Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-48/protect-hana/task_install_snapcenter_plug_in_for_sap_hana_database.html on September 26, 2025. Always check docs.netapp.com for the latest.

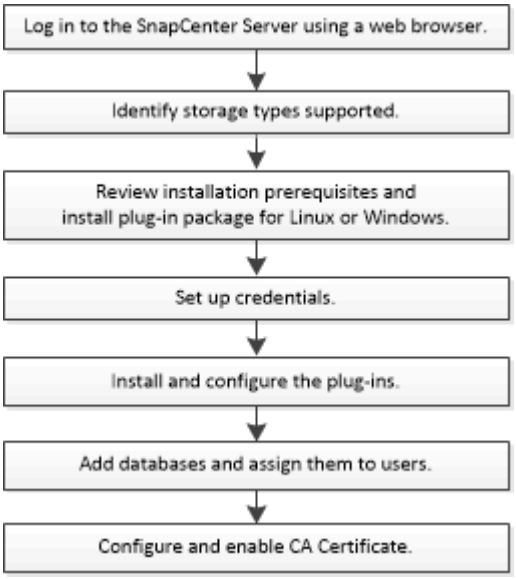
Tabla de contenidos

Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA . . . 1
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA . . . 1
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA . . . 1
Host Windows . . . 2
Hosts Linux . . . 2
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 2
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 3
Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA . . . 4
Configurar GMSA en Windows Server 2012 o posterior . . . 7
Instale el plugin de SnapCenter para base de datos SAP HANA . . . 8
Añada hosts e instale paquetes de plugins en hosts remotos . . . 8
Instale paquetes de plugins de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets . . . 12
Instale el plugin de SnapCenter para base de datos SAP HANA en hosts Linux mediante la interfaz de la línea de comandos . . . 12
Supervise el estado de la instalación del plugin para SAP HANA . . . 13
Configurar certificado de CA . . . 14
Genere un archivo CSR de certificado de CA . . . 14
Importar certificados de CA . . . 14
Obtenga la huella digital del certificado de CA . . . 15
Configure el certificado de CA con servicios de plugins de host de Windows . . . 16
Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Linux . . . 17
Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Windows . . . 19
Habilite certificados de CA para plugins . . . 22

Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA

Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA

Debe instalar y configurar el plugin de SnapCenter para base de datos SAP HANA si desea proteger las bases de datos SAP HANA.



Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. Plugin SnapCenter para base de datos SAP HANA está disponible en entornos Windows y Linux.

- Debe haber instalado Java 1.8 64 bit en su host.

  IBM Java no es compatible.

- Debe haber instalado el terminal interactivo de base de datos SAP HANA (cliente HDBSQL) en el host.
- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows "'LocalSystem'", que es el comportamiento predeterminado cuando el plugin para base de datos SAP HANA se instala como administrador de dominio.
- Para Windows, se deben crear claves de almacenamiento como usuario SYSTEM.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host. El plugin de SnapCenter para Microsoft Windows se pondrá en marcha de forma predeterminada con el plugin de SAP HANA en hosts Windows.

- Para host Linux, se accede a las claves de almacenamiento de usuario seguro HDB como usuario de sistema operativo HDBSQL.
- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host de base de datos SAP HANA.

Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Cuando se instala el plugin para base de datos SAP HANA en un host Windows, el plugin de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 1.8 64 bit en su host de Windows.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

Hosts Linux

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 1.8 64 bit en su host Linux.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

- Para bases de datos SAP HANA que se ejecutan en un host Linux, mientras se instala el plugin para base de datos SAP HANA, el plugin de SnapCenter para UNIX se instala automáticamente.

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

Elemento	Requisitos
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	5 GB Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.
Paquetes de software obligatorios	• Microsoft .NET Framework 4.7.2 o posterior • Windows Management Framework (WMF) 4.0 o posterior • PowerShell 4.0 o posterior Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

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

Antes de instalar el paquete de plugins de SnapCenter para Linux, tiene que conocer bien algunos requisitos básicos de espacio y tamaño del sistema host.

Elemento	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) 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

Elemento	Requisitos
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 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, según la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.
Paquetes de software obligatorios	Tipos Java 1.8.x (64 bits)Oracle Java y OpenJDK 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. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA

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.

Acerca de esta tarea

- Hosts Linux

  Debe configurar credenciales para instalar plugins en hosts Linux.

  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

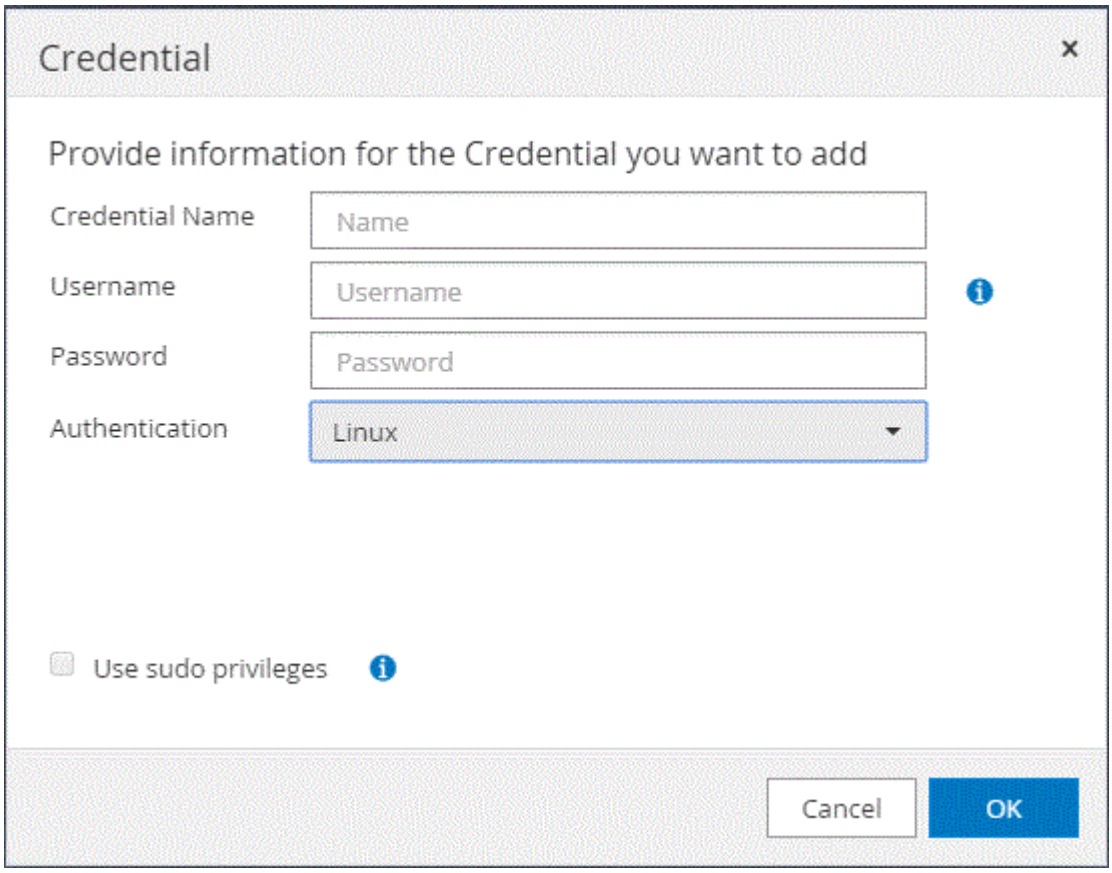
Debe configurar credenciales de Windows antes de instalar plugins.

Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.

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.

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

5. Haga clic en **Aceptar**.

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

Configurar GMSA en Windows Server 2012 o posterior

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

Lo que necesitará

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

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

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

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

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

   Para ello, ejecute el siguiente comando desde PowerShell:

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

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


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

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie el host.

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

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

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

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

Instale el plugin de SnapCenter para base de datos SAP HANA

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 paquetes de plugins para un host individual o para un clúster.

Lo que necesitará

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.

- Debe asegurarse de que el servicio de cola de mensajes está en ejecución.
- La documentación de administración contiene información sobre la gestión de los hosts.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configure la cuenta de servicio gestionado de grupo en Windows Server 2012 o posterior para SAP HANA"

Acerca de esta tarea

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Para que la replicación de sistemas SAP HANA detecte recursos en los sistemas primarios y secundarios, se recomienda añadir los sistemas primario y secundario mediante el usuario root o sudo.
- Pasos*

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

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione el tipo de host: • Windows • Linux El plugin para SAP HANA está instalado en el host de cliente de HDBSQL, y este host puede estar en un sistema Windows o Linux.
Nombre de host	Introduzca el nombre de host de comunicación. Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN. Debe configurar al cliente de HDBSQL y a HDBUserStore en este host.

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

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) haga clic en **más opciones**.

Para este campo…	Realice lo siguiente…
Puerto	Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado. Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error.
Ruta de instalación	El plugin para SAP HANA está instalado en el host de cliente de HDBSQL, y este host puede estar en un sistema Windows o Linux. • En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta. • Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta.

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

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

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

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

8. Si el tipo de host es Linux, verifique la huella digital y, a continuación, haga clic en **Confirmar y enviar**.

   En una configuración de clúster, debe comprobar la huella de cada uno de los nodos del clúster.

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

1. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación están en /custom_location/snapcenter/logs.

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

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

Lo que necesitará

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

- Pasos*

  1. Inicie PowerShell.
  2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
  3. Instale el plugin 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 -skipprecheck cuando haya instalado los plugins manualmente y no quiera validar si el host cumple los requisitos para instalar el plugin.

  1. Introduzca sus credenciales para la instalación remota.

Instale el plugin de SnapCenter para base de datos SAP HANA en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para base de datos SAP HANA mediante la interfaz de usuario de SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar el plugin para base de datos SAP HANA en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

Lo que necesitará

- Debe instalar el plugin para base de datos SAP HANA en cada host Linux en el que resida el cliente HDBSQL.
- El host Linux en el que se instala el plugin de SnapCenter para base de datos SAP HANA debe cumplir con los requisitos dependientes de software, base de datos y sistema operativo.

  La herramienta de matriz de interoperabilidad (IMT) contiene la última información sobre las configuraciones soportadas.

  "Herramienta de matriz de interoperabilidad de NetApp"

- El plugin de SnapCenter para base de datos SAP HANA forma parte del paquete de plugins de SnapCenter para Linux. Antes de instalar el paquete de plugins de SnapCenter para Linux, debe haber instalado SnapCenter en un host de Windows.

- Pasos*

1. Copie el paquete de plugins de SnapCenter para el archivo de instalación de Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar el plugin para la base de datos SAP HANA.

   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
```

1. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y añada el parámetro PLUGINS_ENABLED = hana:3.0.
2. 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".

Supervise el estado de la instalación del plugin para SAP HANA

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

Acerca de esta tarea

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

- En curso
- Completado correctamente
- Error

- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página Monitor, haga clic en **Jobs**.
  3. En la página Jobs, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de plugins, proceda como sigue:
     a. Haga clic en **filtro**.
     b. Opcional: Indique las fechas de inicio y finalización.
     c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
     d. En el menú desplegable de estado, seleccione el estado de instalación.
     e. Haga clic en **aplicar**.
  4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Configurar certificado de CA

Genere un archivo CSR de certificado de CA

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

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

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

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

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

Importar certificados de CA

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

- Pasos*
  1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** >

Agregar o quitar Snapin.

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

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

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

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

Obtenga la huella digital del certificado de CA

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

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

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

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

    Get-ChildItem -Path Cert:\LocalMachine\My

    b. Copie la huella digital.

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

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

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

- Pasos*

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

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

    Por ejemplo:

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

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

    Por ejemplo:

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

Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Linux

Debe gestionar la contraseña del almacén de claves de plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados intermedios o raíz para el almacén de confianza de los plugins personalizados, y configurar la pareja de claves firmadas de CA como almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* tanto como en su almacén de confianza como en su almacén de claves.

Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

- Pasos*

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

   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 de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

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

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado: /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 en el almacén de confianza del plugin personalizado.
```

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

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado /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 predeterminada del plugin personalizado keystore es el valor de key 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 firmado de CA en el almacén de confianza del plugin personalizado.

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

Acerca de esta tarea

- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados 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 SAP HANA de SnapCenter en el host Windows

Debe gestionar la contraseña del almacén de claves de plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados intermedios o raíz para el almacén de confianza de los plugins personalizados, y configurar la pareja de claves firmadas de CA como almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*, tanto como su almacén de confianza como su almacén de claves.

Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

- Pasos*

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

   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*.

1. Reinicie el servicio después de cambiar la contraseña.

   > La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

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

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\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 en el almacén de confianza del plugin personalizado.

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

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\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 predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

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

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

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

2. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

Configurar la lista de revocación de certificados (CRL) para los plugins personalizados 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 personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados 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.

Lo que necesitará

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

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. 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 © 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.