Instalar y configurar SnapCenter Server

SnapCenter software

NetApp
November 06, 2025

Tabla de contenidos

Instalar y configurar SnapCenter Server

Prepárese para instalar el servidor SnapCenter

Requisitos para instalar SnapCenter Server

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

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

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

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

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

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

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

Requisitos de espacio y tamaño

Debe estar familiarizado con los requisitos de espacio y tamaño.

Artículo	Requisitos del host de Windows	Requisitos del host Linux
Sistemas operativos	Microsoft Windows Solo se admiten las versiones en inglés, alemán, japonés y chino simplificado de los sistemas operativos. Para obtener la información más reciente sobre las versiones compatibles, consultehttps://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["Herramienta de matriz de interoperabilidad de NetApp"^] .	• Red Hat Enterprise Linux (RHEL) 8 y 9 • Servidor empresarial SUSE Linux (SLES) 15 Para obtener la información más reciente sobre las versiones compatibles, consultehttps://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["Herramienta de matriz de interoperabilidad de NetApp"^] .

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

Artículo	Requisitos del host de Windows	Requisitos del host Linux
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell 7.4.2 o posterior Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conectividad a Internet" .	• .NET Framework 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell 7.4.2 o posterior • Nginx es un servidor web que se puede utilizar como proxy inverso • Pam-devel PAM (Módulos de autenticación conectables) es una herramienta de seguridad del sistema que permite a los administradores del sistema establecer políticas de autenticación sin tener que volver a compilar los programas que realizan la autenticación.

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

Requisitos del host SAN

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

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

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

Requisitos del navegador

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

Requisitos del puerto

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

- Las aplicaciones no pueden compartir un puerto.

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

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

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

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

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

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

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

Regístrese para acceder al SnapCenter software

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

Antes de empezar

- Debe tener acceso a la ID de correo electrónico corporativa.
- Si usa Azure NetApp Files, debe tener el identificador de suscripción de Azure.
- Si está utilizando Amazon FSx for NetApp ONTAP, debe tener el ID del sistema de archivos de su sistema de archivos FSx para ONTAP .

Acerca de esta tarea

Su registro está sujeto a validaciones de información y puede demorar hasta un día para confirmar y actualizar la nueva cuenta del Sitio de soporte de NetApp (NSS) a acceso **completo** desde acceso **de invitado**.

Pasos

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

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

b. En el campo NÚMERO DE SERIE, ingrese el ID de suscripción de Azure si usa Azure NetApp Files o el ID del sistema de archivos si usa Amazon FSx for NetApp ONTAP.

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

Autenticación multifactor (MFA)

Administrar la autenticación multifactor (MFA)

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

Habilitar la autenticación multifactor (MFA)

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

Acerca de esta tarea

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

Antes de empezar

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

  El certificado CA es obligatorio por las siguientes razones:

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

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

Pasos

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

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

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

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

    SnapCenter ahora se refleja como una parte confiable con el nombre para mostrar proporcionado.
11. Seleccione el nombre y realice los siguientes pasos:

a. Haga clic en **Editar política de emisión de reclamaciones**.
b. Haga clic en **Agregar regla** y haga clic en **Siguiente**.
c. Especifique un nombre para la regla de reclamación.
d. Seleccione **Active Directory** como almacén de atributos.
e. Seleccione el atributo como **User-Principal-Name** y el tipo de reclamo saliente como **Name-ID**.
f. Haga clic en **Finalizar**.

12. Ejecute los siguientes comandos de PowerShell en el servidor ADFS.

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

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

13. Realice los siguientes pasos para confirmar que los metadatos se importaron correctamente.
    a. Haga clic con el botón derecho en la cuenta de confianza del usuario confiante y seleccione **Propiedades**.
    b. Asegúrese de que los campos Puntos finales, Identificadores y Firma estén completos.
14. Cierre todas las pestañas del navegador y vuelva a abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

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

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

Actualizar metadatos de MFA de AD FS

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

Pasos

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

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

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

Actualizar metadatos de MFA de SnapCenter

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

Pasos

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

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

   c. Habilitar la autenticación multifactor (MFA).

      Ver "Habilitar la autenticación multifactor" .
2. Cierre todas las pestañas del navegador y vuelva a abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Deshabilitar la autenticación multifactor (MFA)

Pasos

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

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

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

Configurar AD FS como OAuth/OIDC

Configurar AD FS mediante el asistente de GUI de Windows

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

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

4. Seleccione **Generar secreto compartido**.

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

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

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

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

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

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

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

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

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

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

16. Abra la herramienta **Administración de AD FS** ubicada en el menú **Herramientas** en la parte superior derecha del Administrador del servidor.
    a. Seleccione la carpeta **Grupos de aplicaciones** en la barra lateral izquierda.
    b. Seleccione la API web y haga clic en **EDITAR**.
    c. Ir a la pestaña Reglas de transformación de emisión
17. Haga clic en **Agregar regla**.
    a. Seleccione **Enviar atributos LDAP como reclamos** en el menú desplegable Plantilla de regla de reclamo.
    b. Haga clic en **Siguiente**.
18. Introduzca el nombre de la **regla de reclamación**.
    a. Seleccione **Active Directory** en el menú desplegable Almacén de atributos.
    b. Seleccione **Nombre principal del usuario** en el menú desplegable **Atributo LDAP** y **UPN** en el menú desplegable **Tipo de reclamación saliente**.
    c. Haga clic en **Finalizar**.

Crear un grupo de aplicaciones mediante comandos de PowerShell

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

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

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

   `ClientRoleIdentifier`nombre de su grupo de aplicaciones

   `redirectURL`URL válida para redirección después de la autorización

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

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

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

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

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

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

4. Obtenga el ID del cliente y el secreto del cliente de la salida de los siguientes comandos porque solo se muestran una vez.

   ```
   "client_id = $identifier"

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

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

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

   $transformrule = @"

   @RuleTemplate = "LdapClaims"

   @RuleName = "AD User properties and Groups"

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

   "AD AUTHORITY"]
   ```

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

"@
```

6. Escriba el archivo de reglas de transformación.

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

7. Nombre la aplicación de API web y defina sus reglas de transformación de emisión utilizando un archivo externo.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Actualizar el tiempo de expiración del token de acceso

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

Acerca de esta tarea

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

Paso

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

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

Obtener el token portador de AD FS

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

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

Campo	Valor
Tipo de subvención	Código de autorización

URL de devolución de llamada	Ingrese la URL base de su aplicación si no tiene una URL de devolución de llamada.
URL de autorización	[nombre-de-dominio-adfs]/adfs/oauth2/authorize
URL del token de acceso	[nombre-de-dominio-adfs]/adfs/oauth2/token
ID de cliente	Introduzca el ID del cliente de AD FS
Secreto del cliente	Ingrese el secreto del cliente de AD FS
Alcance	OpenID
Autenticación del cliente	Enviar como encabezado de autenticación básico
Recurso	En la pestaña **Opciones avanzadas**, agregue el campo Recurso con el mismo valor que la URL de devolución de llamada, que viene como un valor “aud” en el token JWT.

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

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

Autenticación CLI de MFA de SnapCenter

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

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

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

Autenticación de API Rest de MFA de SnapCenter

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

Flujo de trabajo de la API Rest de MFA

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

Acerca de esta tarea

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

para realizar cualquier operación.

Pasos

Para autenticarse a través de AD FS MFA

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

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

   + Los nombres de usuario deben tener el formato usuario@dominio o dominio\usuario.

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

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

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

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

8. Utilizando el nombre de usuario y el nombre del rol, SnapCenter autentica al usuario para una ejecución de API.

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

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

GUI

Pasos

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

Interfaz de PowerShell

Pasos

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

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

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

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

2. Verifique el estado y la configuración de MFA mediante el `Get-SmMultiFactorAuthentication` cmdlet.

Interfaz SCCLI

Pasos

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

API REST

1. Ejecute la siguiente API de publicación para habilitar MFA para GUI, API Rest, PowerShell y SCCLI.

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

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

Parámetro	Valor

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

Instalar el servidor SnapCenter

Instalar el servidor SnapCenter en el host de Windows

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

Opcionalmente, puede realizar varios procedimientos de instalación y configuración mediante cmdlets de PowerShell. Debe utilizar PowerShell 7.4.2 o posterior.

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

Antes de empezar

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

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

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

Pasos

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

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

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

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

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

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

4. Haga clic en **Instalar ahora**.

   Si ha especificado algún valor que no es válido, se mostrarán los mensajes de error correspondientes. Debe volver a ingresar los valores y luego iniciar la instalación.

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

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

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

Funciones habilitadas en el host de Windows durante la instalación

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

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

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

Instalar el servidor SnapCenter en el host Linux

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

Antes de empezar

- Si desea instalar SnapCenter Server utilizando un usuario que no sea root y que no tenga privilegios suficientes para instalar SnapCenter, obtenga el archivo de suma de comprobación de sudoers del sitio de soporte de NetApp . Debe utilizar el archivo de suma de comprobación apropiado según la versión de Linux.
- Si el paquete sudo no está disponible en SUSE Linux, instálelo para evitar errores de autenticación.
- Para SUSE Linux, configure el nombre de host para evitar errores de instalación.
- Compruebe el estado seguro de Linux ejecutando el comando `sestatus` . Si el *estado de SELinux* está "habilitado" y el *modo actual* está "aplicando", realice lo siguiente:
  - Ejecute el comando: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

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

    El valor predeterminado de *WEBAPP_EXTERNAL_PORT* es 8146
  - Ejecute los siguientes comandos desde el directorio donde tiene permiso de lectura y escritura:

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

          Si el comando devuelve "no hay nada que hacer", vuelva a ejecutarlo después de instalar SnapCenter Server.

        - Si el comando crea *my-nginx.pp*, ejecute el comando para activar el paquete de políticas: `sudo semodule -i my-nginx.pp`
    - La ruta utilizada para el directorio PID de MySQL es */var/opt/mysqld*. Ejecute los siguientes comandos para configurar los permisos para la instalación de MySQL.
        - `mkdir /var/opt/mysqld`
        - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
        - `sudo restorecon -Rv /var/opt/mysqld`
    - La ruta utilizada para el directorio de datos MySQL es */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Ejecute los siguientes comandos para establecer los permisos para el directorio de datos MySQL.
        - `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
        - `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
        - `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

Acerca de esta tarea

- Cuando SnapCenter Server se instala en el host Linux, se instalan servicios de terceros como MySQL, RabbitMq y Errlang. No debes desinstalarlos.
- El servidor SnapCenter instalado en el host Linux no admite:
    - Alta disponibilidad
    - complementos de Windows
    - Active Directory (solo admite usuarios locales, tanto usuarios root como no root con credenciales)
    - Autenticación basada en clave para iniciar sesión en SnapCenter
- Durante la instalación del entorno de ejecución de .NET, si la instalación no logra resolver las dependencias de la biblioteca *libicu*, instale *libicu* ejecutando el comando: `yum install -y libicu`
- Si la instalación de SnapCenter Server falla debido a la falta de disponibilidad de *Perl*, instale *Perl* ejecutando el comando: `yum install -y perl`

Pasos

1. Descargue lo siguiente desde "Sitio de soporte de NetApp" al directorio */home*.
    - Paquete de instalación de SnapCenter Server: **snapcenter-linux-server-(el8/el9/sles15).bin**
    - Archivo de clave pública - **snapcenter_public_key.pub**
    - Archivo de firma respectivo: **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. Validar el archivo de firma. `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Para la instalación por parte de usuarios no root, agregue el contenido de visudo especificado en **snapcenter_server_checksum_(el8/el9/sles15).txt** disponible junto con el instalador .bin.

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

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

Si quieres realizar…	Haz esto…
Instalación no interactiva	`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 pasar para instalar SnapCenter Server: • DWEBAPP_EXTERNAL_PORT: Puerto externo de la aplicación web que se utiliza para acceder a SnapCenter Server fuera del host Linux. El valor predeterminado es 8146. • DWEBAPP_INTERNAL_PORT: Puerto interno de la aplicación web que se utiliza para acceder a SnapCenter Server dentro del host Linux. El valor predeterminado es 8147. • DSMCORE_PORT: puerto SMCore en el que se ejecutan los servicios Smcore. El valor predeterminado es 8145. • DSCHEDULER_PORT: Puerto del programador en el que se ejecutan los servicios del programador. El valor predeterminado es 8154. • DSNAPCENTER_SERVER_USER: Usuario de SnapCenter Server que instalará SnapCenter Server. Para *DSNAPCENTER_SERVER_USER*, el valor predeterminado es el usuario que ejecuta el instalador. • 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

¿Que sigue?

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

predeterminado.

- DSELINUX: Si el *estado SELinux* está "habilitado", el *modo actual* está "aplicando" y ha ejecutado los comandos mencionados en la sección Antes de comenzar, debe especificar este parámetro y asignar el valor como 1. El valor predeterminado es 0.
- DUPGRADE: El valor predeterminado es 0. Especifique este parámetro y su valor como cualquier entero distinto de 0 para actualizar el servidor SnapCenter .

Funciones habilitadas en el host Linux durante la instalación

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

- Rabbitmq
- Erlang

Registrarse en SnapCenter

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

Pasos

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

Inicie sesión en SnapCenter mediante la autorización RBAC

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

Antes de empezar

- Debe habilitar el Servicio de activación de procesos de Windows (WAS) en el Administrador de servidor de Windows.
- Si desea utilizar Internet Explorer como navegador para iniciar sesión en el servidor SnapCenter , debe asegurarse de que el Modo protegido en Internet Explorer esté deshabilitado.
- Si SnapCenter Server está instalado en un host Linux, debe iniciar sesión con la cuenta de usuario que se utilizó para instalar SnapCenter Server.

Acerca de esta tarea

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

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

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

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

Para una implementación de alta disponibilidad (HA), debe acceder a SnapCenter mediante la IP del clúster virtual *https://Virtual_Cluster_IP_or_FQDN:8146*. Si no ve la interfaz de usuario de SnapCenter cuando navega a *https://Virtual_Cluster_IP_or_FQDN:8146* en Internet Explorer (IE), debe agregar la dirección IP o el FQDN del clúster virtual como un sitio confiable en IE en cada host de complemento, o debe deshabilitar la seguridad mejorada de IE en cada host de complemento. Para obtener más información, consulte "No se puede acceder a la dirección IP del clúster desde la red externa" .

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

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

Pasos

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

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

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

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

Resultado

Se muestra la página del Panel de Control.

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

Después de terminar

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

Si tiene dominios de Active Directory que no son de confianza y desea que SnapCenter admita, debe registrar esos dominios con SnapCenter antes de configurar los roles para los usuarios en dominios que no son de confianza. "Más información" .

Si desea agregar el host del complemento en SnapCenter ejecutándose en el host Linux, debe obtener el archivo de suma de comprobación de la ubicación: */opt/ NetApp/snapcenter/SnapManagerWeb/Repository*.

A partir de la versión 6.0, se crea un acceso directo para SnapCenter PowerShell en el escritorio. Puede acceder directamente a los cmdlets de PowerShell de SnapCenter mediante el acceso directo.

Inicie sesión en SnapCenter mediante la autenticación multifactor (MFA)

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

Antes de empezar

Deberías haber habilitado MFA. Para obtener información sobre cómo habilitar MFA, consulte"Habilitar la autenticación multifactor"

Acerca de esta tarea

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

Pasos

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

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

   - Si el nombre de usuario o la contraseña son válidos

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

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

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

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

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

Pasos

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

Proteja el servidor web de SnapCenter deshabilitando SSL 3.0

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

Existen fallas en el protocolo SSL 3.0 que un atacante puede utilizar para provocar fallas de conexión o realizar ataques de intermediario y observar el tráfico de cifrado entre su sitio web y sus visitantes.

Pasos

1. Para iniciar el Editor del Registro en el host del servidor web de SnapCenter , haga clic en **Inicio** > **Ejecutar** y luego ingrese regedit.
2. En el Editor del Registro, navegue a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Si la clave del servidor ya existe:
     i. Seleccione el DWORD habilitado y luego haga clic en **Editar** > **Modificar**.
     ii. Cambie el valor a 0 y luego haga clic en **Aceptar**.

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

3. Cerrar el Editor del Registro.

Configurar el servidor SnapCenter

Agregar y aprovisionar el sistema de almacenamiento

Añadir sistemas de almacenamiento

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

Puede agregar un SVM independiente o un clúster compuesto por varios SVM. Si está utilizando Amazon FSx for NetApp ONTAP, puede agregar un LIF de administrador de FSx que comprenda múltiples SVM mediante la cuenta fsxadmin o agregar FSx SVM en SnapCenter.

Antes de empezar

- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que las instalaciones del complemento no estén en curso.

  Las instalaciones de complementos de host no deben estar en progreso mientras se agrega una conexión al sistema de almacenamiento porque es posible que la memoria caché del host no se actualice y el estado de las bases de datos puede mostrarse en la GUI de SnapCenter como “No disponible para respaldo” o "`No en almacenamiento de NetApp ".

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

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

Acerca de esta tarea

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

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

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

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

Pasos

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

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

Para este campo…	Haz esto…
Nombre de usuario/Contraseña	Ingrese las credenciales del usuario de almacenamiento que tiene los privilegios necesarios para acceder al sistema de almacenamiento.
Configuración del sistema de gestión de eventos (EMS) y AutoSupport	Si desea enviar mensajes EMS al syslog del sistema de almacenamiento o si desea que se envíen mensajes de AutoSupport al sistema de almacenamiento para protección aplicada, operaciones de restauración completadas u operaciones fallidas, seleccione la casilla de verificación correspondiente. Cuando selecciona la casilla de verificación **Enviar notificación de AutoSupport para operaciones fallidas al sistema de almacenamiento**, la casilla de verificación **Registrar eventos del servidor SnapCenter en syslog** también se selecciona porque se requieren mensajes EMS para habilitar las notificaciones de AutoSupport .

4. Haga clic en **Más opciones** si desea modificar los valores predeterminados asignados a la plataforma, el protocolo, el puerto y el tiempo de espera.

   a. En Plataforma, seleccione una de las opciones de la lista desplegable.

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

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

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

      El puerto predeterminado 443 normalmente funciona.

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

      El valor predeterminado es 60 segundos.

   d. Si el SVM tiene múltiples interfaces de administración, seleccione la casilla de verificación **IP preferida** y luego ingrese la dirección IP preferida para las conexiones SVM.
   e. Haga clic en **Guardar**.
5. Haga clic en **Enviar**.

Resultado

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

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

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

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

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

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

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

Después de terminar

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

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

El administrador de la máquina virtual de almacenamiento (SVM) no tiene acceso a AutoSupport.

Conexiones de almacenamiento y credenciales

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

Conexiones de almacenamiento

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

Cartas credenciales

- Administrador del dominio o cualquier miembro del grupo de administradores

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

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

- *Nombre de usuario@upn*

- Administrador local (sólo para grupos de trabajo)

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

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

- Credenciales para grupos de recursos individuales

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

Aprovisionar almacenamiento en hosts de Windows

Crear y administrar igroups

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

Crear un igroup

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

Pasos

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

En este campo…	Haz esto…
Sistema de almacenamiento	Seleccione la SVM para el LUN que asignará al igroup.
Host	Seleccione el host en el que desea crear el igroup.
Nombre del igroup	Introduzca el nombre del igroup.
Iniciadores	Seleccione el iniciador.
Tipo	Seleccione el tipo de iniciador, iSCSI, FCP o mixto (FCP e iSCSI).

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

   SnapCenter crea el igroup en el sistema de almacenamiento.

Cambiar el nombre de un igroup

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

Pasos

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

Modificar un igroup

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

Pasos

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

Eliminar un igroup

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

Pasos

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

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

   SnapCenter elimina el igroup.

Crear y administrar discos

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

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

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

Ver los discos en un host

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

Pasos

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

   Se enumeran los discos.

Ver discos agrupados

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

Pasos

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

   Se enumeran los discos.

Establecer una sesión iSCSI

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Sesión iSCSI**.
3. En la lista desplegable **Máquina virtual de almacenamiento**, seleccione la máquina virtual de almacenamiento (SVM) para el destino iSCSI.
4. En la lista desplegable **Host**, seleccione el host para la sesión.
5. Haga clic en **Establecer sesión**.

   Se muestra el asistente para establecer sesión.

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

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

7. Cuando esté satisfecho con sus entradas, haga clic en **Conectar**.

   SnapCenter establece la sesión iSCSI.

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

Crear LUN o discos conectados mediante FC o iSCSI

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

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

Antes de empezar

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

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

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

- Debe haber iniciado el servicio FC o iSCSI en el sistema de almacenamiento.
- Si está utilizando iSCSI, debe haber establecido una sesión iSCSI con el sistema de almacenamiento.
- El paquete de complementos de SnapCenter para Windows debe instalarse únicamente en el host en el que está creando el disco.

Acerca de esta tarea

- No se puede conectar un LUN a más de un host a menos que el LUN se comparta entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.
- Si un LUN es compartido por hosts en un clúster de conmutación por error de Windows Server que usa CSV (volúmenes compartidos de clúster), debe crear el disco en el host que posee el grupo de clústeres.

Pasos

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

   Se abre el asistente para crear disco.

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

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

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

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

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

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

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

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

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

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

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

Seleccionar…	Si…
Crear un nuevo igroup para los iniciadores seleccionados	Desea crear un nuevo igroup para los iniciadores seleccionados.
Elija un igroup existente o especifique un nuevo igroup para los iniciadores seleccionados	Desea especificar un igroup existente para los iniciadores seleccionados o crear un nuevo igroup con el nombre que especifique. Escriba el nombre del igroup en el campo **nombre del igroup**. Escriba las primeras letras del nombre del igroup existente para completar automáticamente el campo.

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

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

Cambiar el tamaño de un disco

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

Acerca de esta tarea

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

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

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

Pasos

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

   Se enumeran los discos.

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

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

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

   SnapCenter cambia el tamaño del disco.

Conectar un disco

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

Antes de empezar

- Debe haber iniciado el servicio FC o iSCSI en el sistema de almacenamiento.
- Si está utilizando iSCSI, debe haber establecido una sesión iSCSI con el sistema de almacenamiento.
- No se puede conectar un LUN a más de un host a menos que el LUN se comparta entre los hosts de un clúster de conmutación al nodo de respaldo de Windows Server.
- Si el LUN es compartido por hosts en un clúster de conmutación por error de Windows Server que usa CSV (volúmenes compartidos de clúster), entonces debe conectar el disco en el host que posee el grupo de clústeres.
- El complemento para Windows debe instalarse únicamente en el host en el que está conectando el disco.

Pasos

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

3. Seleccione el host de la lista desplegable **Host**.
4. Haga clic en **Conectar**.

   Se abre el asistente Conectar disco.

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

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

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

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

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

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

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

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

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

Seleccionar…	Si…
Crear un nuevo igroup para los iniciadores seleccionados	Desea crear un nuevo igroup para los iniciadores seleccionados.
Elija un igroup existente o especifique un nuevo igroup para los iniciadores seleccionados	Desea especificar un igroup existente para los iniciadores seleccionados o crear un nuevo igroup con el nombre que especifique. Escriba el nombre del igroup en el campo **nombre del igroup**. Escriba las primeras letras del nombre del igroup existente para completar el campo automáticamente.

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

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

Desconectar un disco

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

Antes de empezar

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

Acerca de esta tarea

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

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

Pasos

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

   Se enumeran los discos.

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

SnapCenter desconecta el disco.

Eliminar un disco

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

Pasos

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

   Se enumeran los discos.

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

   SnapCenter elimina el disco.

Crear y administrar recursos compartidos SMB

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

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

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

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

Crear un recurso compartido SMB

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

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

Pasos

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

Se abre el cuadro de diálogo Nuevo recurso compartido.

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

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

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

   SnapCenter crea el recurso compartido SMB en la SVM.

Eliminar un recurso compartido SMB

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

Pasos

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

   SnapCenter elimina el recurso compartido SMB del SVM.

Recuperar espacio en el sistema de almacenamiento

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

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

Antes de empezar

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

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

Acerca de esta tarea

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

  Hacerlo puede ralentizar el proceso de recuperación.

Paso

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

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

drive_path es la ruta de la unidad asignada al LUN.

Aprovisionamiento de almacenamiento mediante cmdlets de PowerShell

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

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

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

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

Aprovisionamiento de almacenamiento en entornos VMware

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

Plataformas de sistema operativo invitado VMware compatibles

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

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

- LUN de RDM

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

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

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

Limitaciones relacionadas con el servidor VMware ESXi

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

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

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

Privilegios mínimos de vCenter necesarios para las operaciones de SnapCenter RDM

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

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

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

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

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

Administrar LUN FC RDM en un clúster de Microsoft

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

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

Requisitos

El complemento para Windows proporciona soporte para clústeres de Microsoft que utilizan LUN FC RDM en dos máquinas virtuales diferentes que pertenecen a dos servidores ESX o ESXi diferentes, también conocidos como clúster entre cuadros, cuando cumple con requisitos de configuración específicos.

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

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

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

  No se pueden utilizar discos virtuales para almacenamiento compartido.

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

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

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

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

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

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

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

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

Limitaciones

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

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

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

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

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

Crear un LUN FC RDM compartido

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

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

Agregar licencias basadas en controlador de SnapCenter Standard

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

La licencia basada en controlador tiene las siguientes características:

- El derecho a SnapCenter Standard está incluido con la compra de Premium o Flash Bundle (no con el paquete básico)
- Uso de almacenamiento ilimitado
- Se agrega directamente al controlador de almacenamiento FAS, AFF o ASA mediante el Administrador del sistema ONTAP o la CLI de ONTAP .

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

- Bloqueado al número de serie del controlador

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

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

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

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

Pasos

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

     Cuando selecciona el nombre del clúster, todas las SVM que forman parte del clúster se muestran en la sección Máquinas virtuales de almacenamiento.
3. En la lista Conexiones de almacenamiento, busque la columna Licencia del controlador.

   La columna Licencia del controlador muestra el siguiente estado:

   - Indica que hay una licencia de SnapManager Suite instalada en un sistema de almacenamiento primario FAS, AFF o ASA .
   - Indica que no hay una licencia de SnapManager Suite instalada en un sistema de almacenamiento primario FAS, AFF o ASA .
   - No aplicable indica que una licencia de SnapManager Suite no es aplicable porque el controlador de almacenamiento está en Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select o plataformas de almacenamiento secundarias.

Paso 2: Identificar las licencias instaladas en el controlador

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

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

Pasos

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

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

Ejemplo de salida

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

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

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

En el ejemplo, la licencia de SnapManagerSuite está instalada, por lo tanto, no se requiere ninguna acción de licencia adicional de SnapCenter .

Paso 3: Recupere el número de serie del controlador

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

Pasos

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

Ejemplo de salida

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: 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 controlador

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

Antes de empezar

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

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

- Debes tener el número de serie del controlador.

Pasos

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

   Se muestra una lista de licencias para el controlador especificado.

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

Paso 5: Agregar licencia basada en controlador

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

Antes de empezar

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

Acerca de esta tarea

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

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

Pasos

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

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

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

3. Verifique que la licencia de SnapManagerSuite esté instalada:

   ```
   license show
   ```

Paso 6: Eliminar la licencia de prueba

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

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

Pasos

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

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

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

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

Configurar alta disponibilidad

Configurar servidores SnapCenter para alta disponibilidad

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

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

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

Configurar la alta disponibilidad mediante F5

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

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

- Agregar SmServerCluster
- Agregar servidor Sm
- Eliminar SmServerCluster

  Para más información, consulte "Guía de referencia de cmdlets del software SnapCenter" .

Información adicional

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

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

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

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

Configurar alta disponibilidad usando AWS Elastic Load Balancing (ELB)

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

Pasos

1. Configurar la IP superpuesta privada virtual en AWS. Para obtener más información, consulte "Configurar la IP superpuesta privada virtual" .

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

Configurar la alta disponibilidad mediante el equilibrador de carga de Azure

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

Pasos

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

== Cambiar de NLB a F5 para alta disponibilidad

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

Pasos

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

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

Alta disponibilidad para el repositorio MySQL de SnapCenter

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

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

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

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

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

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

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

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

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

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

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

Configurar el control de acceso basado en roles (RBAC)

Crear un rol

Además de utilizar los roles existentes de SnapCenter , puede crear sus propios roles y personalizar los permisos.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Roles**.
3. Hacer clic .
4. Especifique un nombre y una descripción para el nuevo rol.

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

5. Seleccione **Todos los miembros de este rol pueden ver los objetos de otros miembros** para permitir que otros miembros del rol vean recursos como volúmenes y hosts después de actualizar la lista de recursos.

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

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

6. En la página Permisos, seleccione los permisos que desea asignar al rol o haga clic en **Seleccionar todo** para otorgar todos los permisos al rol.
7. Haga clic en **Enviar**.

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

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

Antes de empezar

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

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

  Siempre debes asignar primero los privilegios de acceso total.

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

Acerca de esta tarea

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

Esta herramienta maneja automáticamente la configuración correcta de los privilegios de ONTAP . Por ejemplo, la herramienta RBAC User Creator para NetApp ONTAP agrega automáticamente los privilegios en el orden correcto para que los privilegios de acceso total aparezcan primero. Si agrega primero los privilegios de solo lectura y luego agrega los privilegios de acceso total, ONTAP marca los privilegios de acceso total como duplicados y los ignora.

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

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

Pasos

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

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

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

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

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

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

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

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

3. Asigne el rol al usuario ingresando el siguiente comando:

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

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

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

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

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

Crear roles SVM con privilegios mínimos

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

Pasos

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

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

   Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

Comandos CLI de ONTAP para crear roles SVM y asignar permisos

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

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

"lun igroup add" -access all

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

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

"volume qtree modify" -access all

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

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

Crear roles SVM para sistemas ASA r2

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

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

Pasos

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

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

   Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

Comandos CLI de ONTAP para crear roles SVM y asignar permisos

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

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

"lun igroup delete" -access all

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

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

"volume restrict" -access all

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

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

"volume delete" -access all

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

Crear roles de clúster de ONTAP con privilegios mínimos

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

Pasos

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

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

   Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

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

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

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

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

"lun offline" -access all

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

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

"system node modify" -access all

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

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

"vserver cifs show" -access all

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

Crear roles de clúster ONTAP para sistemas ASA r2

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

Pasos

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

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

   Debes repetir este comando para cada permiso.

2. Crea un usuario y asígnale el rol.

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

3. Desbloquear al usuario.

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

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

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

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

"lun igroup rename" -access all

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

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

"snapmirror show" -access all

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

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

"vserver" -access all

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

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

Agregar un usuario o grupo y asignarle roles y activos

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

Antes de empezar

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

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

- SnapCenter incluye varios roles predefinidos.

  Puede asignar estos roles al usuario o crear roles nuevos.

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

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

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

Operación	Cesión de activos
Proteger los recursos	anfitrión, política
Respaldo	host, grupo de recursos, política

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

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

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

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

  Debe agregar activos antes de asignar acceso a los usuarios.

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

Pasos

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

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

4. Haga clic en **Asignar** y, a continuación, en la página Asignar activos:
   a. Seleccione el tipo de activo de la lista desplegable **Activo**.
   b. En la tabla Activos, seleccione el activo.

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

c. Repita este procedimiento para todos los activos necesarios.

d. Haga clic en **Guardar**.

5. Haga clic en **Enviar**.

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

Configurar los ajustes del registro de auditoría

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

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

Deberías haber iniciado sesión como rol "SnapCenterAdmin".

Acerca de esta tarea

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

  No se admiten unidades compartidas o montadas en red.

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

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

Pasos

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

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

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

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

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

Configurar conexiones MySQL seguras con SnapCenter Server

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

Configurar conexiones MySQL seguras para configuraciones independientes de SnapCenter Server

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

Se generan los siguientes certificados:

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

Pasos

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

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

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

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

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

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

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

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

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

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

   El siguiente ejemplo muestra los certificados y archivos de clave copiados en la sección [mysqld] del archivo my.ini en la carpeta predeterminada `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Inicie la aplicación web SnapCenter Server en IIS.

Configurar conexiones MySQL seguras para configuraciones de alta disponibilidad

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

Se generan los siguientes certificados:

- Certificado CA

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

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

Pasos

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

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

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

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

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

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

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

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

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

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

   El siguiente ejemplo muestra los certificados y los archivos de clave copiados en la sección [mysqld] del archivo my.ini en la carpeta predeterminada C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data.

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

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

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

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

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

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

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

4. Para el segundo nodo HA, copie el certificado de CA y genere el certificado público del servidor, los archivos de clave privada del servidor, el certificado público del cliente y los archivos de clave privada del cliente. Realice los siguientes pasos:

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

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

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

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

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

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

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

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

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

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

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

El siguiente ejemplo muestra los certificados y los archivos de clave copiados en la sección [mysqld] del archivo my.ini en la carpeta predeterminada C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data.

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

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

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

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

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

+

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

+

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

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

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

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

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

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

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

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

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

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

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

Configurar la autenticación basada en certificados

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

Habilitar la autenticación basada en certificados

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

- Para habilitar la autenticación basada en certificado de cliente:

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

- Para deshabilitar la autenticación basada en certificado de cliente:

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

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

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

Antes de empezar

Deberías haber configurado el SSL bidireccional.

Pasos

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

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

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

Importar certificado de CA a los hosts del complemento de Windows

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

Pasos

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

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

Importar certificado CA a los hosts del complemento UNIX

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

Acerca de esta tarea

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

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves SPL desde el archivo de propiedades SPL. Es el valor correspondiente a la clave `SPL_KEYSTORE_PASS` .
2. Cambiar la contraseña del almacén de claves: `$ keytool -storepasswd -keystore keystore.jks`
3. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Actualice lo mismo para la clave SPL_KEYSTORE_PASS en `spl.properties` archivo.
5. Reinicie el servicio después de cambiar la contraseña.

Configurar certificados raíz o intermedios para el almacén de confianza SPL

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

Pasos

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

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

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del SPL `/var/opt/snapcenter/spl/etc` .
2. Localizar el archivo `keystore.jks` ` .
3. Enumere los certificados agregados en el almacén de claves: `$ keytool -list -v -keystore keystore.jks`
4. Agregue el certificado CA que tenga clave privada y pública. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Enumere los certificados agregados en el almacén de claves. `$ keytool -list -v -keystore keystore.jks`
6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. Cambie la contraseña de clave privada agregada para el certificado de CA a la contraseña del almacén de claves.

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

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

8. Si el nombre de alias en el certificado de CA es largo y contiene espacios o caracteres especiales ("*",","), cambie el nombre de alias a un nombre simple: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks` `
9. Configure el nombre de alias del almacén de claves ubicado en `spl.properties` archivo. Actualice este

valor con la clave SPL_CERTIFICATE_ALIAS.

10. Reinicie el servicio después de configurar el par de claves firmadas por CA en el almacén de confianza SPL.

Exportar certificados de SnapCenter

Debe exportar los certificados de SnapCenter en formato .pfx.

Pasos

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

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

Configurar el certificado CA para el host de Windows

Generar archivo CSR de certificado de CA

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

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

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

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

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

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

Importar certificados de CA

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

Pasos

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

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

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

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

Obtenga la huella digital del certificado CA

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

Pasos

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

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

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

      Get-ChildItem -Path Certificado:\LocalMachine\Mi

   b. Copiar la huella digital.

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

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

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

Pasos

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

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

   Por ejemplo:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Vincule el certificado recién instalado con los servicios del
complemento de host de Windows, ejecutando los siguientes comandos:
```

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

Por ejemplo:

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

Configurar el certificado de CA con el sitio de SnapCenter

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

Pasos

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

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

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

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

Habilitar certificados CA para SnapCenter

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

Antes de empezar

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

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

Pasos

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

Después de terminar

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

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

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

Configurar el certificado CA para el host Linux

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

Configurar el certificado nginx

Pasos

1. Vaya a */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`

2. Abra **snapcenter.conf** usando vi o cualquier editor de texto.
3. Navegue a la sección del servidor en el archivo de configuración.
4. Modifique las rutas de *ssl_certificate* y *ssl_certificate_key* para que apunten al certificado de CA.
5. Guarde y cierre el archivo.
6. Recargar nginx: `$nginx -s reload`

Configurar el certificado de registro de auditoría

Pasos

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

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

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

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

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

Configurar el certificado de servicios de SnapCenter

Pasos

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

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

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

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

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

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

Configurar la comunicación SSL bidireccional en el host de Windows

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

Antes de empezar

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

  Para más detalles, consulte "Sección de configuración del certificado CA."

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

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

Pasos

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

   a. Elimine el enlace del puerto del certificado autofirmado de SnapCenter existente mediante el siguiente comando de PowerShell.

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

   Por ejemplo,

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

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

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

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

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

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

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

Por ejemplo,

```
> $cert = "abc123abc123abc123abc123"

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

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

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

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

> netsh http show sslcert ipport=0.0.0.0:8146

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

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

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

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

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

Debe configurar el complemento de Windows de SnapCenter para la comunicación SSL bidireccional mediante comandos de PowerShell.

Antes de empezar

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

Pasos

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

   a. Elimine el enlace del puerto del certificado autofirmado de SnapCenter existente mediante el siguiente comando de PowerShell.

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

      Por ejemplo,

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

   b. Vincula el certificado CA recién adquirido con el puerto SMCore.

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

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

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

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

      Por ejemplo,

      ```
      > $cert = "abc123abc123abc123abc123"

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

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

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

Habilitar la comunicación SSL bidireccional en el host de Windows

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

Antes de empezar

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

Pasos

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

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

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

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

2. Realice la operación de reciclaje del grupo de aplicaciones de IIS SnapCenter mediante el siguiente comando. `> Restart-WebAppPool -Name "SnapCenter"`
3. Para los complementos de Windows, reinicie el servicio SMCore ejecutando el siguiente comando de PowerShell:

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

Deshabilitar la comunicación SSL bidireccional

Puede deshabilitar la comunicación SSL bidireccional mediante comandos de PowerShell.

Acerca de esta tarea

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

Pasos

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

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

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

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

2. Realice la operación de reciclaje del grupo de aplicaciones de IIS SnapCenter mediante el siguiente comando. `> Restart-WebAppPool -Name "SnapCenter"`
3. Para los complementos de Windows, reinicie el servicio SMCore ejecutando el siguiente comando de

PowerShell:

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

Configurar y habilitar la comunicación SSL bidireccional en el host Linux

Configurar la comunicación SSL bidireccional en el host Linux

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

Antes de empezar

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

Pasos

1. Copie **certificate.pem** a */etc/pki/ca-trust/source/anchors/*.
2. Agregue los certificados en la lista de confianza de su host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Verifique si los certificados se agregaron a la lista de confianza. `trust list | grep "<CN of your certificate>"`
4. Actualice **ssl_certificate** y **ssl_certificate_key** en el archivo **nginx** de SnapCenter y reinicie.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Actualice el enlace de la GUI del servidor SnapCenter .
6. Actualice los valores de las siguientes claves en * SnapManager.Web.UI.dll.config* ubicado en _ /<ruta de instalación>/ NetApp/snapcenter/SnapManagerWeb_ y * SMCoreServiceHost.dll.config* ubicado en */<ruta de instalación>/ NetApp/snapcenter/SMCore*.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<ruta del certificado.pfx>" />
   - <add key="CONTRASEÑA_DEL_CERTIFICADO_DE_SERVICIO" value="<contraseña>"/>
7. Reinicie los siguientes servicios.
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. Verifique que el certificado esté adjunto al puerto web de SnapManager . `openssl s_client -connect localhost:8146 -brief`
9. Verifique que el certificado esté adjunto al puerto smcore. `openssl s_client -connect localhost:8145 -brief`

10. Administrar la contraseña para el almacén de claves y alias de SPL.
    a. Recupere la contraseña predeterminada del almacén de claves SPL asignada a la clave **SPL_KEYSTORE_PASS** en el archivo de propiedades SPL.
    b. Cambiar la contraseña del almacén de claves. `keytool -storepasswd -keystore keystore.jks`
    c. Cambiar 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. Reiniciar el servicio.
11. En el host Linux del complemento, agregue los certificados raíz e intermedio en el almacén de claves del complemento SPL.
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
        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 de **certificate.pfx** almacenado en *keystore.jks* y reinicie el servicio SPL: `systemctl restart spl`
13. Verifique que el certificado esté adjunto al puerto smcore. `openssl s_client -connect localhost:8145 -brief`

Habilitar la comunicación SSL en el host Linux

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

Paso

1. Realice lo siguiente para habilitar la comunicación SSL unidireccional.
    a. Inicie sesión en la GUI de SnapCenter .
    b. Haga clic en **Configuración** > **Configuración global** y seleccione **Habilitar validación de certificado en SnapCenter Server**.
    c. Haga clic en **Hosts** > **Hosts administrados** y seleccione el host de complemento para el que desea habilitar SSL unidireccional.
    d. Hacer clic  icono y, a continuación, haga clic en **Habilitar validación de certificado**.
2. Habilite la comunicación SSL bidireccional desde el host Linux del servidor SnapCenter .

- `Open-SmConnection`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
- `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

Configurar Active Directory, LDAP y LDAPS

Registrar dominios de Active Directory que no sean de confianza

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

Antes de empezar

Protocolos LDAP y LDAPS

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

Protocolo LDAP

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

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

Protocolo LDAPS

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

  "Configurar el certificado de cliente de CA para LDAPS"

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

Acerca de esta tarea

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

Pasos

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

2. En la página de Configuración, haga clic en **Configuración global**.
3. En la página Configuración global, haga clic en **Configuración de dominio**.
4. Hacer clic + para registrar un nuevo dominio.
5. En la página Registrar nuevo dominio, seleccione **LDAP** o **LDAPS**.
   a. Si selecciona **LDAP**, especifique la información necesaria para registrar el dominio no confiable para LDAP:

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

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

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

6. Haga clic en **Aceptar**.

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

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

Pasos

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

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

Configurar el certificado de cliente de CA para LDAPS

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

Pasos

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

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

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