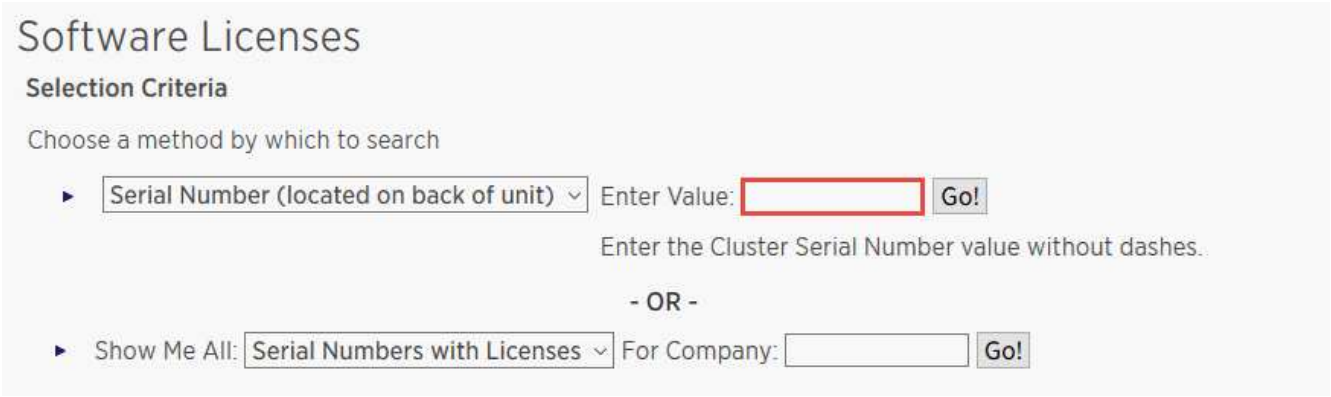
- Debe tener credenciales de inicio de sesión válidas en el sitio de soporte de NetApp.

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

- Debe tener el número de serie de la controladora.

Pasos

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



Se muestra una lista de licencias para la controladora especificada.

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

Paso 5: Añada una licencia basada en controladora

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

Antes de empezar

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

Acerca de esta tarea

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

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

Pasos

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

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

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

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

```
license show
```

Paso 6: Eliminar la licencia de prueba

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

> La eliminación manual de una licencia de prueba solo es necesaria si utiliza una licencia estándar basada en controladora de SnapCenter.

Pasos

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

      Para obtener información sobre los cmdlets, consulte "Guía de referencia de cmdlets de SnapCenter Software" .
2. Abra el símbolo del sistema y ejecute mysql -u root -p para conectarse a MySQL.

   MySQL le solicita la contraseña. Introduzca las credenciales que proporcionó al restablecer la contraseña.
3. Elimine la licencia de prueba de la base de datos:

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

Configuración de la alta disponibilidad

Configurar servidores SnapCenter para alta disponibilidad

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

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

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

Configurar la alta disponibilidad con F5

Para obtener instrucciones sobre cómo configurar los servidores SnapCenter para alta disponibilidad mediante el balanceador de carga F5, consulte "Cómo configurar instancias de SnapCenter Server para obtener una alta disponibilidad mediante el balanceador de carga F5" .

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

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

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

Información adicional

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

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

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

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

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

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

Pasos

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

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

Configure la alta disponibilidad con el balanceador de carga de Azure

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

Pasos

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

== Cambiar de NLB a F5 para alta disponibilidad

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

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

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

Alta disponibilidad del repositorio MySQL de SnapCenter

La replicación de MySQL es una de las características de MySQL Server que permite replicar datos de un servidor de bases de datos de MySQL (maestro) a otro servidor de

bases de datos de MySQL (esclavo). SnapCenter admite la replicación de MySQL para alta disponibilidad solamente en dos nodos habilitados para el balanceo de carga de red (NLB, Network Load Balancing).

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

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

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

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

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

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

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

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

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

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

Configurar el control de acceso basado en roles (RBAC)

Crear un rol

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

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

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.

2. En la página Configuración, haga clic en **roles**.
3. Haga clic en +.
4. Especifique un nombre y una descripción para el nuevo rol.

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

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

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

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

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

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

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

Antes de empezar

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

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

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

- Asigne roles a los usuarios.
- Identifique su configuración dependiendo de si sus complementos de SnapCenter están conectados a la IP del administrador de clúster para todo el clúster o conectados directamente a una SVM dentro del clúster.

Acerca de esta tarea

Para simplificar la configuración de estos roles en los sistemas de almacenamiento, puede utilizar la herramienta RBAC User Creator para NetApp ONTAP, que se encuentra publicada en el Foro de Comunidades de NetApp.

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

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

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

Pasos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cree roles de SVM con privilegios mínimos

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

- Pasos*

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

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

Debe repetir este comando para cada permiso.

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

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

2. Desbloquee el usuario.

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

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

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

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

"lun igroup add" -access all

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

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

"volume qtree modify" -access all

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

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

Crear roles de SVM para sistemas ASA R2

Hay varios comandos CLI de ONTAP que debe ejecutar para crear una función para un

nuevo usuario de SVM en sistemas ASA r2. Esta función es necesaria si configura SVM en sistemas ASA r2 para usar con SnapCenter y no desea utilizar la función vsadmin.

- Pasos*

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

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

   Debe repetir este comando para cada permiso.

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

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

2. Desbloquee el usuario.

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

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

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

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

"lun igroup delete" -access all

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

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

"volume restrict" -access all

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

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

"volume delete" -access all

- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

Cree roles de clúster ONTAP con privilegios mínimos

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

- Pasos*

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

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

Debe repetir este comando para cada permiso.

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

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

2. Desbloquee el usuario.

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

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

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

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun offline" -access all

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

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

"system node modify" -access all

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

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

"vserver cifs show" -access all

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

Cree roles de clúster de ONTAP para sistemas ASA R2

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

- Pasos*

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

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

Debe repetir este comando para cada permiso.

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

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

2. Desbloquee el usuario.

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

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

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

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

"lun igroup rename" -access all

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

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

"snapmirror show" -access all

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

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

"vserver" -access all

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

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

Añada un usuario o grupo y asigne roles y activos

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

Antes de empezar

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

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

- SnapCenter incluye varios roles predefinidos.

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

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

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

- Es necesario asignar un rol al usuario o grupo en algún momento para aprovechar los permisos y las eficiencias de RBAC.
- Puede asignar activos como host, grupos de recursos, políticas, conexión de almacenamiento, plugin, y las credenciales para el usuario mientras crea el usuario o el grupo.
- Los activos mínimos que debe asignar un usuario para realizar ciertas operaciones son los siguientes:

Funcionamiento	Asignación de activos
Proteja los recursos	host, política
Backup	host, grupo de recursos, política

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

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

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

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

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

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

- Pasos*

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

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

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

b. En la tabla Asset, seleccione el activo.

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

c. Repita este procedimiento para todos los activos necesarios.

d. Haga clic en **Guardar**.

5. Haga clic en **Enviar**.

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

Configure los ajustes del registro de auditoría

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

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

Inició sesión con el rol de administrador de SnapCenter.

Acerca de esta tarea

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

  No se admiten las unidades compartidas o montadas en red.

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

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

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

Pasos

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

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

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

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

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

Configure las conexiones MySQL protegidas con SnapCenter Server

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

Configure conexiones MySQL protegidas para configuraciones de servidor SnapCenter independientes

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

Se generan los siguientes certificados:

- Certificado de CA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

Configure conexiones MySQL protegidas para configuraciones de alta disponibilidad

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

Se generan los siguientes certificados:

- Certificado de CA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

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

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

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

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

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

+

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

+

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

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

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

Configure la autenticación basada en certificados

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

Habilite la autenticación basada en certificados

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

- Para habilitar la autenticación basada en certificados de cliente:

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

- Para desactivar la autenticación basada en certificados de cliente:

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

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

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

Antes de empezar

Debe haber configurado el SSL bidireccional.

- Pasos*

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

Para esta opción…	Haga lo siguiente…
Exportar clave privada	Seleccione **No, no exporte la clave privada** y luego haga clic en **Siguiente**.
Exportar formato de archivo	Haga clic en **Siguiente**.
Nombre de archivo	Haga clic en **Examinar** y especifique la ruta del archivo para guardar el certificado, y haga clic en **Siguiente**.
Finalización del Asistente para exportación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la exportación.

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

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

Para usar el certificado de CA de servidor de SnapCenter exportado, es necesario importar el certificado relacionado a los hosts del plugin de Windows de SnapCenter mediante la consola de gestión de Microsoft (MMC).

- Pasos*
  1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
  2. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
  3. En la ventana Certificados Snap-in, seleccione la opción **Cuenta de computadora** y luego haga clic en **Finalizar**.
  4. Haga clic en **Console root** > **Certificados - Equipo local** > **Personal** > **Certificados**.
  5. Haga clic con el botón derecho en la carpeta “Personal” y seleccione **Todas las tareas** > **Importar** para iniciar el asistente de importación.
  6. Realice las siguientes acciones en el asistente.

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

Importe el certificado de CA en los hosts del plugin UNIX

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

Acerca de esta tarea

- Puede gestionar la contraseña del almacén de claves del SPL y el alias de la pareja de claves firmada de CA en uso.
- La contraseña para el almacén de claves SPL y para toda la contraseña de alias asociada de la clave privada deben ser la misma.
- Pasos*
  1. Puede recuperar la contraseña predeterminada del almacén de claves del SPL desde el archivo de propiedades del SPL. Es el valor correspondiente a la clave `SPL_KEYSTORE_PASS`.
  2. Cambie la contraseña del almacén de claves: `$ keytool -storepasswd -keystore keystore.jks`
  3. Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. Actualice lo mismo para la clave spl_KEYSTORE_PASS IN `spl.properties` archivo.
  5. Reinicie el servicio después de cambiar la contraseña.

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

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

- Pasos*
  1. Desplácese hasta la carpeta que contiene el almacén de claves de SPL: `/var/opt/snapcenter/spl/etc`.
  2. Busque el archivo `keystore.jks`.
  3. Enumere los certificados añadidos al almacén de claves: `$ keytool -list -v -keystore keystore.jks`
  4. Añada un certificado raíz o intermedio: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
  5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza de SPL.

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

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

- Pasos*
  1. Navegue a la carpeta que contiene el almacén de claves del SPL `/var/opt/snapcenter/spl/etc`.
  2. Busque el archivo `keystore.jks`.

3. Enumere los certificados añadidos al almacén de claves: `$ keytool -list -v -keystore keystore.jks`
4. Agregue el certificado de CA con clave pública y privada. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Enumere los certificados añadidos al almacén de claves. `$ keytool -list -v -keystore keystore.jks`
6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

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

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

1. Si el nombre del alias del certificado de CA es largo y contiene espacio o caracteres especiales ("*",","), cambie el nombre del alias por un nombre simple: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. Configure el nombre de alias desde el almacén de claves ubicado en `spl.properties` archivo. Actualice este valor contra la clave SPL_CERTIFICATE_ALIAS.
3. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza SPL.

Exportar certificados SnapCenter

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

- Pasos*

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

En esta ventana del asistente…	Haga lo siguiente…
Exportar clave privada	Seleccione la opción **Sí, exporte la clave privada** y, a continuación, haga clic en **Siguiente**.
Exportar formato de archivo	No realice cambios; haga clic en **Siguiente**.
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**.
Archivo a exportar	Especifique un nombre de archivo para el certificado exportado (debe utilizar .pfx) y, a continuación, haga clic en **Siguiente**.
Finalización del Asistente para exportación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la exportación.

Configurar certificado de CA para el host de Windows

Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

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

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

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

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

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

Importar certificados de CA

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

Pasos

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

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

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

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

Obtenga la huella digital del certificado de CA

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

Pasos

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

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

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

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie la huella digital.

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

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

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

Pasos

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

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

   Por ejemplo:

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

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por ejemplo:

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

Configurar el certificado de CA con el sitio SnapCenter

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

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

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

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

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

Habilite los certificados de CA para SnapCenter

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

Antes de empezar

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

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

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

3. Haga clic en **aplicar**.

Después de terminar

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

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

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

Configurar certificado de CA para el host Linux

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

Configure el certificado nginx

Pasos

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

Configure el certificado de registro de auditoría

Pasos

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

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

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

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

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

Configurar el certificado de SnapCenter

Pasos

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

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

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

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

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

Configure y habilite la comunicación SSL bidireccional en el host Windows

Configure la comunicación SSL bidireccional en el host de Windows

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

Antes de empezar

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

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

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

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

Pasos

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

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

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

Por ejemplo:

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

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

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

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

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

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

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

Por ejemplo:

```
> $cert = "abc123abc123abc123abc123"

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

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

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

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

> netsh http show sslcert ipport=0.0.0.0:8146

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

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

e. Seleccione el certificado SnapCenter.

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

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

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

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

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

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

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

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

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

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

Antes de empezar

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

Pasos

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

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

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

      Por ejemplo:

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

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

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

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

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

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

Por ejemplo:

```
> $cert = "abc123abc123abc123abc123"

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

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

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

Habilite la comunicación SSL bidireccional en el host Windows

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

Antes de empezar

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

- Pasos*

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

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

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

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

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

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

Desactive la comunicación SSL bidireccional

Puede deshabilitar la comunicación SSL bidireccional mediante comandos de PowerShell.

Acerca de esta tarea

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

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

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

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

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

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

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

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

Configure y habilite la comunicación SSL bidireccional en el host Linux

Configure la comunicación SSL bidireccional en el host Linux

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

Antes de empezar

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

Pasos

1. Copie **certificate.pem** a */etc/pki/ca-trust/source/anchors/*.
2. Añada los certificados en la lista de confianza del host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Compruebe si los certificados se han agregado a la lista de confianza. `trust list | grep "<CN of your certificate>"`

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

```
localhost:8145 -brief
```

Active la comunicación SSL en el host Linux

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

Paso

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

Configure Active Directory, LDAP y LDAPS

Registrar dominios de Active Directory que no son de confianza

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

Antes de empezar

Protocolo LDAP y LDAPS

- Puede registrar los dominios de directorio activo que no son de confianza mediante los protocolos LDAP o LDAPS.
- Debe haber habilitado la comunicación bidireccional entre los hosts del plugin y SnapCenter Server.
- La resolución de DNS se debe configurar desde el servidor de SnapCenter a los hosts del plugin y viceversa.

Protocolo LDAP

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

  Puede registrar un dominio no confiable con el FQDN. Si el FQDN no se puede resolver desde el servidor

SnapCenter, puede registrarse con una dirección IP de una controladora de dominio y esto debe poder resolverse desde el servidor SnapCenter.

Protocolo LDAPS

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

  "Configure el certificado de cliente de CA para LDAPS"

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

Acerca de esta tarea

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

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

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

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

6. Haga clic en **Aceptar**.

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

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

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

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

Configure el certificado de cliente de CA para LDAPS

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

- Pasos*
  1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.

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

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

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