Instale el plugin de SnapCenter para Microsoft Windows

SnapCenter Software 4.5

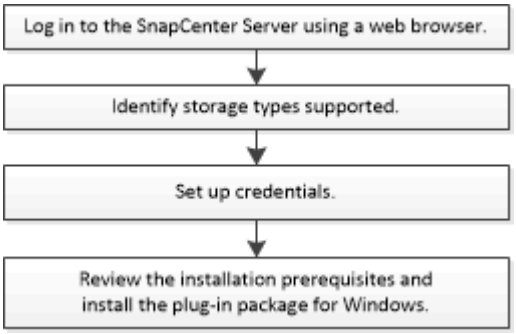
NetApp
January 18, 2024

Tabla de contenidos

Instale el plugin de SnapCenter para Microsoft Windows

Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft Windows

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



Requisitos de instalación del plugin de SnapCenter para Microsoft Windows

Debe estar al tanto de determinados requisitos de instalación antes de instalar el plugin para Windows.

Antes de empezar a utilizar el plugin para Windows, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas de requisitos previos.

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

  La función de administrador de SnapCenter debe tener privilegios de administración.

- Debe haber instalado y configurado el servidor SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada 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 una replicación de backup.

Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows

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

Elemento	Requisitos
Sistemas operativos	Microsoft Windows Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".
RAM mínima para el plugin de SnapCenter en el host	1 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	5 GB Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.
Paquetes de software obligatorios	• Microsoft .NET Framework 4.5.2 o posterior • Windows Management Framework (WMF) 4.0 o posterior • PowerShell 4.0 o posterior Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Configure sus credenciales para el plugin para Windows

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

Lo que necesitará

- Debe configurar credenciales de Windows antes de instalar plugins.
- Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador, en el host remoto.
- Si se configuran credenciales para grupos de recursos individuales y el usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al usuario.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.

2. En la página Settings, haga clic en **Credential**.
3. Haga clic en **Nuevo**.
4. En la página Credential, haga lo siguiente:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Introduzca un nombre para las credenciales.
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña para la autenticación. • Administrador de dominio o cualquier miembro del grupo de administradores Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Username son los siguientes: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Administrador local (sólo para grupos de trabajo) Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es el siguiente: `UserName` No utilice comillas dobles (") ni marcas de retroceso (') en las contraseñas. No debe usar el signo menos de (<) y el signo de exclamación (!) los símbolos juntos en las contraseñas. Por ejemplo, arrendhan<!10, les10<!, backtick'12.
Contraseña	Introduzca la contraseña usada para autenticación.

5. Haga clic en **Aceptar**.

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

Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

Lo que necesitará

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

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

   ```
    domainName\accountName$
   .. Agregar objetos de equipo 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,…>
   .. Ejecución `Get-ADServiceAccount` comando para verificar la
   cuenta de servicio.
   ```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, 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 el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

   1. Asigne los privilegios administrativos al GMSA configurado en el host.
   2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

      El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

Lo que necesitará

- Debe tener un controlador de dominio de Windows Server 2012 o posterior.
- Debe tener un host de Windows Server 2012 o posterior, que es miembro del dominio.
- Pasos*

  1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
  2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
  3. Crear y configurar su GMSA:

a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo 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,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la
cuenta de servicio.
```

4. Configure el GMSA en sus hosts:

   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

      Para ello, 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 el host.
   b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
   c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`
      1. Asigne los privilegios administrativos al GMSA configurado en el host.

2. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

   El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

Añada hosts e instale el plugin de SnapCenter para Microsoft Windows

Puede utilizar la página SnapCenter Add Host para añadir hosts de Windows. El plugin de SnapCenter para Microsoft Windows está instalado automáticamente en el host especificado. Este es el método recomendado para la instalación de plugins. Puede añadir un host e instalar un plugin para un host individual o para un clúster.

Lo que necesitará

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada 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 en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configurar la cuenta de servicio administrado de grupo en Windows Server 2012 o posterior para el sistema de archivos de Windows"

Acerca de esta tarea

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Plugins de Windows
  - Microsoft Windows
  - Servidor de Microsoft Exchange
  - Microsoft SQL Server
  - SAP HANA
  - Plugins personalizados
- Instalar plugins en un clúster

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

- Almacenamiento E-series

  No puede instalar el plugin para Windows en un host de Windows conectado al almacenamiento E-series.

- Pasos*

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

Para este campo…	**Realice lo siguiente…**
Tipo de host	Seleccione el tipo de host **Windows**. El servidor de SnapCenter añade el host y, a continuación, instala el plugin para Windows si aún no está instalado en el host.
Nombre de host	Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el nombre de dominio completamente cualificado (FQDN). Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • Clustering de conmutación al nodo de respaldo de Windows Server (WSFC) Si va a añadir un host mediante SnapCenter y forma parte de un subdominio, debe proporcionar el FQDN.

Para este campo…	Realice lo siguiente…
Credenciales	Seleccione el nombre de credencial que ha creado o cree las credenciales nuevas. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte los detalles de cómo crear una credencial. Los detalles sobre las credenciales, incluidos el nombre de usuario, el dominio y el tipo de host, se muestran colocando el cursor sobre el nombre de las credenciales que ha proporcionado. El modo de autenticación se determina por el tipo de host que especifique en el asistente Add host.

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.

   Para nuevas implementaciones, no aparece ningún paquete de plugins.

6. (Opcional) haga clic en **más opciones**.

Para este campo…	Realice lo siguiente…
Puerto	Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado. Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error.
Ruta de instalación	La ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta. Para el paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Sin embargo, si lo desea, puede personalizar la ruta predeterminada.

Para este campo…	Realice lo siguiente…
Añada todos los hosts del clúster	Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un WSFC.
Omitir comprobaciones previas a la instalación	Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin.
Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in	Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de complemento. Proporcione el nombre de GMSA con el siguiente formato: *Domainname\accountName$*. GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows.

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación **Skip prechecks**, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. Se comprueban el espacio en disco, la memoria RAM, la versión de PowerShell, la versión de NET y la ubicación comparando estos elementos con los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

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

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

1. Supervise el progreso de la instalación.

Instale el plugin de SnapCenter para Microsoft Windows en varios hosts remotos mediante cmdlets de PowerShell

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

Tiene que haber iniciado sesión en SnapCenter como usuario del dominio con derechos de administrador local en cada host en el que desee instalar los plugins.

- Pasos*
  1. Inicie PowerShell.
  2. En el host del servidor SnapCenter, establezca una sesión mediante el `Open-SmConnection` cmdlet y, a continuación, introduzca las credenciales.
  3. Añada el host o el clúster independiente a SnapCenter mediante el `Add-SmHost` cmdlet y los parámetros necesarios.

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

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

     Puede utilizar el `-skipprecheck` opción cuando instaló los plugins manualmente y no desea validar si el host cumple con los requisitos para instalar el plugin.

Instale el plugin de SnapCenter para Microsoft Windows silenciosamente desde la línea de comandos

Puede instalar el plugin de SnapCenter para Microsoft Windows localmente en un host de Windows si no puede instalar el plugin de forma remota desde la interfaz gráfica de usuario de SnapCenter. Puede ejecutar el programa de instalación del plugin de SnapCenter para Microsoft Windows sin supervisión y en el modo silencioso desde la línea de comandos de Windows.

Lo que necesitará

- Debe haber instalado Microsoft.Net 4.5.2 o superior.
- Debe haber instalado PowerShell 4.0 o posterior.
- Debe haber activado la cola de mensajes de Windows.
- Debe ser un administrador local en el host.
- Pasos*
  1. Descargue el plugin de SnapCenter para Microsoft Windows desde su ubicación de instalación.

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

     Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.

  2. Copie el archivo de instalación en el host en el que desea instalar el plugin.
  3. Desde el símbolo del sistema, desplácese hasta el directorio en el que ha descargado el archivo de instalación.
  4. Introduzca el siguiente comando y sustituya las variables por 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 que se pasan durante la instalación del plugin para Windows distinguen entre mayúsculas y minúsculas.

Introduzca los valores para las siguientes variables:

Variable	Valor
/DEBUGLOG"<Debug_Log_Path>	Especifique el nombre y la ubicación del archivo de registro del instalador del paquete, como en el ejemplo siguiente: setup.exe /DEBUGLOG"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Indique el puerto en el que SnapCenter se comunica con SMCore.
SUITE_INSTALLDIR	Indique el directorio de instalación para el paquete de plugins del host.
BI_SERVICEACCOUNT	Indique la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
BI_SERVICEPWD	Indique la contraseña para la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
ISFeatureInstall	Indique la solución que debe aplicar SnapCenter en un host remoto.

El parámetro *DEBUGLOG* incluye la ruta del archivo de registro para SnapCenter. Escribir en este archivo de registro es el método preferido para obtener información de resolución de averías, ya que el archivo contiene los resultados de las comprobaciones que se realizan durante la instalación con respecto a los requisitos del plugin.

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

La instalación del plugin para Windows registra el plugin en el host, no en el servidor de SnapCenter. Es posible registrar el plugin en SnapCenter Server. Para ello, se debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Una vez añadido el host, el plugin se detecta automáticamente.

Supervise el estado de instalación del paquete de plugins de SnapCenter

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

Acerca de esta tarea

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

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **Jobs**, para filtrar la lista de modo que sólo se muestren las operaciones de instalación del plug-in, haga lo siguiente:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de 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**.

Configure el certificado de CA

Genere un archivo CSR de certificado de CA

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

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

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

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

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

Importar certificados de CA

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

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

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

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

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

Obtenga la huella digital del certificado de CA

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

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

        Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".
  2. Realice lo siguiente desde PowerShell:
     a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

        Get-ChildItem -Path Cert:\LocalMachine\My

     b. Copie la huella digital.

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

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

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

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

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

     Por ejemplo:

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

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

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

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

Por ejemplo:

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

Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

Lo que necesitará

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

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

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **hosts**.
  2. En la página hosts, haga clic en **Managed hosts**.
  3. Seleccione uno o varios hosts de plugins.
  4. Haga clic en **más opciones**.
  5. Seleccione **Activar validación de certificados**.

Después de terminar

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

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

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