Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server

SnapCenter Software 4.8

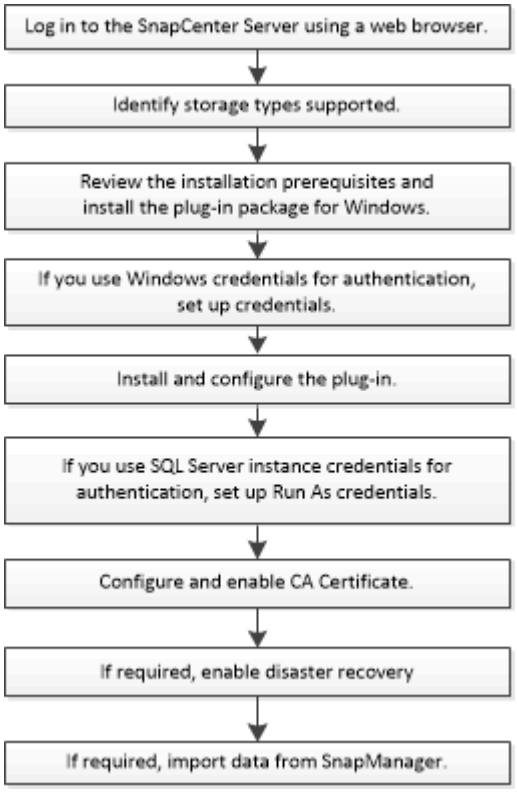
NetApp
January 18, 2024

Tabla de contenidos

Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server

Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft SQL Server

Tendrá que instalar y configurar el plugin de SnapCenter para Microsoft SQL Server si desea proteger las bases de datos de SQL Server.



Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft SQL Server

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Debe tener un usuario con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Si gestiona nodos de clúster en SnapCenter, debe tener un usuario con privilegios de administrador para todos los nodos del clúster.
- Debe tener un usuario con permisos de administrador del sistema en SQL Server.

  El plugin de SnapCenter para Microsoft SQL Server utiliza Microsoft VDI Framework, para lo que se requiere acceso de sysadmin.

"Artículo de soporte de Microsoft 2926557: Las operaciones de backup y restauración de VDI de SQL Server requieren privilegios de administrador del sistema"

- 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.
- Si está instalado SnapManager para Microsoft SQL Server, debe haber detenido o deshabilitado el servicio y las programaciones.

  Si prevé importar tareas de backup o clonado a SnapCenter, no desinstale SnapManager para Microsoft SQL Server.

- El host debe poder resolverse con el nombre de dominio completo (FQDN) del servidor.

  Si el archivo hosts se modifica para que pueda resolverse y si se especifican tanto el nombre corto como el FQDN en el archivo hosts, cree una entrada en el archivo hosts SnapCenter con el siguiente formato: <ip_address> <host_fqdn> <host_name>

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.

Elemento	Requisitos
Paquetes de software obligatorios	• Microsoft .NET Framework 4.7.2 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". Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

Configure credenciales para el paquete de plugins de SnapCenter 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 o bases de datos.

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.
- Autenticación SQL en hosts Windows

  Debe configurar credenciales de SQL después de instalar plugins.

  Si va a implementar el plugin de SnapCenter para Microsoft SQL Server, debe configurar las credenciales de SQL después de instalar plugins. Configure una credencial para un usuario con permisos de administrador del sistema en SQL Server.

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

- 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, especifique la información necesaria para configurar las credenciales:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Escriba un nombre para la credencial.
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • Administrador del dominio Especifique el administrador de dominio en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Administrador local (sólo para grupos de trabajo) Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: `UserName` 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.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar. Si selecciona el modo de autenticación de SQL, también debe especificar la instancia de SQL Server y el host donde está ubicada esa instancia.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, se recomienda asignar el mantenimiento de credenciales a un usuario o un grupo de usuarios en la página User and Access.

Configure las credenciales para un recurso individual de SQL Server

Es posible configurar credenciales para realizar trabajos de protección de datos en un recurso individual de SQL Server para cada usuario. Si bien es posible configurar las credenciales de manera global, se recomienda hacerlo solo para un recurso particular.

Acerca de esta tarea

- Si utiliza credenciales de Windows para la autenticación, debe configurar las credenciales para poder instalar plugins.

  Sin embargo, si utiliza una instancia de SQL Server para la autenticación, debe añadir la credencial después de instalar los plugins.

- Si ha habilitado la autenticación SQL durante la configuración de las credenciales, la instancia o base de datos detectadas se mostrarán con un icono de candado de color rojo.

  Si aparece el icono de candado, debe especificar las credenciales de la instancia o la base de datos para añadir correctamente la instancia o la base de datos al grupo de recursos.

- Debe asignar la credencial a un usuario de control de acceso basado en roles (RBAC) sin acceso de administrador del sistema cuando se cumplan las siguientes condiciones:
  - La credencial se asigna a una instancia de SQL.
  - La instancia o el host de SQL se asignan a un usuario de RBAC.

    El usuario debe tener privilegios tanto del grupo de recursos como de backup.

Paso 1: Agregar y configurar credenciales

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Settings, haga clic en **Credential**.
   a. Para agregar una nueva credencial, haga clic en **Nuevo**.
   b. En la página Credential, configure las credenciales:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Introduzca un nombre para las credenciales.

Para este campo…	Realice lo siguiente…
Nombre de usuario	Introduzca el nombre de usuario utilizado para autenticación de SQL Server. • Administrador de dominio o cualquier miembro del grupo de administradores Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo **Nombre de usuario** son: ◦ *NetBIOS\Username* ◦ *Domain FQDN\Username* • 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 locales si la cuenta de usuario tiene privilegios elevados o el usuario La función de control de acceso está deshabilitada en el sistema host. El formato válido para el campo **Nombre de usuario** es: *Username*
Contraseña	Introduzca la contraseña usada para autenticación.
Modo de autenticación	Seleccione el modo de autenticación SQL Server. También es posible seleccionar la autenticación de Windows si el usuario de Windows tiene privilegios de administrador del sistema en el servidor SQL.
Host	Seleccione el host.
Instancia de SQL Server	Seleccione la instancia de SQL Server.

c. Haga clic en **Aceptar** para agregar la credencial.

Paso 2: Configurar instancias

1. En el panel de navegación de la izquierda, haga clic en **Recursos**.
2. En la página Resources, seleccione **Instance** en la lista **View**.
   a. Haga clic en y, a continuación, seleccione el nombre de host para filtrar las instancias.
   b. Haga clic en para cerrar el panel de filtros.
3. En la página Instance Protect, proteja la instancia y, si es necesario, haga clic en **Configure Credentials**.

   Si el usuario que ha iniciado sesión en el servidor SnapCenter no tiene acceso al complemento SnapCenter para Microsoft SQL Server, el usuario deberá configurar las credenciales.

   La opción de credencial no se aplica a las bases de datos y los grupos de disponibilidad.

4. Haga clic en **Actualizar recursos**.

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.

Instale el plugin de SnapCenter para Microsoft SQL Server

Añada hosts e instale el paquete de plugins de SnapCenter para Windows

Debe utilizar la página SnapCenter **Add Host** para añadir hosts e instalar el paquete de plugins. Los plugins se instalan automáticamente en hosts remotos.

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 incorporada, deberá deshabilitar UAC en el host.
- 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 SQL"

Acerca de esta tarea

No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

Puede añadir un host e instalar los paquetes de los plugins para un host individual o para un clúster. Si está instalando los plugins en un clúster o clustering de conmutación al nodo de respaldo de Windows Server (WSFC), los plugins se instalan en todos los nodos del clúster.

Para obtener información sobre la gestión de los hosts, consulte "Gestionar hosts".

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página hosts, haga lo siguiente:

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione Windows como tipo de host. El servidor de SnapCenter añade el host e instala el plugin para Windows si el plugin todavía no está instalado en el host. Si selecciona la opción de Microsoft SQL Server en la página Plug-ins, SnapCenter Server instala el plugin para SQL Server.
Nombre de host	Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. La dirección IP es compatible con hosts de dominio que no son de confianza solo si se resuelve en el FQDN. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • WSFC Si va a añadir un host mediante SnapCenter y el host 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 nuevas credenciales. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales. Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host.

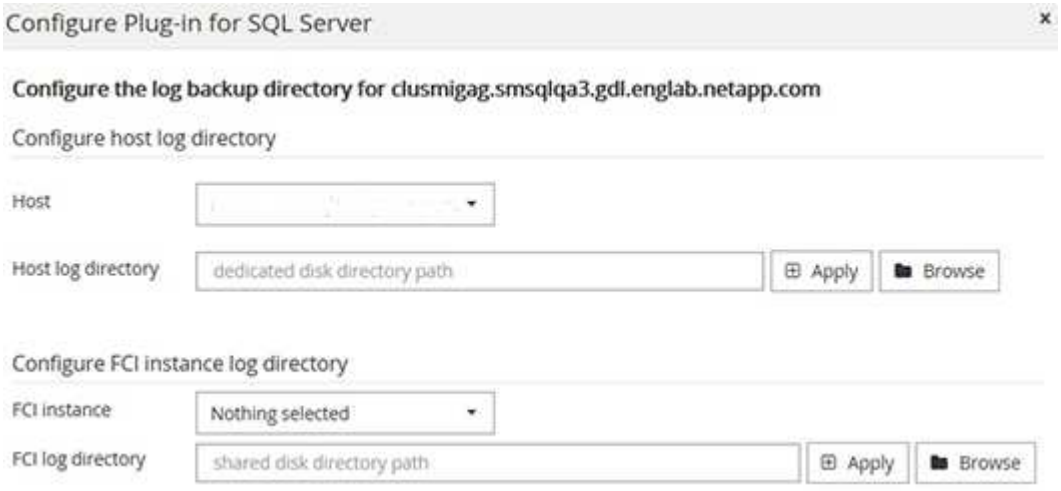
5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.
6. Haga clic en **más opciones**.

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.
Añada todos los hosts del clúster	Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un WSFC o un Availability Group de SQL. Debe añadir todos los nodos del clúster seleccionando la casilla de comprobación correspondiente del clúster en la GUI si desea gestionar e identificar varios grupos de disponibilidad SQL disponibles en un clúster.

Para este campo…	Realice lo siguiente…
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: Nombre_de_dominio\accountName$. Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador de sistema, el GMSA se utilizará para conectarse a la instancia de SQL.

7. Haga clic en **Enviar**.
8. Para el plugin de SQL, seleccione el host para configurar el directorio de registro.
   a. Haga clic en **Configurar directorio de registro** y, en la página Configurar directorio de registro de host, haga clic en **examinar** y complete los siguientes pasos:

      Tan solo se enumeran las unidades NetApp LUN como disponibles para su selección. SnapCenter realiza un backup y replica el directorio de registro del host como parte de la operación de backup.



      i. Seleccione la letra de la unidad o el punto de montaje del host donde se almacenará el registro del host.
      ii. Si es necesario, elija un subdirectorio.
      iii. Haga clic en **Guardar**.
9. 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. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a 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 RAM, es posible 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 SQL Server en varios hosts remotos mediante cmdlets

Puede instalar el plugin de SnapCenter para Microsoft SQL Server en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

Lo que necesitará

Debe haberse registrado en SnapCenter como usuario del dominio con derechos de administrador local en cada host en el que desee instalar el paquete de plugins.

- Pasos*

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
3. Instale el plugin de SnapCenter para Microsoft SQL Server en varios hosts remotos mediante el cmdlet Install-SmHostPackage y los parámetros requeridos.

   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".

Puede utilizar la opción -skipprecheck cuando ya haya instalado los plugins manualmente y no desee validar si el host cumple los requisitos para instalar el plugin.

1. Introduzca sus credenciales para la instalación remota.

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

Debe instalar el plugin de SnapCenter para Microsoft SQL Server desde la interfaz de usuario de SnapCenter. Sin embargo, si no puede hacerlo por algún motivo, puede ejecutar el programa de instalación del plugin para SQL Server sin supervisión en el modo silencioso desde la línea de comandos de Windows.

Lo que necesitará

- Debe eliminar la versión anterior del plugin de SnapCenter para Microsoft SQL Server antes de instalar.

  Para obtener más información, consulte "Cómo instalar un plugin de SnapCenter de forma manual y directa desde el host del plugin".

- Pasos*

  1. Compruebe si existe una carpeta C:\temp en el host del plugin y el usuario que ha iniciado sesión tiene acceso completo a ella.
  2. Descargue el software del plugin para SQL Server desde C:\ProgramData\NetApp\SnapCenter\Package Repository.

     Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.
  3. Copie el archivo de instalación en el host en el que desea instalar el plugin.
  4. Desde el símbolo del sistema de Windows en el host local, desplácese hasta el directorio en el que guardó los archivos de instalación del plugin.
  5. Instale el software del plugin para SQL Server:

     ```
     "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
     /log"Log_Path" BI_SNAPCENTER_PORT=Num
     SUITE_INSTALLDIR="Install_Directory_Path"
     BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
     ISFeatureInstall=SCW,SCSQL
     ```

     Sustituya los valores del marcador de posición por sus datos

     - Debug_Log_Path es el nombre y la ubicación del archivo de registro del instalador de la suite.
     - Log_Path es la ubicación de los registros de instalación de los componentes del plugin (SCW, SCSQL y SMCore).
     - Num es el puerto en el que SnapCenter se comunica con SMCore
     - Install_Directory_Path es el directorio de instalación del paquete de plugins del host.
     - Domain\Administrator es la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
     - La contraseña es la contraseña de la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
       ```
       "snapcenter_windows_host_plugin.exe"/silent
       /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
       SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
       BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
       ISFeatureInstall=SCW,SCSQL
       ```

     Todos los parámetros que se pasan durante la instalación del plugin para SQL Server distinguen entre mayúsculas y minúsculas.

  1. Supervise el programador de tareas de Windows, el archivo de registro de instalación principal C:\Installdebug.log y los archivos de instalación adicionales en C:\Temp.
  2. Supervise el directorio %temp% para comprobar que los msiexe.exe instaladores están instalando el

software sin errores.

> La instalación del plugin para SQL Server registra el plugin en el host y 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 la instalación del plugin para SQL Server

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 **Jobs**.
  3. En la página Jobs, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de plugins, proceda como sigue:
     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**.

Configurar certificado de CA

Genere un archivo CSR de certificado de CA

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

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

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

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

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

Importar certificados de CA

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

- Pasos*

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

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

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

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

Obtenga la huella digital del certificado de CA

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

- Pasos*

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

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

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

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie la huella digital.

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

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

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

- Pasos*

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

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

   Por ejemplo:

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

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

Por ejemplo:

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

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.

Configure la recuperación ante desastres

Recuperación ante desastres del plugin de SnapCenter para SQL Server

Cuando el plugin de SnapCenter para SQL Server está inactivo, realice los siguientes pasos para cambiar a un host de SQL diferente y recuperar los datos.

Lo que necesitará

- El host secundario debe tener el mismo sistema operativo, aplicación y nombre de host que el host primario.
- Inserte el complemento SnapCenter para SQL Server en un host alternativo utilizando la página **Agregar host** o **Modificar host**. Consulte "Gestionar hosts" si quiere más información.

Pasos

1. Seleccione el host en la página **hosts** para modificar e instalar el plugin de SnapCenter para SQL Server.
2. (Opcional) reemplace los archivos de configuración del plugin de SnapCenter para SQL Server desde un backup de recuperación ante desastres (DR) a la máquina nueva.
3. Importe las programaciones de Windows y SQL desde la carpeta del plugin de SnapCenter para SQL Server desde el backup de recuperación ante desastres.

Si quiere más información

Consulte "API de recuperación ante desastres" vídeo.

Recuperación ante desastres de almacenamiento (DR) para el plugin de SnapCenter para SQL Server

Para recuperar el almacenamiento del plugin de SnapCenter para SQL Server, habilitar el modo DR para almacenamiento en la página Global Settings.

Lo que necesitará

- Compruebe que los plugins estén en modo de mantenimiento.
- Rompa la relación de SnapMirror/SnapVault. "Romper las relaciones de SnapMirror"
- Conecte el LUN de secundario al equipo host con la misma letra de unidad.
- Asegúrese de que todos los discos estén conectados utilizando las mismas letras de unidad que se usaron antes de la recuperación ante desastres.
- Reinicie el servicio de servidor MSSQL.

- Asegúrese de que los recursos SQL vuelven a estar en línea.

Acerca de esta tarea

No se admite la recuperación ante desastres en las configuraciones VMDK y RDM.

- Pasos*
  1. En la página Configuración, vaya a **Ajustes** > **Ajustes globales** > **recuperación ante desastres**.
  2. Seleccione **Activar recuperación ante desastres**.
  3. Haga clic en **aplicar**.
  4. Compruebe si el trabajo DR está activado o no haciendo clic en **Monitor** > **trabajos**.

Después de terminar

- Si se crean bases de datos nuevas después de la conmutación al nodo de respaldo, las bases de datos se pondrán en modo sin recuperación ante desastres.

  Las nuevas bases de datos seguirán funcionando como lo hicieron antes del fallo.

- Los backups nuevos que se crearon en modo de recuperación ante desastres se enumeran en SnapMirror o SnapVault (secundario) en la página Topology.

  Se muestra un icono "i" junto a los nuevos backups para indicar que estos backups se han creado durante el modo de recuperación ante desastres.

- Puede eliminar los backups del plugin de SnapCenter para SQL Server que se crearon durante la conmutación por error usando la interfaz de usuario o el siguiente cmdlet de: `Remove-SmBackup`
- Después de la conmutación por error, si desea que algunos de los recursos estén en modo no DR, use el cmdlet siguiente: `Remove-SmResourceDRMode`

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

- SnapCenter Server gestionará los recursos de almacenamiento individuales (bases de datos SQL) que están en modo DR o no DR, pero no el grupo de recursos con recursos de almacenamiento que se encuentran en modo DR o en modo no DR.

Conmutación tras recuperación del plugin de SnapCenter para almacenamiento secundario de SQL Server al almacenamiento principal

Una vez que el almacenamiento primario del plugin de SnapCenter para SQL Server vuelve a estar en línea, debe recuperar el almacenamiento principal.

Lo que necesitará

- Coloque el plugin de SnapCenter para SQL Server en el modo **Mantenimiento** de la página Managed hosts.
- Desconecte el almacenamiento secundario del host y conéctelo del almacenamiento primario.
- Para volver a realizar la conmutación tras recuperación al almacenamiento principal, asegúrese de que la dirección de la relación sigue siendo la misma que antes de la conmutación por error realizando la operación de resincronización inversa.

Para conservar los roles del almacenamiento primario y secundario después de la operación de resincronización inversa, vuelva a ejecutar la operación de resincronización inversa.

Para obtener más información, consulte "Volver a sincronizar las relaciones de reflejos"

- Reinicie el servicio de servidor MSSQL.
- Asegúrese de que los recursos SQL vuelven a estar en línea.

> Durante la conmutación por error o la conmutación tras recuperación del plugin, el estado general del plugin no se actualiza de forma inmediata. El estado general del host y el plugin se actualiza durante la operación de actualización del host posterior.

- Pasos*
  1. En la página Configuración, vaya a **Ajustes** > **Ajustes globales** > **recuperación ante desastres**.
  2. Deseleccione **Activar recuperación ante desastres**.
  3. Haga clic en **aplicar**.
  4. Compruebe si el trabajo DR está activado o no haciendo clic en **Monitor** > **trabajos**.

Después de terminar

- Puede eliminar los backups del plugin de SnapCenter para SQL Server que se crearon durante la conmutación por error usando la interfaz de usuario o el siguiente cmdlet de: `Remove-SmDRFailoverBackups`