



# Instalar el complemento SnapCenter para Microsoft Windows

SnapCenter software

NetApp  
November 06, 2025

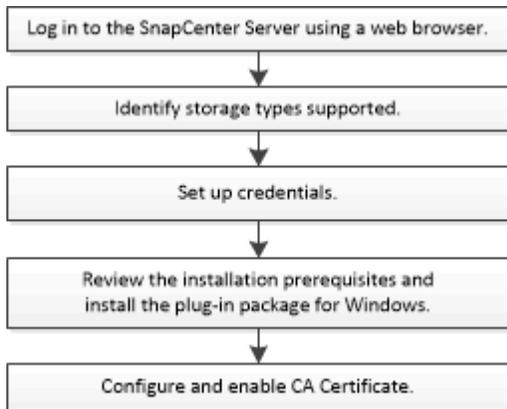
# Tabla de contenidos

- Instalar el complemento SnapCenter para Microsoft Windows . . . . . 1
  - Flujo de trabajo de instalación del complemento SnapCenter para Microsoft Windows . . . . . 1
  - Requisitos de instalación del complemento SnapCenter para Microsoft Windows . . . . . 1
    - Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows . . . . . 1
    - Configure sus credenciales para el complemento para Windows . . . . . 2
    - Configurar gMSA en Windows Server 2016 o posterior . . . . . 4
- Agregar hosts e instalar el complemento SnapCenter para Microsoft Windows . . . . . 6
- Instalar el complemento SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell . . . . . 10
- Instale el complemento SnapCenter para Microsoft Windows de forma silenciosa desde la línea de comandos . . . . . 10
- Supervisar el estado de instalación del paquete de complementos de SnapCenter . . . . . 12
- Configurar el certificado de CA . . . . . 13
  - Generar archivo CSR de certificado de CA . . . . . 13
  - Importar certificados de CA . . . . . 13
  - Obtenga la huella digital del certificado CA . . . . . 14
  - Configurar el certificado de CA con los servicios del complemento de host de Windows . . . . . 15
  - Habilitar certificados CA para complementos . . . . . 15

# Instalar el complemento SnapCenter para Microsoft Windows

## Flujo de trabajo de instalación del complemento SnapCenter para Microsoft Windows

Debe instalar y configurar el complemento SnapCenter para Microsoft Windows si desea proteger archivos de Windows que no sean archivos de base de datos.



## Requisitos de instalación del complemento SnapCenter para Microsoft Windows

Debe tener en cuenta ciertos requisitos de instalación antes de instalar el complemento para Windows.

Antes de comenzar a utilizar el complemento para Windows, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas previas requeridas.

- Debe tener privilegios de administrador de SnapCenter para instalar el complemento para Windows.

El rol de administrador de SnapCenter debe tener privilegios de administrador.

- Debe tener instalado y configurado el servidor SnapCenter .
- Al instalar un complemento en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Debe configurar SnapMirror y SnapVault si desea replicar la copia de seguridad.

## Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows

Antes de instalar el paquete de complementos de SnapCenter para Windows, debe familiarizarse con algunos requisitos básicos de espacio y tamaño del sistema host.

Artículo	Requisitos
Sistemas operativos	<p>Microsoft Windows</p> <p>Para obtener la información más reciente sobre las versiones compatibles, consulte la <a href="#">"Herramienta de matriz de interoperabilidad de NetApp"</a> .</p> <p>Si está en una configuración de clúster de Windows, también debe instalar y configurar la Administración remota de Windows (WinRM).</p>
RAM mínima para el complemento SnapCenter en el host	1 GB
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	<p>5 GB</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.</p> </div>
Paquetes de software necesarios	<ul style="list-style-type: none"> <li>• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores)</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Para obtener la información más reciente sobre las versiones compatibles, consulte la <a href="#">"Herramienta de matriz de interoperabilidad de NetApp"</a> .</p> <p>Para obtener información de solución de problemas específicos de .NET, consulte <a href="#">"La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."</a></p>

## Configure sus credenciales para el complemento para Windows

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar complementos de SnapCenter y credenciales adicionales para realizar operaciones de protección de datos en los sistemas de archivos de Windows.

### Lo que necesitarás

- Debe configurar las credenciales de Windows antes de instalar complementos.

- Debe configurar las credenciales con privilegios de administrador, incluidos derechos de administrador, en el host remoto.
- Si configura credenciales para grupos de recursos individuales y el usuario no tiene privilegios de administrador completos, debe asignarle al menos los privilegios de grupo de recursos y de respaldo.

## Pasos

1. En el panel de navegación izquierdo, haga clic en **Configuración**.
2. En la página de Configuración, haga clic en **Credencial**.
3. Haga clic en **Nuevo**.
4. En la página Credencial, haga lo siguiente:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para las credenciales.

Para este campo...	Haz esto...
Nombre de usuario/Contraseña	<p>Introduzca el nombre de usuario y la contraseña utilizados para la autenticación.</p> <ul style="list-style-type: none"> <li>Administrador del dominio o cualquier miembro del grupo de administradores</li> </ul> <p>Especifique el administrador del dominio o cualquier miembro del grupo de administradores del sistema donde va a instalar el complemento de SnapCenter . Los formatos válidos para el campo Nombre de usuario son los siguientes:</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> <li>◦ UserName@upn</li> </ul> <ul style="list-style-type: none"> <li>Administrador local (sólo para grupos de trabajo)</li> </ul> <p>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema donde va a instalar el complemento de SnapCenter . Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores locales si esta cuenta tiene privilegios elevados o si la función de control de acceso de usuario está deshabilitada en el sistema host. El formato válido para el campo Nombre de usuario es el siguiente: <code>UserName</code></p> <p>No utilice comillas dobles (") ni tildes invertidas (´) en las contraseñas. No debe utilizar los símbolos menor que (&lt;) y exclamación (!) juntos en las contraseñas. Por ejemplo, menos que&lt;!10, menos que10&lt;!, acento grave`12.</p>
Password	Introduzca la contraseña utilizada para la autenticación.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, es posible que desee asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página Usuario y acceso.

## Configurar gMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrada de grupo (gMSA) que

proporciona administración automatizada de contraseñas de cuentas de servicio desde una cuenta de dominio administrada.

### Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 o posterior, que sea miembro del dominio.

### Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto en su gMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Cree y configure su gMSA:
  - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Añade objetos de computadora al grupo.  
.. Utilice el grupo de usuarios que acaba de crear para crear el  
gMSA.
```

Por ejemplo,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Correr `Get-ADServiceAccount` Comando para verificar la cuenta de  
servicio.
```

4. Configure el gMSA en sus hosts:
  - a. Habilite el módulo Active Directory para Windows PowerShell en el host donde desea utilizar la cuenta gMSA.

Para hacer esto, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Reinicie su host.
  - b. Instale gMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
  - c. Verifique su cuenta gMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`
5. Asigne los privilegios administrativos al gMSA configurado en el host.
  6. Agregue el host de Windows especificando la cuenta gMSA configurada en el servidor SnapCenter .

SnapCenter Server instalará los complementos seleccionados en el host y la gMSA especificada se utilizará como cuenta de inicio de sesión de servicio durante la instalación del complemento.

## Agregar hosts e instalar el complemento SnapCenter para Microsoft Windows

Puede utilizar la página Agregar host de SnapCenter para agregar hosts de Windows. El complemento SnapCenter para Microsoft Windows se instala automáticamente en el host especificado. Este es el método recomendado para instalar complementos. Puede agregar un host e instalar un complemento para un host individual o para un clúster.

### Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del complemento es Windows 2022, debe realizar lo siguiente:
  - Actualizar a Windows Server 2019 (compilación del SO 17763.5936) o posterior
  - Actualizar a Windows Server 2022 (compilación del SO 20348.2402) o posterior
- Debe ser un usuario asignado a un rol que tenga permisos de instalación y desinstalación de complementos, como el rol de administrador de SnapCenter .
- Al instalar un complemento en un host de Windows, si especifica una credencial que no está incorporada

o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.

- El usuario de SnapCenter debe agregarse a la función "Iniciar sesión como servicio" del servidor Windows.
- Debe asegurarse de que el servicio de cola de mensajes esté en estado de ejecución.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos.

["Configurar la cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para el sistema de archivos de Windows"](#)

#### Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .
- complementos de Windows
  - Microsoft Windows
  - Servidor Microsoft Exchange
  - Microsoft SQL Server
  - SAP HANA
- Instalación de complementos en un clúster

Si instala complementos en un clúster (WSFC, Oracle RAC o Exchange DAG), se instalan en todos los nodos del clúster.

- Almacenamiento de la serie E

No es posible instalar el complemento para Windows en un host Windows conectado al almacenamiento de la serie E.



SnapCenter no admite la adición del mismo host (host de complemento) a SnapCenter si el host ya es parte de un grupo de trabajo y cambió a otro dominio o viceversa. Si desea agregar el mismo host, debe eliminarlo de SnapCenter y agregarlo nuevamente.

#### Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Asegúrese de que **Hosts administrados** esté seleccionado en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, haga lo siguiente:

Para este campo...	Haz esto...
Tipo de host	Seleccione el tipo de host <b>Windows</b> .  SnapCenter Server agrega el host y luego instala el complemento para Windows si aún no está instalado en el host.

Para este campo...	Haz esto...
Host name	<p>Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host.</p> <p>SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el nombre de dominio completo (FQDN).</p> <p>Puede introducir las direcciones IP o el FQDN de uno de los siguientes:</p> <ul style="list-style-type: none"> <li>• Host independiente</li> <li>• Agrupación en clústeres de conmutación por error de Windows Server (WSFC)</li> </ul> <p>Si está agregando un host mediante SnapCenter y es parte de un subdominio, debe proporcionar el FQDN.</p>
Cartas credenciales	<p>Seleccione el nombre de la credencial que creó o cree las nuevas credenciales.</p> <p>La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre cómo crear una credencial.</p> <p>Los detalles sobre las credenciales, incluido el nombre de usuario, el dominio y el tipo de host, se muestran al colocar el cursor sobre el nombre de la credencial proporcionada.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>El modo de autenticación está determinado por el tipo de host que especifique en el asistente Agregar host.</p> </div>

5. En la sección **Seleccionar complementos para instalar**, seleccione los complementos que desea instalar.

Para las nuevas implementaciones, no se enumeran paquetes de complementos.

6. (Opcional) Haga clic en **Más opciones**.

Para este campo...	Haz esto...
Puerto	<p>Mantenga el número de puerto predeterminado o especifique el número de puerto.</p> <p>El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Si instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla. </div>
Ruta de instalación	<p>La ruta predeterminada es C:\Archivos de programa\ NetApp\ SnapCenter.</p> <p>Opcionalmente puedes personalizar la ruta. Para el paquete de complementos de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\ NetApp\ SnapCenter. Sin embargo, si lo desea, puede personalizar la ruta predeterminada.</p>
Agregar todos los hosts en el clúster	<p>Seleccione esta casilla de verificación para agregar todos los nodos del clúster en un WSFC.</p>
Omitir comprobaciones de preinstalación	<p>Seleccione esta casilla de verificación si ya instaló los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.</p>
Utilice la cuenta de servicio administrada grupal (gMSA) para ejecutar los servicios del complemento	<p>Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio administrada de grupo (gMSA) para ejecutar los servicios del complemento.</p> <p>Proporcione el nombre de gMSA en el siguiente formato: <i>domainName\accountName\$</i>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows. </div>

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla **Omitir comprobaciones previas**, se valida el host para comprobar si cumple los requisitos para instalar el complemento. El espacio en disco, la RAM, la versión de PowerShell,

la versión de .NET y la ubicación se verifican según los requisitos mínimos. Si no se cumplen los requisitos mínimos, se muestran mensajes de error o advertencia correspondientes.

Si el error está relacionado con el espacio en disco o la RAM, puede actualizar el archivo `web.config` ubicado en `C:\Program Files\NetApp\SnapCenter WebApp` para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, debes solucionar el problema.



En una configuración de alta disponibilidad, si está actualizando el archivo `web.config`, debe actualizar el archivo en ambos nodos.

8. Supervisar el progreso de la instalación.

## Instalar el complemento SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell

Si desea instalar el complemento SnapCenter para Microsoft Windows en varios hosts a la vez, puede hacerlo mediante el `Install-SmHostPackage` Cmdlet de PowerShell.

Debe haber iniciado sesión en SnapCenter como usuario de dominio con derechos de administrador local en cada host en el que desee instalar complementos.

### Pasos

1. Inicie PowerShell.
2. En el host del servidor SnapCenter , establezca una sesión utilizando el `Open-SmConnection` cmdlet y luego ingrese sus credenciales.
3. Agregue el host independiente o el clúster a SnapCenter mediante el `Add-SmHost` cmdlet y los parámetros requeridos.

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

4. Instale el complemento en varios hosts mediante el `Install-SmHostPackage` cmdlet y los parámetros requeridos.

Puedes utilizar el `-skipprecheck` Opción cuando ha instalado los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.

## Instale el complemento SnapCenter para Microsoft Windows de forma silenciosa desde la línea de comandos

Puede instalar el complemento de SnapCenter para Microsoft Windows localmente en un host de Windows si no puede instalar el complemento de forma remota desde la GUI de SnapCenter . Puede ejecutar el programa de instalación del complemento SnapCenter para Microsoft Windows sin supervisión, en modo silencioso, desde la línea de comandos de Windows.

## Antes de empezar

- Debe tener instalado el paquete de alojamiento ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores).
- Debe tener instalado PowerShell 7.4.2 o posterior.
- Debes ser un administrador local en el host.

## Pasos

1. Descargue el complemento SnapCenter para Microsoft Windows desde su ubicación de instalación.

Por ejemplo, la ruta de instalación predeterminada es C:\ProgramData\NetApp\SnapCenter\Package Repository.

Se puede acceder a esta ruta desde el host donde está instalado el servidor SnapCenter .

2. Copie el archivo de instalación en el host en el que desea instalar el complemento.
3. Desde el símbolo del sistema, navegue hasta el directorio donde descargó el archivo de instalación.
4. Ingrese el siguiente comando, reemplazando las variables con sus datos:

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""  
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=  
ISFeatureInstall=SCW
```

Por ejemplo:

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository  
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:  
\HPPW_SCW_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW`
```



Todos los parámetros pasados durante la instalación del complemento para Windows distinguen entre mayúsculas y minúsculas.

Introduzca los valores para las siguientes variables:

Variable	Valor
/debuglog"<Ruta_del_registro_de_depuración>	Especifique el nombre y la ubicación del archivo de registro del instalador de la suite, como en el siguiente ejemplo: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
PUERTO BI_SNAPCENTER	Especifique el puerto en el que SnapCenter se comunica con SMCORE.

Variable	Valor
SUITE_INSTALLDIR	Especifique el directorio de instalación del paquete del complemento de host.
BI_CUENTA DE SERVICIO	Especifique el complemento SnapCenter para la cuenta de servicio web de Microsoft Windows.
BI_SERVICEPWD	Especifique la contraseña para la cuenta de servicio web del complemento SnapCenter para Microsoft Windows.
Instalación de ISFeature	Especifique la solución que SnapCenter implementará en el host remoto.

El parámetro *debuglog* incluye la ruta del archivo de registro de SnapCenter. Escribir en este archivo de registro es el método preferido para obtener información de solución de problemas, porque el archivo contiene los resultados de las comprobaciones que realiza la instalación para verificar los requisitos previos del complemento.

Si es necesario, puede encontrar información adicional de solución de problemas en el archivo de registro del paquete SnapCenter para Windows. Los archivos de registro del paquete se enumeran (el más antiguo primero) en la carpeta *%Temp%*, por ejemplo, *C:\temp\*.



La instalación del complemento para Windows registra el complemento en el host y no en el servidor SnapCenter. Puede registrar el complemento en el servidor SnapCenter agregando el host mediante la GUI de SnapCenter o el cmdlet de PowerShell. Una vez agregado el host, el complemento se descubre automáticamente.

## Supervisar el estado de instalación del paquete de complementos de SnapCenter

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

- En curso
- Completado exitosamente
- Fallido
- Completado con advertencias o no se pudo iniciar debido a advertencias
- En cola

### Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
  - a. Haga clic en **Filtro**.
  - b. Opcional: especifique la fecha de inicio y finalización.
  - c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
  - d. En el menú desplegable Estado, seleccione el estado de la instalación.
  - e. Haga clic en **Aplicar**.
4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configurar el certificado de CA

### Generar archivo CSR de certificado de CA

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

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



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

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



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

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

### Importar certificados de CA

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

#### Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y haga clic en **Archivo > Agregar o quitar complemento**.
2. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.

3. En la ventana del complemento Certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
4. Haga clic en **Consola raíz > Certificados – Equipo local > Autoridades de certificación raíz de confianza > Certificados**.
5. Haga clic con el botón derecho en la carpeta “Autoridades de certificación raíz de confianza” y luego seleccione **Todas las tareas > Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

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



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

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

## Obtenga la huella digital del certificado CA

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

### Pasos

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

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

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

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

- b. Copiar la huella digital.

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

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

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

### Pasos

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

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

Por ejemplo:

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

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

Por ejemplo:

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

## Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

### Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.

- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

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

### Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

### Después de terminar

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

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



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

## Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.