Establecer una conexión segura

entre Exchange Reporter Plus y MS SQL

ManageEngine
Exchange Reporter Plus

Resumen del documento

Exchange Reporter Plus admite una base de datos MS SQL externa además de la base de datos PostgreSQL incluida. Este documento está dirigido a los administradores que deseen proteger la conexión entre su base de datos MS SQL y Exchange Reporter Plus con un certificado SSL. Al aplicar un certificado SSL en MS SQL Server, puede asegurarse de que los datos transferidos entre Exchange Reporter Plus y SQL Server se cifran y permanecen seguros durante la transmisión.

Nota: Esta guía es para usuarios que ya han migrado a la base de datos MS SQL. En caso de que esté utilizando una base de datos PostgreSQL o MySQL, asegúrese de migrar primero a un servidor MS SQL.

Prerrequisitos

- Necesitará un certificado SSL válido en formato PFX que no caduque pronto. Si tiene un certificado en otro formato, conviértalo en un archivo PFX. Para crear un certificado auto-firmado utilizando IIS, siga los pasos que se mencionan aquí.
- El **Nombre común** en el campo Sujeto del certificado debe coincidir con el nombre de dominio completo (FQDN) del equipo en el que está instalado MS SQL Server.
- El certificado debe emitirse para la autenticación del servidor, por lo que la propiedad Uso mejorado de claves del certificado debe incluir **Autenticación del servidor (1.3.6.1.5.5.7.3.1).**

Los pasos para comprobar si su certificado cumple estos requisitos se enumeran aquí.

Importante: Si ya aplicó un certificado SSL válido (que cumpla los requisitos indicados en la sección de Prerrequisitos) en su servidor SQL, puede comenzar en el Paso 3.

Paso 1

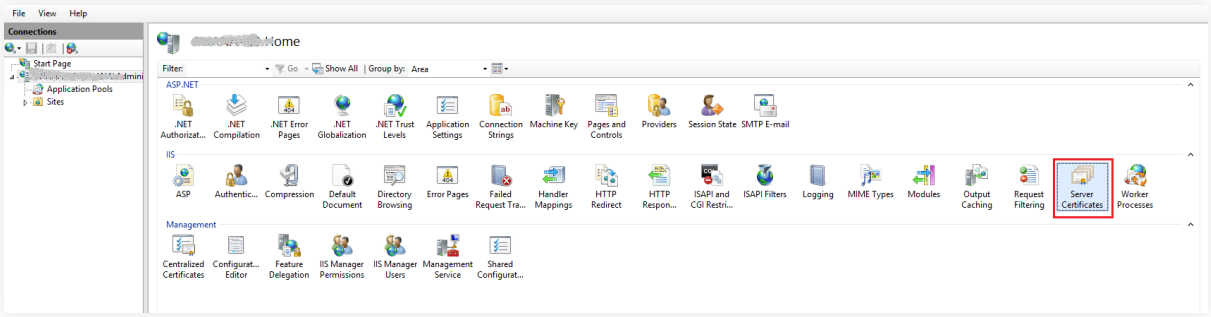
Importar el certificado al almacén de certificados

Si está utilizando un certificado SSL auto-firmado generado mediante Internet Information Services (IIS) Manager, puede empezar en el Paso 2.

Si utiliza un certificado generado a través de otros modos, primero deberá importarlo al almacén de certificados de SQL Server. Puede importar el certificado utilizando IIS Manager o el complemento de Microsoft Management Console (MMC).

Importar el certificado usando IIS Manager

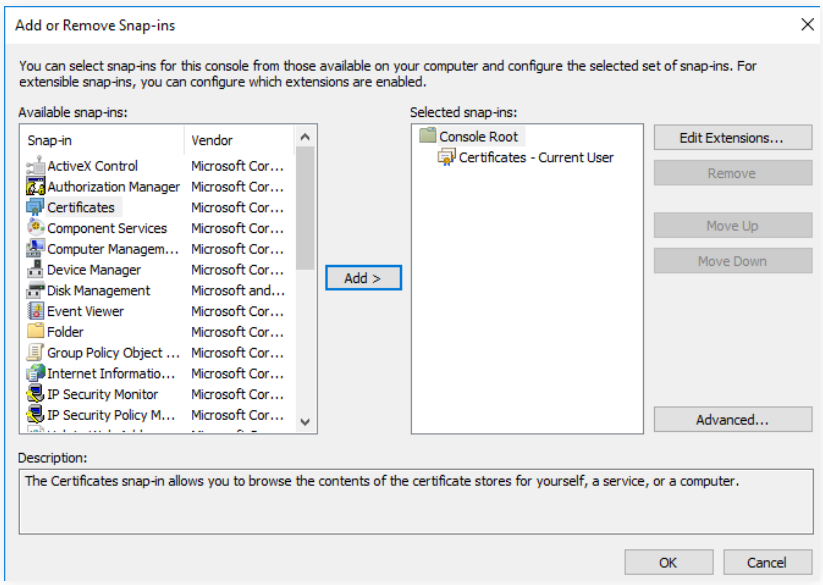
1. Abra **IIS Manager.**
2. Haga clic en el nombre del servidor en la columna Conexiones del panel izquierdo. En la fila central de iconos, haga doble clic en **Certificados del servidor.**



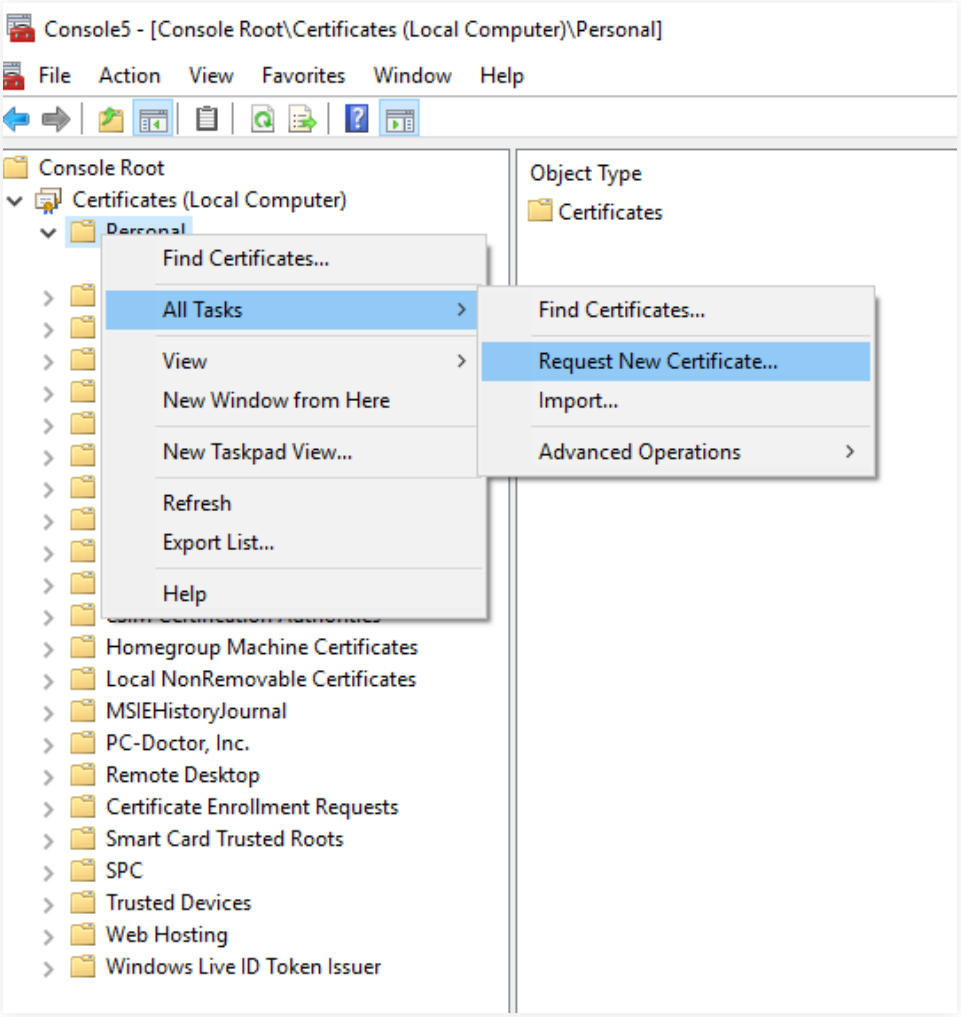
3. Haga clic en **Importar** en el panel Acciones.
4. Busque y seleccione el **Archivo de certificado PFX.**
5. Ingrese la **contraseña** que utilizó al generar el archivo de certificado.
6. Haga clic en **Aceptar.**

Importar el certificado usando MMC

1. Abra **MMC.**
2. En el menú Archivo, haga clic en **Agregar o quitar** complementos.
3. Seleccione **Certificados**, y luego haga clic en **Agregar.**



4. Se le pedirá que abra el complemento para su cuenta de usuario, la cuenta de servicio o la cuenta de equipo. Seleccione la **Cuenta de equipo.**
5. Seleccione **Equipo local,** y luego haga clic en **Finalizar.**
6. Haga clic en **Aceptar** para salir de la ventana **Agregar o quitar complementos.**
7. De vuelta en MMC, haga doble clic en **Certificados (Equipo local)** para expandir la vista en árbol.
8. Haga clic derecho en **Personal**, y luego seleccione **Todas las tareas > Solicitar un nuevo certificado...**

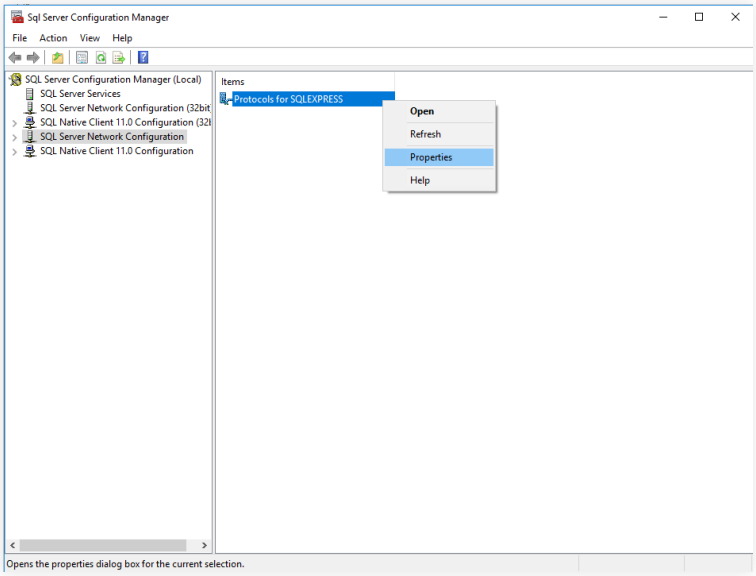


9. Haga clic en **Siguiente** en el Asistente de solicitud de certificados que se abre.
10. Seleccione **Equipo** como el tipo de certificado.
11. Puede ingresar un nombre en el cuadro de texto o dejarlo en blanco. A continuación, complete el asistente haciendo clic en **Inscribir y Finalizar.**

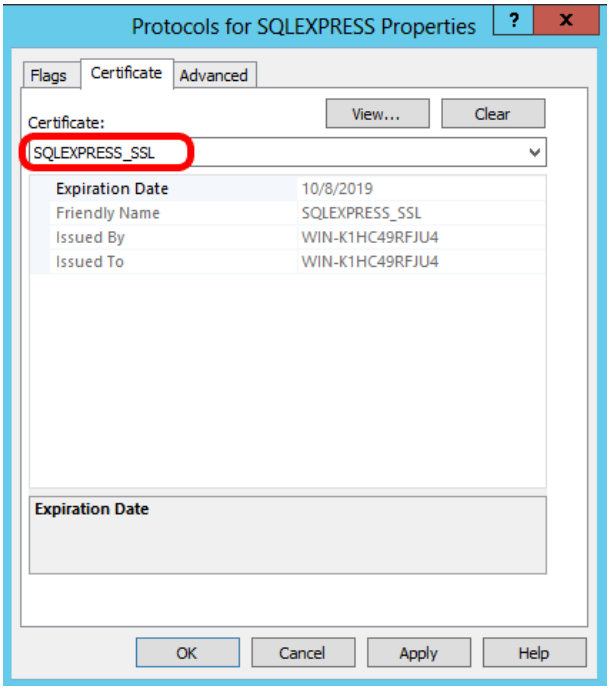
Paso 2

Asociar el certificado con MS SQL Server

1. Abra el **Administrador de configuración de SQL Server.**
2. Expanda **Configuración de red de SQL Server** y haga clic derecho en **Protocolos** para la instancia de MS SQL Server que desea asociar con el certificado. Haga clic en **Propiedades.**



3. En la pestaña Marcadores, seleccione **Sí** en la casilla **Forzar cifrado.**
4. En la pestaña **Certificado,** seleccione el certificado que desea utilizar.



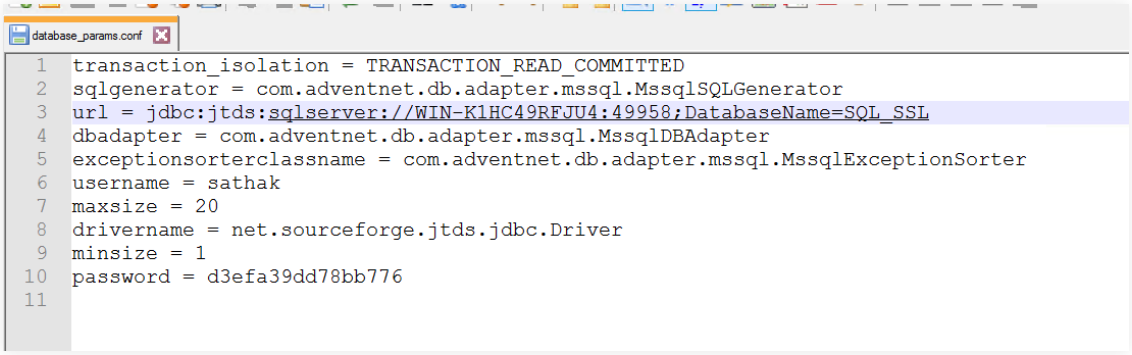
5. Haga clic en **Aceptar.**
6. Reinicie SQL Server.

Paso 3

Configurar Exchange Reporter Plus

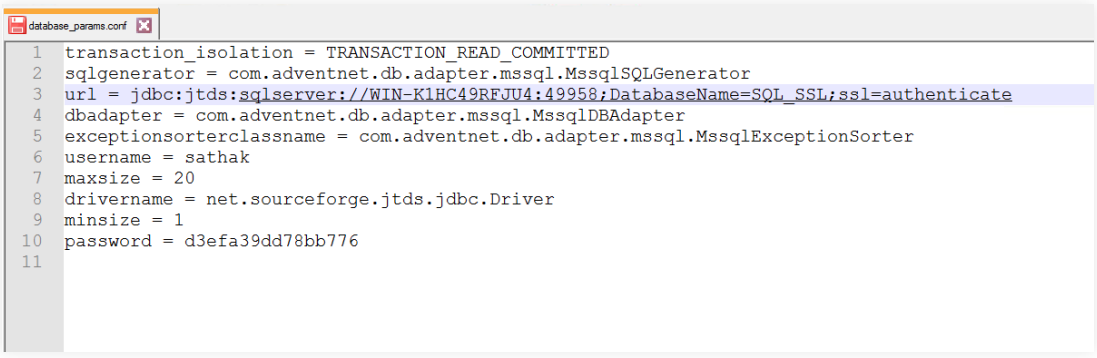
Después de asociar el certificado con SQL Server, deberá configurar Exchange Reporter Plus para que utilice la conexión segura con la base de datos. Siga los pasos que se indican a continuación:

1. Vaya a la carpeta de inicio de Exchange Reporter Plus (<install_dir>\conf) y abra el archivo database_params.conf en un editor de texto. La ruta de instalación predeterminada es C: \ManageEngine\ Exchange Reporter Plus. Aquí verá una lista de entradas como **inicio de sesión, contraseña y url.**



2. Bajo la entrada url, añada **ssl=authenticate** al valor de la URL.

   Por ejemplo, si la entrada existente es:
   url=jdbc:jtds:sqlserver://WIN-K1HC49RFJU4:49958;DatabaseName=SQL_SSL Entonces cámbiela por:
   url=jdbc:jtds:sqlserver://WIN-K1HC49RFJU4:49958;DatabaseName=SQL_SSL;**ssl=authenticate**



3. En la misma carpeta \conf, abra **wrapper.conf** en un editor de texto.
4. Busque **wrapper.java.additional.** Obtendrá una lista de entradas numeradas empezando por 1.
5. Añada la siguiente línea después de la última entrada wrapper.java.additional.

   "wrapper.java.additional.xx=-Djsse.enableCBCProtection=false"

   Aquí **xx** denota el valor siguiente al entero de la línea precedente.

   Por ejemplo:

   wrapper.java.additional.1=-Dcatalina.home=..

   wrapper.java.additional.2=-Dserver.home=..

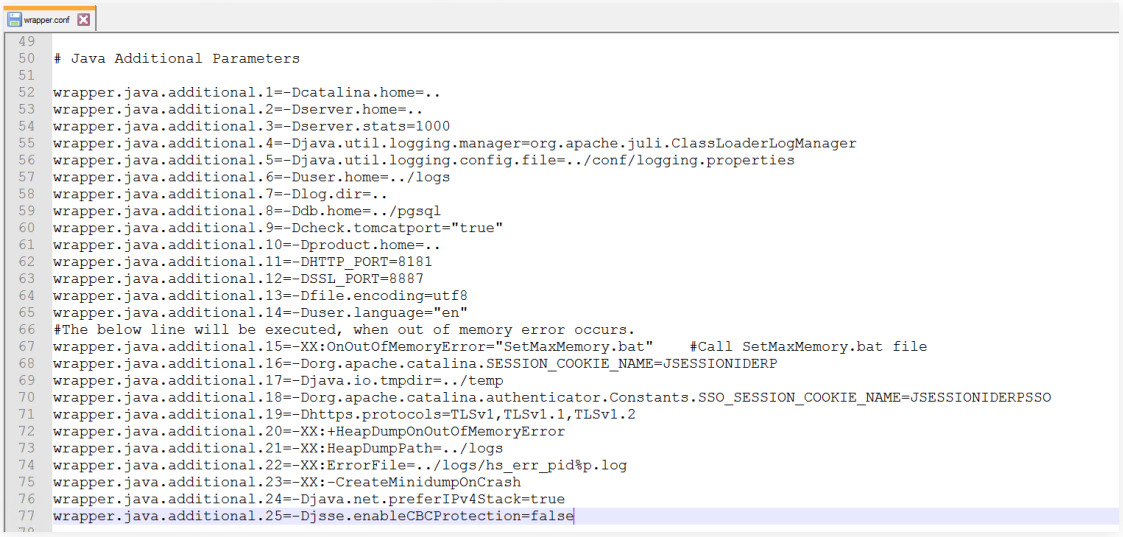
   wrapper.java.additional.3=-Dserver.stats=1000

   ...

   ...

   wrapper.java.additional.12=-DSSL_PORT=8887

   wrapper.java.additional.13=-Djsse.enableCBCProtection=false



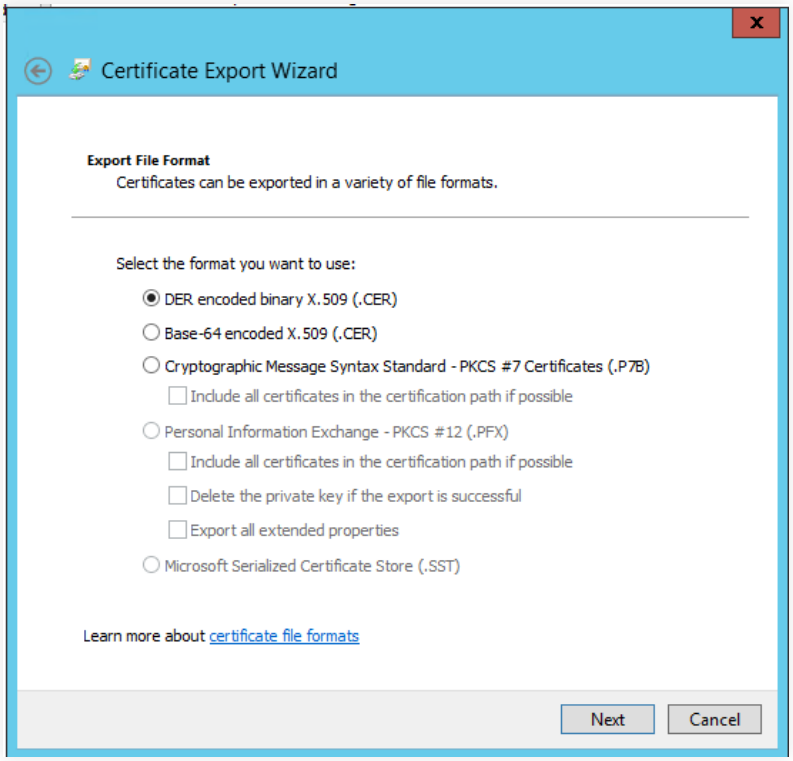
6. Reinicie Exchange Reporter Plus para que los cambios surtan efecto.

Paso 4

Asociar el certificado con el almacén de claves Java

Debe asociar el certificado al almacén de claves Java de Exchange Reporter Plus para establecer la confianza. Siga los pasos que se indican a continuación en el equipo en el que está instalado Exchange Reporter Plus:

1. Abra **IIS Manager.**
2. En el panel central, haga clic en **Certificados del servidor.**
3. Abra el certificado que desea utilizar.
4. Haga clic en la pestaña **Detalles.**
5. Haga clic en **Copiar a archivo.**
6. Haga clic en **Siguiente** en el Asistente para la exportación de certificados que se abre.
7. En la pantalla Exportar clave privada, seleccione **No, no exportar la clave privada,** y haga clic en **Siguiente.**
8. En la pantalla Formato del archivo de exportación, seleccione **DER binario codificado X.509 (.CER)** o **Base-64 codificado X.509 (.CER)**, y haga clic en **Siguiente.**

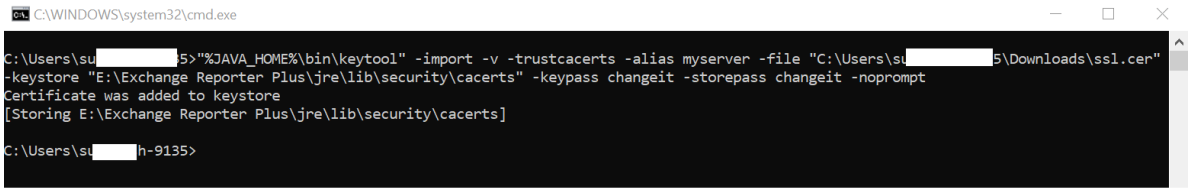


9. Ingrese un nombre para el archivo y haga clic en **Siguiente.**

10. Haga clic en **Finalizar.**

11. Utilice el siguiente comando para asociar el certificado al almacén de claves Java:

“%JAVA_HOME%\bin\keytool" -import -v -trustcacerts -alias myserver -file ssl.cer -keystore "%JAVA_HOME%\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt



Apéndice

Encriptación SSL para failover clustering en SQL Server

Si desea utilizar conexiones cifradas en un entorno de clusters, deberá disponer de un certificado emitido con el nombre DNS completo de la instancia de failover cluster. Este certificado también se debe instalar en todos los nodos del failover cluster. Además, tendrá que editar la huella digital del certificado en el registro porque está establecida como Nula en un entorno cluster.

Debe realizar los siguientes pasos en todos los nodos del cluster:

1. Abra el **certificado** utilizando el **complemento de certificados MMC.**
2. Copie el valor **hexadecimal** de la propiedad **Huella digital** de la pestaña Detalles en el bloc de notas y elimine los espacios.
3. Inicie **regedit** y copie el **valor hexadecimal** en esta clave: HKLM\SOFTWARE\Microsoft \Microsoft SQL Server\<YourSQLServerInstance>\MSSQLServer\SuperSocketNetLib \Certificate.
4. Ahora tendrá que reiniciar su nodo, por lo que se recomienda que primero realice un failover a otro nodo.
5. Repita este procedimiento en todos los nodos.

Crear certificados auto-firmados usando IIS

1. Abra **IIS Manager.**
2. Haga clic en el **nombre del servidor** en la columna Conexiones del panel izquierdo.
3. Haga doble clic en **Certificados del servidor** en el panel central.
4. Haga clic en **Crear certificado auto-firmado** en la columna **Acciones** de la derecha.
5. Ingrese un nombre y haga clic en **Aceptar** para continuar.
6. Haga clic en **Aceptar.**

Ahora debería ver que el certificado **SSL** es válido durante un año.

Comprobar la validez del certificado SSL

1. Abra **MMC.**
2. En el menú **Archivo,** haga clic en **Agregar o quitar complemento.**
3. Seleccione **Certificados** y haga clic en **Agregar.**
4. Se le pedirá que abra el complemento para su cuenta de usuario, la cuenta de servicio o la cuenta de equipo. Seleccione la **Cuenta de equipo.**
5. Seleccione **Equipo local,** y luego haga clic en **Finalizar.**
6. Haga clic en **Aceptar** para salir de la ventana **Agregar o quitar complementos.**
7. De nuevo en **MMC**, abra el complemento **Certificados.**
8. Haga doble clic en **Personal**, y luego en **Certificados.**
9. En el panel derecho, localice el **certificado** que va a utilizar.
10. El valor de la columna **Propósito planteado** debe ser **Autenticación del servidor.**
11. El valor de la columna **Emitido para** debe ser el **nombre del servidor.**
12. Haga doble clic en el **certificado** para ver sus propiedades.
13. En la pestaña **General**, debería poder ver este mensaje: **Tiene una clave privada correspondiente a este certificado.**
14. En la pestaña **Detalles**, el valor del campo Sujeto debe ser el nombre del servidor.
15. El valor del campo **Uso mejorado de claves** debe ser **Autenticación del servidor (1.3.6.1.5.5.7.3.1).**
16. En la pestaña Ruta de certificación, el **nombre del servidor** debe aparecer bajo la ruta de certificación.