



Preparar la instalación de complementos compatibles con NetApp

SnapCenter software

NetApp
January 09, 2026

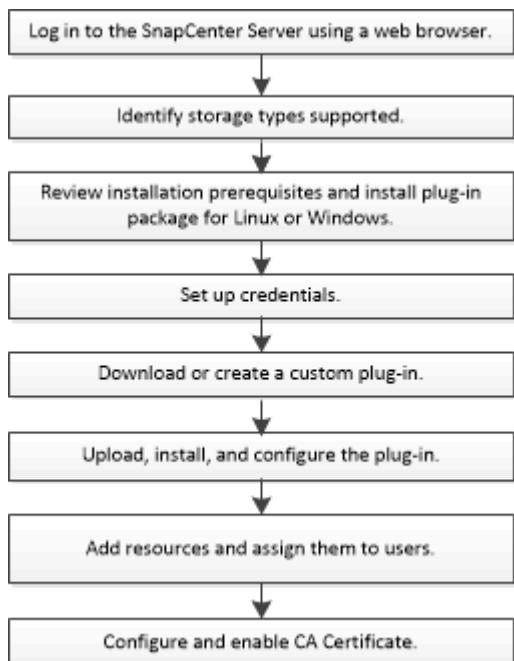
Tabla de contenidos

Preparar la instalación de complementos compatibles con NetApp	1
Flujo de trabajo de instalación de plugins compatibles con SnapCenter NetApp	1
Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX	1
Generales.....	2
Host Windows	2
Hosts Linux y AIX	2
Requisitos del host AIX	3
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows	6
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux y AIX	7
Configure credenciales para plugins compatibles con NetApp	8
Configurar GMSA en Windows Server 2016 o posterior	10
Instale los complementos compatibles con NetApp	11
Añada hosts e instale paquetes de plugins en hosts remotos	11
Instale paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts remotos mediante cmdlets	15
Instale los plugins compatibles con NetApp en los hosts Linux mediante la interfaz de línea de comandos.....	16
Supervise el estado de instalación de los plugins compatibles con NetApp	17
Configurar certificado de CA	17
Genere un archivo CSR de certificado de CA	17
Importar certificados de CA	18
Obtenga la huella digital del certificado de CA	19
Configure el certificado de CA con servicios de plugins de host de Windows	19
Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host Linux ..	20
Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host de Windows	22
Habilite certificados de CA para plugins	25

Preparar la instalación de complementos compatibles con NetApp

Flujo de trabajo de instalación de plugins compatibles con SnapCenter NetApp

Deber instalar y configurar plugins compatibles con SnapCenter NetApp si desea proteger los recursos de plugins compatibles con NetApp.



Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos. Los plugins compatibles con NetApp son compatibles con entornos Windows, Linux y AIX.



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

- Debe haber instalado Java 11 en el host Linux, Windows o AIX.



IBM Java no es compatible con el host Windows y Linux.

- Al instalar un plugin 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.
- Los complementos compatibles con NetApp, como MongoDB, ORASCPM, aplicaciones Oracle, SAP ASE, SAP MaxDB y el complemento de almacenamiento deben estar disponibles en el host del cliente desde el que se ejecuta la operación de añadir host.

Generales

Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.

Host Windows

- Debe tener un usuario de dominio 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 seleccionar manualmente el plugin de SnapCenter para Microsoft Windows.

["Descargar JAVA para Windows"](#)

Hosts Linux y AIX



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

Si utiliza Windows Server 2019 o Windows Server 2016 para el host de SnapCenter Server, debe instalar Java 11.

["Descargar JAVA para Linux"](#)

["Descargar JAVA para AIX"](#)

- Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux.



Asegúrese de utilizar sudo versión 1.8.7 o posterior.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt si el servidor SnapCenter está instalado en el host de Windows.
- /opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt si el servidor SnapCenter está instalado en el host Linux.



Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

Requisitos del host AIX

Debe asegurarse de que el host cumpla los requisitos antes de instalar el paquete de plugins de SnapCenter para AIX.



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.



El plugin de SnapCenter para UNIX que forma parte del paquete de plugins de SnapCenter para AIX, no admite grupos de volúmenes concurrentes.

Elemento	Requisitos
Sistemas operativos	AIX 7,1 o posterior

Elemento	Requisitos
RAM mínima para el plugin de SnapCenter en el host	4 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	<p>2 GB</p> <p></p> <p>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.</p>
Paquetes de software obligatorios	<p>Java 11 IBM Java</p> <p>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.</p>

Configure privilegios sudo para usuarios que no son raíz para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para AIX e inicie el proceso del plugin. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

Lo que necesitará

- Sudo versión 1.8.7 o posterior.
- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos de código de autenticación de mensajes: Macs hmac-sha2-256 y MACs hmac-sha2-512.

Reinic peace el servicio sshd después de actualizar el archivo de configuración.

Ejemplo:

```

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256

```

Acerca de esta tarea

Tiene que configurar los privilegios sudo para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- /Home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl
- Pasos*
 1. Inicie sesión en el host AIX en el que desee instalar el paquete de plugins de SnapCenter para AIX.
 2. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de Linux.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo /etc/oracle/olr.loc.

AIX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt si el servidor SnapCenter está instalado en el host de Windows.
- /opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt si el servidor SnapCenter está instalado en el host Linux.



Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

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	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) Hosting Bundle • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK <p>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.""</p>

Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux y AIX

Debe asegurarse de que el host cumpla los requisitos antes de instalar el paquete de plugins de SnapCenter para Linux o AIX.



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

Elemento	Requisitos
Sistemas operativos	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
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	<p>2 GB</p> <p></p> <p>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.</p>

Elemento	Requisitos
Paquetes de software obligatorios	<p>Java 11 Oracle Java u OpenJDK</p> <p>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.</p>

Para obtener la información más reciente sobre las versiones compatibles, consulte "["Herramienta de matriz de interoperabilidad de NetApp"](#)

Configure credenciales para plugins compatibles con NetApp

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.

Antes de empezar

- Hosts Linux o AIX

Debe configurar credenciales para instalar plugins en hosts Linux o AIX.

Debe configurar las credenciales para el usuario raíz o un usuario que no sea raíz que tenga privilegios sudo para instalar e iniciar el proceso del plugin.

Práctica recomendada: aunque se permite crear credenciales para Linux después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

- Host Windows

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.

- Aplicaciones de complementos compatibles con NetApp

El plugin utiliza las credenciales seleccionadas o creadas al añadir un recurso. Si un recurso no requiere credenciales durante las operaciones de protección de datos, puede establecer las credenciales como **Ninguno**.

Acerca de esta tarea

Si se configuran las 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 backup al nombre de 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**, especifique la información necesaria para configurar las credenciales:

Para este campo...	Realice lo siguiente...
Nombre de credencial	Introduzca un nombre para las credenciales.
Nombre de usuario	<p>Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.</p> <ul style="list-style-type: none">• Administrador de dominio o cualquier miembro del grupo de administradores <p>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:</p> <ul style="list-style-type: none">◦ <i>NetBIOS\Username</i>◦ <i>Domain FQDN\Username</i> <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 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: <i>Username</i></p>
Contraseña	Introduzca la contraseña usada para autenticación.
Tipo de autenticación	Seleccione el tipo de autenticación que desea usar.
Use privilegios sudo	Seleccione la casilla de verificación Use sudo Privileges si va a crear credenciales para usuarios que no son raíz.  Aplicable únicamente a usuarios Linux y AIX.

5. Haga clic en **Aceptar**.

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

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 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.

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 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>`
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.

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 los complementos compatibles con NetApp

Añada hosts e instale paquetes de plugins en hosts remotos

Debe usar la página SnapCenter Add Host para añadir hosts y, a continuación, instalar los paquetes de los plugins. Los plugins se instalan automáticamente en hosts remotos. Puede añadir un host e instalar los paquetes de los plugins para un host individual o para un clúster.

Antes de empezar

- 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.
- Debe asegurarse de que el servicio de cola de mensajes está 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 2016 o posterior para aplicaciones personalizadas"](#)

- Para el host de Windows, debe asegurarse de seleccionar el plugin de SnapCenter para Windows.

Acerca de esta tarea

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Si instala plugins en un clúster (WSFC), los plugins se instalan en todos los nodos del clúster.

Pasos

1. En el panel de navegación izquierdo, seleccione **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página hosts, realice las siguientes acciones:

Para este campo...	Realice lo siguiente...
Tipo de host	<p>Seleccione el tipo de host:</p> <ul style="list-style-type: none"> • Windows • Linux • AIX <p> Los plugins compatibles con NetApp se pueden utilizar en entornos de Windows, Linux y AIX.</p> <p> El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.</p>
Nombre de host	<p>Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.</p> <p>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.</p> <p>En los entornos de Windows, la dirección IP es compatible con los hosts de dominio que no son de confianza solo si se resuelve en el FQDN.</p> <p>Puede introducir las direcciones IP o el FQDN de un host independiente.</p> <p>Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar el FQDN.</p>

Para este campo...	Realice lo siguiente...
Credenciales	<p>Seleccione el nombre de la credencial que ha creado o cree nuevas credenciales.</p> <p>Las credenciales deben tener derechos de administración en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales.</p> <p>Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado.</p> <p> El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host.</p>

5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.

Puede instalar los siguientes plugins de la lista:

- MongoDB
- ORASCPM (se muestra como Aplicaciones Oracle)
- SAP ASE
- MaxDB de SAP
- Reducida

6. (Opcional) Seleccione **Más opciones** para instalar los otros plug-ins.

Para este campo...	Realice lo siguiente...
Puerto	<p>Conserve 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 ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error.</p>

Para este campo...	Realice lo siguiente...
Ruta de instalación	<p>Los plugins compatibles con NetApp pueden instalarse en sistemas Windows o Linux.</p> <ul style="list-style-type: none"> En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. <p>Opcionalmente, puede personalizar la ruta.</p> <ul style="list-style-type: none"> Para el paquete de plugins de SnapCenter para Linux y el paquete de plugins de SnapCenter para AIX, la ruta predeterminada es /opt/NetApp/snapcenter. <p>Opcionalmente, puede personalizar la ruta.</p>
Omitir comprobaciones previas a la instalación	<p>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.</p>
Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in	<p>En el caso de host de Windows, seleccione esta casilla de comprobación si desea utilizar una cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de plugin.</p> <p> Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName\$.</p> <p> GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows.</p>

7. Seleccione 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, 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 SnapManager.web.ui.dll.config, debe actualizar el archivo en ambos nodos y reiniciar el grupo de aplicaciones de SnapCenter.

La ruta predeterminada de Windows es C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

La ruta predeterminada de Linux es

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. Si el tipo de host es Linux, verifique la huella dactilar y, a continuación, seleccione **Confirmar y Enviar**.



La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

9. Supervise el progreso de la instalación.

Los archivos de registro específicos de la instalación se encuentran en
/custom_location/snapcenter/ registros.

Instale paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

Antes de empezar

El usuario que agrega un host debe tener derechos administrativos en el host.



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

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 en varios hosts 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*. Alternativamente, también puede consultar la "[Guía de referencia de cmdlets de SnapCenter Software](#)".

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

4. Introduzca sus credenciales para la instalación remota.

Instale los plugins compatibles con NetApp en los hosts Linux mediante la interfaz de línea de comandos

Debe instalar los plugins compatibles de NetApp mediante la interfaz de usuario (UI) de SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar los complementos compatibles con NetApp en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

Pasos

1. Copie el archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar los plugins compatibles de NetApp.

Puede acceder a esta ruta desde el host en el que está instalado el servidor SnapCenter.

2. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el archivo de instalación.
3. Instale el plugin: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT indica el puerto de comunicación HTTPS de SMCore.
 - -DSERVER_IP indica la dirección IP del servidor SnapCenter.
 - -DSERVER_HTTPS_PORT indica el puerto HTTPS del servidor SnapCenter.
 - -DUSER_INSTALL_DIR indica el directorio en el que desea instalar el paquete de plugins de SnapCenter para Linux.
 - _DINSTALL_LOG_NAME indica el nombre del archivo de registro.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
_DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Añada el host al servidor de SnapCenter con el cmdlet Add-Smhost y los parámetros requeridos.

La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando `Get-Help nombre_comando`. Alternativamente, también puede consultar la "[Guía de referencia de cmdlets de SnapCenter Software](#)".

5. Inicie sesión en SnapCenter y cargue el plugin compatible con NetApp desde la interfaz de usuario de o mediante cmdlets de PowerShell.

En la sección, puede cargar el plugin compatible con NetApp desde la interfaz de usuario "[Añada hosts e instale paquetes de plugins en hosts remotos](#)" .

La ayuda sobre cmdlet de SnapCenter y la información de referencia sobre cmdlet contienen más información acerca de cmdlets de PowerShell.

Supervise el estado de instalación de los plugins compatibles con NetApp

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 solo se enumeren las operaciones de instalación de 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**.

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.



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

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 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: "a90d82dd82a41433e6f83886b00d4277a32a7b".

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"
```

Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host Linux

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en `/opt/NetApp/snapcenter/scc/etc` como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

Es el valor correspondiente a la clave 'KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña para todos los alias de las entradas de clave
privada en el almacén de claves por la misma contraseña utilizada para
el almacén de claves:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para el archivo key KEYSTORE_PASS en `agent.properties`.

3. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento:
/opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Añada un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

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

Pasos

1. Navegue a la carpeta que contiene el almacén de claves del complemento
/opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado de CA con clave pública y privada.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados añadidos al almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se

añadió al almacén de claves.

7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

La contraseña del almacén de claves del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
. Si el nombre del alias del certificado de CA es largo y contiene espacio o caracteres especiales ("*",","), cambie el nombre del alias por un nombre simple:
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configure el nombre del alias del certificado de CA en el archivo agent.properties.
```

Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

8. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para complementos

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos de SnapCenter es 'opt/NetApp/snapcenter/scc/etc/crl'.

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host de Windows

Debe administrar la contraseña del almacén de claves de los complementos y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de los complementos y configurar el par de claves firmadas de CA para el almacén de confianza de los complementos con el servicio de complementos de SnapCenter para activar el certificado digital instalado.

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en C:\Program

Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves del complemento y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del complemento desde el archivo de propiedades del agente del complemento.

Es el valor que corresponde a la clave *KEYSTORE_PASS*.

2. Cambie la contraseña del almacén de claves:

```
keytool -storepasswd -keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool por su ruta completa.

```
C:\Archivos de programa\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore.jks
```

3. Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves:

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Actualice lo mismo para el archivo key *KEYSTORE_PASS* en *agent.properties*.

4. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves del complemento y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para conectar el almacén de confianza

Debe configurar los certificados raíz o intermedios sin la clave privada para conectar el almacén de confianza.

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore.jks
```

4. Añada un certificado raíz o intermedio:

```
Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.



Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc
2. Busque el archivo *keystore.jks*.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore.jks
```

4. Agregue el certificado de CA con clave pública y privada.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore.jks -deststoretype JKS
```

5. Enumere los certificados añadidos al almacén de claves.

```
keytool -list -v -keystore.jks
```

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

La contraseña del almacén de claves del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos de SnapCenter

Acerca de esta tarea

- Para descargar el último archivo CRL del certificado de CA relacionado, consulte "[Cómo actualizar el archivo de lista de revocación de certificados en el certificado de CA de SnapCenter](#)".
- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos de SnapCenter es 'C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'.

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la CLAVE CRL_PATH.
2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán en cada CRL.

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.

Antes de empezar

- 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`. Alternativamente, 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.

Información de copyright

Copyright © 2026 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.