



Instalar el complemento de SnapCenter para Microsoft Exchange Server

SnapCenter software

NetApp

November 06, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-61/protect-sce/concept_install_snapcenter_plug_in_for_microsoft_exchange_server.html on November 06, 2025. Always check docs.netapp.com for the latest.

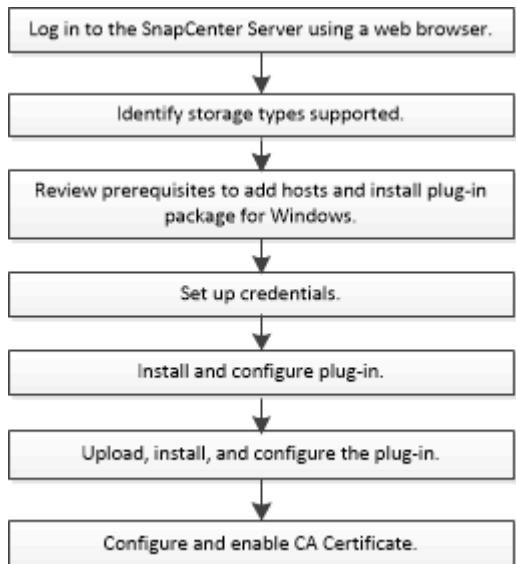
Tabla de contenidos

Instalar el complemento de SnapCenter para Microsoft Exchange Server	1
Flujo de trabajo de instalación del complemento de SnapCenter para Microsoft Exchange Server	1
Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para Microsoft Exchange Server	1
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	2
Se requieren privilegios de Exchange Server	3
Requisitos del host para instalar el paquete de complementos de SnapCenter para Windows	4
Configurar credenciales para el complemento SnapCenter para Windows	5
Configurar gMSA en Windows Server 2016 o posterior	7
Agregar hosts e instalar el complemento para Exchange	8
Configurar un puerto personalizado para la comunicación NET TCP	13
Instalar el complemento para Exchange desde el host del servidor SnapCenter mediante cmdlets de PowerShell	14
Instale el complemento de SnapCenter para Exchange de forma silenciosa desde la línea de comandos ..	15
Supervisar el estado de instalación del paquete de complementos de SnapCenter	16
Configurar el certificado de CA	17
Generar archivo CSR de certificado de CA	17
Importar certificados de CA	17
Obtenga la huella digital del certificado CA	18
Configurar el certificado de CA con los servicios del complemento de host de Windows	19
Habilitar certificados CA para complementos	20
Configurar SnapManager 7.x para que Exchange y SnapCenter coexistan	20

Instalar el complemento de SnapCenter para Microsoft Exchange Server

Flujo de trabajo de instalación del complemento de SnapCenter para Microsoft Exchange Server

Debe instalar y configurar el complemento SnapCenter para Microsoft Exchange Server si desea proteger las bases de datos de Exchange.



Requisitos previos para agregar hosts e instalar el complemento de SnapCenter para Microsoft Exchange Server

Antes de agregar un host e instalar los paquetes de complementos, debe completar todos los requisitos.

- Si está utilizando iSCSI, el servicio iSCSI debe estar ejecutándose.
- Debe tener un usuario de dominio con privilegios de administrador local con permisos de inicio de sesión local en el host remoto.
- Debe utilizar Microsoft Exchange Server 2013, 2016 o 2019 para configuraciones independientes y de grupo de disponibilidad de base de datos.
- 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.
- Si administra nodos de clúster en SnapCenter, debe tener un usuario con privilegios administrativos para todos los nodos del clúster.
- Debe tener un usuario con permisos administrativos en el servidor Exchange.
- Si SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya están instalados, debe anular el registro del proveedor de hardware VSS utilizado por SnapDrive para Windows antes de instalar el complemento para Exchange en el mismo Exchange Server para garantizar una protección de datos

exitosa mediante SnapCenter.

- Si SnapManager para Microsoft Exchange Server y el complemento para Exchange están instalados en el mismo servidor, debe suspender o eliminar del programador de Windows todas las programaciones creadas por SnapManager para Microsoft Exchange Server.
- El host debe poder resolverse al nombre de dominio completo (FQDN) desde el servidor. Si se modifica el archivo de hosts para que se pueda resolver y si tanto el nombre corto como el FQDN se especifican en el archivo de hosts, cree una entrada en el archivo de hosts de SnapCenter con el siguiente formato:
`<dirección_ip> <fqdn_de_host> <nombre_de_host>`.
- Asegúrese de que los siguientes puertos no estén bloqueados en el firewall; de lo contrario, la operación de agregar host fallará. Para resolver este problema, debe configurar el rango de puertos dinámicos. Para obtener más información, consulte "[Documentación de Microsoft](#)" .
 - Rango de puertos 50000 - 51000 para Windows 2016 y Exchange 2016
 - Rango de puertos 6000-6500 para Windows 2012 R2 y Exchange 2013
 - Rango de puertos 49152-65536 para Windows 2019

Para identificar el rango de puertos, ejecute los siguientes comandos:



- netsh int ipv4 muestra puerto dinámico tcp
- netsh int ipv4 muestra puerto dinámico udp
- netsh int ipv6 muestra puerto dinámico tcp
- netsh int ipv6 mostrar puerto dinámico udp

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	Microsoft Windows Para obtener la información más reciente sobre las versiones compatibles, consulte la " Herramienta de matriz de interoperabilidad de NetApp " .
RAM mínima para el complemento SnapCenter en el host	1 GB

Artículo	Requisitos
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	<p>5 GB</p> <p></p> <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>
Paquetes de software necesarios	<ul style="list-style-type: none"> Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) PowerShell Core 7.4.2 Java 11 Oracle Java y OpenJDK <p>Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows.</p> <p>Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp".</p> <p>Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet".</p>

Se requieren privilegios de Exchange Server

Para permitir que SnapCenter agregue Exchange Server o DAG, e instalar el complemento de SnapCenter para Microsoft Exchange Server en un host o DAG, debe configurar SnapCenter con credenciales para un usuario con un conjunto mínimo de privilegios y permisos.

Debe tener un usuario de dominio con privilegios de administrador local y con permisos de inicio de sesión local en el host de Exchange remoto, así como permisos administrativos en todos los nodos del DAG. El usuario del dominio requiere los siguientes permisos mínimos:

- Agregar copia de base de datos de buzón
- Desmontar base de datos
- Obtener la configuración del servidor de anuncios

- Obtener grupo de disponibilidad de base de datos
- Obtener servidor de intercambio
- Obtener base de datos del buzón
- Obtener estado de copia de la base de datos del buzón
- Obtener servidor de buzón
- Obtener estadísticas del buzón
- Obtener base de datos de carpeta pública
- Mover base de datos de buzones activos
- Mover-RutaDeBaseDeDatos -ConfiguraciónSolo:\$true
- Base de datos de montaje
- Nueva base de datos de buzones
- Nueva base de datos de carpetas públicas
- Eliminar base de datos de buzones
- Eliminar copia de la base de datos del buzón
- Eliminar base de datos de carpetas públicas
- Copia de la base de datos del buzón de currículum
- Establecer la configuración del servidor de anuncios
- Establecer-MailboxDatabase -allowfilerestore:\$true
- Copiar base de datos del buzón de correo
- Establecer-Base de datos de carpeta pública
- Suspender-Copia de base de datos de buzones
- Actualizar-Copia de base de datos del buzón

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 "Herramienta de matriz de interoperabilidad de NetApp" .</p>
RAM mínima para el complemento SnapCenter en el host	1 GB

Artículo	Requisitos
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	<p>5 GB</p> <p></p> <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>
Paquetes de software necesarios	<ul style="list-style-type: none"> • Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK <p>Java 11 Oracle Java y OpenJDK solo se requieren para SAP HANA, IBM Db2, PostgreSQL, MySQL, complementos compatibles con NetApp y otras aplicaciones personalizadas que se puedan instalar en el host de Windows.</p> <p>Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .</p> <p>Para obtener información de solución de problemas específicos de .NET, consulte "La actualización o instalación de SnapCenter falla en los sistemas heredados que no tienen conectividad a Internet."</p>

Configurar credenciales para el complemento SnapCenter para Windows

SnapCenter utiliza credenciales para autenticar a los usuarios para las operaciones de SnapCenter . Debe crear credenciales para instalar el paquete de complemento y credenciales adicionales para realizar operaciones de protección de datos en las bases de datos.

Acerca de esta tarea

Debe configurar credenciales para instalar complementos en hosts de Windows. Si bien puede crear credenciales para Windows después de implementar hosts e instalar complementos, la mejor práctica es crear credenciales después de agregar SVM, antes de implementar hosts e instalar complementos.

Configure las credenciales con privilegios de administrador, incluidos derechos de administrador en el host remoto.

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

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**.

Se muestra la ventana Credencial.

4. En la página Credencial, haga lo siguiente:

Para este campo...	Haz esto...
Nombre de la credencial	Introduzca un nombre para la credencial.
Nombre de usuario	<p>Introduzca el nombre de usuario utilizado para la autenticación.</p> <ul style="list-style-type: none">• Administrador del dominio o cualquier miembro del grupo de administradores <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:</p> <ul style="list-style-type: none">◦ NetBIOS\UserName◦ Domain FQDN\UserName <ul style="list-style-type: none">• Administrador local (sólo para grupos de trabajo) <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: UserName</p>

Para este campo...	Haz esto...
Password	Introduzca la contraseña utilizada para la autenticación.
Autenticación	Seleccione Windows como modo de autenticación.

5. Haga clic en **Aceptar**.

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 -Effectivelmmediately
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 para Exchange

Puede utilizar la página Agregar host de SnapCenter para agregar hosts de Windows. El complemento para Exchange 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 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 servicio de cola de mensajes debe estar ejecutándose.
- Si está utilizando una cuenta de servicio administrada grupal (gMSA), debe configurar gMSA con privilegios administrativos. Para obtener más información, consulte "[Configurar una cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para Microsoft Exchange Server](#)" .

Acerca de esta tarea

- No es posible agregar un servidor SnapCenter como host de complemento a otro servidor SnapCenter .
- Puede agregar un host e instalar paquetes de complementos para un host individual o para un clúster.
- Si un nodo de intercambio es parte de un DAG, no puede agregar solo un nodo al servidor SnapCenter .
- Si está instalando complementos en un clúster (DAG de Exchange), se instalan en todos los nodos del clúster incluso si algunos de ellos no tienen bases de datos en LUN de NetApp .

A partir de SnapCenter 4.6, SCE admite la función multitenencia y puede agregar un host mediante los siguientes métodos:

Agregar operación de host	4.5 y anteriores	4.6 y posteriores
Agregar DAG sin IP en dominios cruzados o diferentes	No compatible	Apoyado
Agregue varios DAG de IP con nombres únicos, que residan en el mismo dominio o en varios dominios	Apoyado	Apoyado
Agregue varios DAG con IP o sin IP que tengan los mismos nombres de host y/o nombre de base de datos en dominios cruzados	No compatible	Apoyado
Agregue varios DAG con IP/sin IP con el mismo nombre y dominio cruzado	No compatible	Apoyado
Agregue varios hosts independientes con el mismo nombre y dominio cruzado	No compatible	Apoyado

El complemento para Exchange depende del paquete de complementos de SnapCenter para Windows y las versiones deben ser las mismas. Durante la instalación del complemento para Exchange, el paquete de complementos de SnapCenter para Windows se selecciona de forma predeterminada y se instala junto con el proveedor de hardware VSS.

Si SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya están instalados y desea instalar el complemento para Exchange en el mismo servidor Exchange, debe anular el registro del proveedor de hardware VSS utilizado por SnapDrive para Windows porque es incompatible con el proveedor de hardware VSS instalado con el complemento para Exchange y el paquete de complementos de SnapCenter para Windows. Para obtener más información, consulte "["Cómo registrar manualmente el proveedor de hardware VSS de Data ONTAP"](#)" .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique 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	<p>Seleccione Windows como tipo de host.</p> <p>SnapCenter Server agrega el host y luego instala en el host el complemento para Windows y el complemento para Exchange si aún no están instalados.</p> <p>El complemento para Windows y el complemento para Exchange deben ser de la misma versión. Si previamente se instaló una versión diferente del complemento para Windows, SnapCenter actualiza la versión como parte de la instalación.</p>

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>Una dirección IP solo es compatible con hosts de dominios no confiables si se resuelve en el FQDN.</p> <p>Si está agregando un host mediante SnapCenter y es parte de un subdominio, debe proporcionar el FQDN.</p> <p>Puede ingresar direcciones IP o el FQDN de uno de los siguientes:</p> <ul style="list-style-type: none"> • Host independiente • Intercambio DAG <p>Para un DAG de Exchange, puedes:</p> <ul style="list-style-type: none"> ◦ Agregue un DAG proporcionando el nombre del DAG, la dirección IP del DAG, el nombre del nodo o la dirección IP del nodo. ◦ Agregue el clúster DAG sin IP proporcionando la dirección IP o el FQDN de uno de los nodos del clúster DAG. ◦ Agregue un DAG sin IP que resida en el mismo dominio o en uno diferente. También puedes agregar varios DAG con IP/sin IP con el mismo nombre pero con diferentes dominios. <p> Para un host independiente o un DAG de Exchange (entre dominios o del mismo dominio), se recomienda proporcionar el FQDN o la dirección IP del host o DAG.</p>

Para este campo...	Haz esto...
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>Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó.</p> <p> El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.</p>

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

Cuando selecciona Complemento para Exchange, el Complemento de SnapCenter para Microsoft SQL Server se deselecciona automáticamente. Microsoft recomienda que SQL Server y Exchange Server no se instalen en el mismo sistema debido a la cantidad de memoria utilizada y otros recursos que requiere Exchange.

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> <p> Si instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.</p>
Ruta de instalación	<p>La ruta predeterminada es C:\Program Files\NetApp\SnapCenter .</p> <p>Opcionalmente puedes personalizar la ruta.</p>
Agregar todos los hosts en el DAG	Seleccione esta casilla de verificación cuando agregue un DAG.

Para este campo...	Haz esto...
Omitir comprobaciones de preinstalación	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.
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> <p> gMSA se utilizará como una cuenta de servicio de inicio de sesión únicamente para el servicio del complemento SnapCenter para Windows.</p>

7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla "Omitir comprobaciones previas", se validará el host para determinar si cumple los requisitos para instalar el complemento. Si no se cumplen los requisitos mínimos, se mostrarán 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, 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.

Configurar un puerto personalizado para la comunicación NET TCP

De forma predeterminada, a partir de la versión 6.0 de SnapCenter , el complemento de SnapCenter para Windows utiliza el puerto 909 para la comunicación NET TCP. Si el puerto 909 está en uso, puede configurar otro puerto para la comunicación NET TCP.

Pasos

- Modifique el valor de la clave *NetTCPPort* ubicada en C:\Program Files\ NetApp\ SnapCenter\ SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config al número de puerto requerido. <add key="NetTCPPort" value="new_port_number" />
- Modifique el valor de la clave *NetTCPPort* ubicada en C:\Program Files\ NetApp\ SnapCenter\ SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config al número de puerto requerido. <add key="NetTCPPort" value="new_port_number" />
- Anule el registro del servicio *Data ONTAP VSS Hardware Provider* ejecutando el siguiente comando:

```
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u
```

Verifique que el servicio no se muestre en la lista de servicios en *services.msc*.

4. Registre el servicio *Data ONTAP VSS Hardware Provider* ejecutando el siguiente comando:

```
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"\`
```

Verifique si el servicio ahora se muestra en la lista de servicios en *services.msc*.

5. Reinicie el servicio *Plug-in para Windows*.

Instalar el complemento para Exchange desde el host del servidor SnapCenter mediante cmdlets de PowerShell

Debe instalar el complemento para Exchange desde la GUI de SnapCenter . Si no desea utilizar la GUI, puede usar cmdlets de PowerShell en el host del servidor SnapCenter o en un host remoto.

Antes de empezar

- Es necesario haber instalado y configurado SnapCenter Server.
- Debe ser un administrador local en el host o un usuario con privilegios administrativos.
- Debe ser un usuario asignado a un rol que tenga permisos de complemento, instalación y desinstalación, como el administrador de SnapCenter .
- Debe haber revisado los requisitos de instalación y los tipos de configuraciones compatibles antes de instalar el complemento para Exchange.
- El host en el que desea instalar el complemento para Exchange debe ser un host Windows.

Pasos

1. En el host del servidor SnapCenter , establezca una sesión mediante el cmdlet *Open-SmConnection* y luego ingrese sus credenciales.
2. Agregue el host en el que desea instalar el complemento para Exchange mediante el cmdlet *Add-SmHost* con los parámetros necesarios.

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](#)" .

El host puede ser un host independiente o un DAG. Si especifica un DAG, se requiere el parámetro *-IsDAG*.

3. Instale el complemento para Exchange mediante el cmdlet *Install-SmHostPackage* con los parámetros necesarios.

Este comando instala el complemento para Exchange en el host especificado y luego registra el complemento con SnapCenter.

Instale el complemento de SnapCenter para Exchange de forma silenciosa desde la línea de comandos

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

Antes de empezar

- Debes haber realizado una copia de seguridad de los recursos de Microsoft Exchange Server.
- Debe tener instalados los paquetes de complementos de SnapCenter .
- Debe eliminar la versión anterior del complemento SnapCenter para Microsoft SQL Server antes de instalarlo.

Para obtener más información, consulte "["Cómo instalar un complemento de SnapCenter de forma manual y directa desde el host del complemento"](#)" .

Pasos

1. Valide si la carpeta C:\temp existe en el host del complemento y si el usuario que inició sesión tiene acceso completo a ella.
2. Descargue el complemento de SnapCenter para Microsoft Windows desde C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

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

3. Copie el archivo de instalación en el host en el que desea instalar el complemento.
4. Desde un símbolo del sistema de Windows en el host local, navegue hasta el directorio donde guardó los archivos de instalación del complemento.
5. Introduzca el siguiente comando para instalar el complemento.

```
snapcenter_windows_host_plugin.exe"/silent /debuglog"<Ruta_del_registro_de_depuración>
/log"<Ruta_del_registro>" BI_SNAPCENTER_PORT=<Num>
SUITE_INSTALLDIR=<Ruta_del_directorio_de_instalación>
BI_SERVICEACCOUNT=<dominio\administrador> BI_SERVICEPWD=<contraseña>
ISFeatureInstall=HPPW,SCW,SCE
```

Por ejemplo:

```
C:\ProgramData\ NetApp\ SnapCenter\Repositorio de
paquetes\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log"
/log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Archivos de programa\ NetApp\
SnapCenter" BI_SERVICEACCOUNT=dominio\administrador BI_SERVICEPWD=contraseña
ISFeatureInstall=HPPW,SCW,SCE
```



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

Introduzca los siguientes valores para las 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:\RutaAlRegistro\setupexe.log"
PUERTO BI_SNAPCENTER	Especifique el puerto en el que SnapCenter se comunica con SMCore.
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.

6. Supervise el programador de tareas de Windows, el archivo de registro de instalación principal C:\Install\debug.log y los archivos de instalación adicionales en C:\Temp.
7. Supervise el directorio %temp% para verificar si los instaladores msiexe.exe están instalando el software sin errores.



La instalación del complemento para Exchange 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 deseas 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.empresia.com), el certificado contendrá todos los nombres de host del dominio implícitamente.

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del

host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

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

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



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

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

Obtenga la huella digital del certificado CA

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

Pasos

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

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

2. Realice lo siguiente desde PowerShell:

- 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
```

- 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

- 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.

Configurar SnapManager 7.x para que Exchange y SnapCenter coexistan

Para permitir que el complemento SnapCenter para Microsoft Exchange Server coexista con SnapManager para Microsoft Exchange Server, debe instalar el complemento SnapCenter para Microsoft Exchange Server en el mismo Exchange Server en el que está instalado SnapManager para Microsoft Exchange Server, deshabilitar las programaciones de SnapManager para Exchange y configurar nuevas programaciones y copias de seguridad mediante el complemento SnapCenter para Microsoft Exchange Server.

Antes de empezar

- SnapManager para Microsoft Exchange Server y SnapDrive para Windows ya están instalados, y existen copias de seguridad de SnapManager para Microsoft Exchange Server en el sistema y en el directorio SnapInfo.
- Deberías haber eliminado o recuperado las copias de seguridad realizadas por SnapManager para Microsoft Exchange Server que ya no necesitas.
- Debería haber suspendido o eliminado todas las programaciones creadas por SnapManager para Microsoft Exchange Server desde el programador de Windows.
- El complemento SnapCenter para Microsoft Exchange Server y SnapManager para Microsoft Exchange Server pueden coexistir en el mismo Exchange Server, pero no es posible actualizar instalaciones existentes de SnapManager para Microsoft Exchange Server a SnapCenter.

SnapCenter no ofrece una opción para la actualización.

- SnapCenter no admite la restauración de bases de datos de Exchange desde SnapManager para la copia de seguridad de Microsoft Exchange Server.

Si no desinstala SnapManager para Microsoft Exchange Server después de la instalación del complemento de SnapCenter para Microsoft Exchange Server y luego desea restaurar una copia de seguridad de SnapManager para Microsoft Exchange Server, debe realizar pasos adicionales.

Pasos

1. Mediante PowerShell en todos los nodos DAG, determine si el proveedor de hardware VSS de SnapDrive para Windows está registrado: `vssadmin list providers`

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
    Provider type: Hardware
    Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
    Version: 7. 1. 4. 6845
```

2. Desde el directorio SnapDrive , anule el registro del proveedor de hardware VSS de SnapDrive para Windows: `navssprv.exe -r service -u`
3. Verifique que se haya eliminado el proveedor de hardware VSS: `vssadmin list providers`
4. Agregue el host de Exchange a SnapCenter y luego instale el complemento de SnapCenter para Microsoft Windows y el complemento de SnapCenter para Microsoft Exchange Server.
5. Desde el directorio del complemento SnapCenter para Microsoft Windows en todos los nodos DAG, verifique que el proveedor de hardware VSS esté registrado: `vssadmin list providers`

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
    Provider type: Hardware
    Provider Id: {31fcfa584-72be-45b6-9419-53a3277301d1}
    Version: 7. 0. 0. 5561
```

6. Detener las programaciones de copia de seguridad de SnapManager para Microsoft Exchange Server.
7. Usando la GUI de SnapCenter , cree copias de seguridad a pedido, configure copias de seguridad programadas y configure ajustes de retención.
8. Desinstalar SnapManager para Microsoft Exchange Server.

Si no desinstala SnapManager para Microsoft Exchange Server ahora y más tarde desea restaurar una copia de seguridad de SnapManager para Microsoft Exchange Server:

- a. Anular el registro del complemento de SnapCenter para Microsoft Exchange Server en todos los nodos DAG: `navssprv.exe -r service -u`

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. Desde el directorio `C:\Archivos de programa\ NetApp\ SnapDrive\`, registre SnapDrive para Windows en todos los nodos DAG: `navssprv.exe -r service -a hostname\username -p password`

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.