

Como realizar un backup de SEP11 Manager

Mejores prácticas para la recuperación después de un desastre con Symantec Endpoint Protection

Situación:

¿Cómo utilizo la recuperación después de un desastre con Endpoint Protection?

Solución:

Esta sección incluye información cubierta en la guía de instalación (installation_guide.pdf) proporcionada en la carpeta de la documentación del CD 1 de Symantec Endpoint Protection.

Tareas que se deben realizar para prepararse para la recuperación después de un desastre:

Asegúrese de hacer una copia de respaldo de la base de datos regularmente, preferiblemente de forma semanal, y almacene las copias de respaldo en un lugar apartado.

1. El directorio de la copia de respaldo de la base de datos se encuentra en:
 - \\Archivos de programa\Symantec\ Symantec Endpoint ProtectionManager\data\backup.
 - El archivo de copia de respaldo se llama fecha_marca de fecha.zip.
2. Mueva esta base de datos a otro almacén porque si se desinstala, será eliminada.
3. Localice su archivo de almacén de claves y su archivo server.xml.
 - El nombre del archivo del almacén de claves es keystore_marca de hora.jks. El almacén de claves contiene los pares de claves privadas/públicas y el certificado autofirmado. El nombre de archivo de server.xml es servidor_marca de fecha.xml..
4. Durante la instalación, se hizo una copia de respaldo de estos archivos en el directorio que se llama:
 - \\Archivos de programa\Symantec\Symantec Endpoint Protection Manager\Server PrivateKey Backup.
 - **Nota:** Es posible también hacer copia de respaldo de estos archivos del panel Administrador de la consola de Symantec Endpoint Protection Manager.
5. Cree y abra un archivo de texto con un programa de edición de texto.
6. Asigne al archivo el nombre Backup.txt, o un nombre similar.
7. Abra server.xml, busque la contraseña keystorepass, cópiela y péguela en el archivo de texto.
8. Deje el archivo de texto abierto.
 - **Nota:** La contraseña se utiliza para storepass y keypass. Storepass protege el archivo JKS. Keypass protege la clave privada. Estas contraseñas se escriben para restaurar el certificado. La cadena de la contraseña tiene el siguiente formato:
keystorePass="WjCUZx7kmX\$qA1u1".
9. Copie y pegue la cadena que está entre comillas. (No incluya las comillas).
10. Si tiene un dominio solamente, busque y copie el archivo symlink.xml desde un directorio en:

- \\Archivos de programa\Symantec\Symantec Endpoint ProtectionManager\data\outbox\agent.

11. Péguelo en:

- \\Archivos de programa\Symantec\Symantec Endpoint ProtectionManager\Server Private Key Backup.

12. Si tiene varios dominios, para cada dominio, busque y copie un archivo sylink.xml en un equipo cliente y péguelo en:

- \\Archivos de programa\Symantec\Symantec Endpoint ProtectionManager\Server Private Key Backup.

13. Los ID de dominio son obligatorios si no tiene una copia de respaldo de la base de datos. Este ID está en el archivo sylink.xml de los equipos cliente en cada dominio.

14. Abra cada archivo sylink.xml, busque el ID de dominio, cópielo y péguelo en el archivo de texto Backup.txt.

15. Se agrega este ID a un nuevo dominio que usted cree para que contenga los clientes existentes.

- La cadena del archivo sylink.xml tiene el siguiente formato: DomainId="B44AC676C08A165009ED819B746F1".

16. Copie y pegue la cadena que está entre comillas. (No incluya las comillas)

17. En el archivo Backup.txt, escriba la contraseña de cifrado que utilizó cuando usted instaló el primer sitio en la instancia de instalación.

18. Se vuelve a escribir esta clave cuando se reinstala Symantec Endpoint Protection Manager.

- **Nota:** Es necesario volver a escribir la clave idéntica si no tiene una copia de respaldo de la base de datos para restaurar. No es obligatorio si tiene una copia de respaldo de una base de datos para restaurar, pero es una mejor práctica.

19. En el archivo de texto Backup.txt, escriba la dirección IP y el nombre de host del equipo con Symantec Endpoint Protection Manager.

20. Si ocurre un problema de hardware irreversible, es necesario reinstalar Symantec Endpoint Protection Manager en un equipo que tenga la misma dirección IP y nombre de host.

21. En el archivo Backup.txt, escriba el nombre del sitio que identifica a Symantec Endpoint Protection Manager.

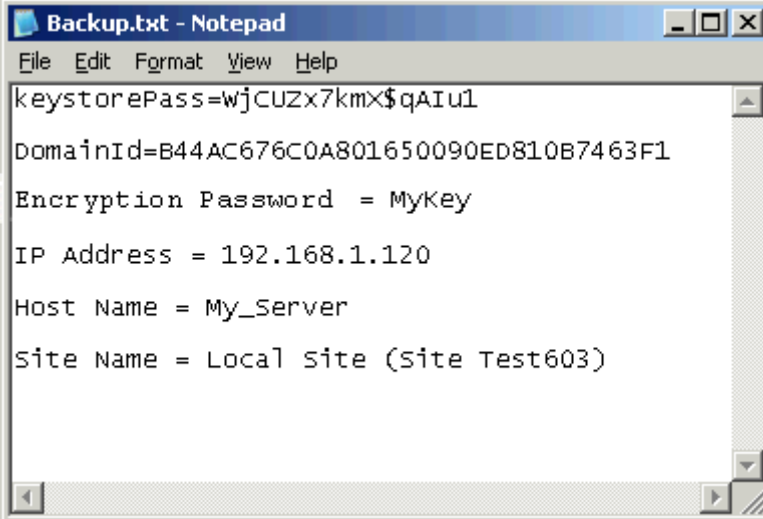
22. Guarde y cierre el archivo Backup.txt, que ahora contiene la información esencial necesaria para la recuperación después de un desastre.

23. Mientras que el nombre del sitio no se necesita terminantemente para la reinstalación, ayuda a crear una restauración coherente.

24. Copie estos archivos en soportes extraíbles y almacene los soportes en una ubicación segura, preferiblemente en una caja fuerte.

25. Una vez que proteja los archivos, debe quitarlos del equipo con Symantec Endpoint Protection Manager.

- A continuación se ilustra un archivo de texto que contiene la información obligatoria para realizar correctamente una recuperación después de un desastre.



```
Backup.txt - Notepad
File Edit Format View Help
keystorePass=wjCUZx7kmX$qAIu1
DomainId=B44AC676C0A801650090ED810B7463F1
Encryption Password = MyKey
IP Address = 192.168.1.120
Host Name = My_Server
Site Name = Local Site (Site Test603)
```

- Si crea este archivo, es posible copiar y pegar esta información cuando sea necesario durante recuperación después de un desastre.

Acerca del proceso de recuperación después de un desastre

El proceso de la recuperación después de un desastre exige completar secuencialmente los tres procedimientos siguientes:

- Restaurar Symantec Endpoint Protection Manager
- Restaurar el certificado de servidor
- Restaurar comunicaciones de clientes

Las forma de restaurar las comunicaciones de los clientes depende de si tiene acceso a una copia de respaldo de la base de datos.

Restauración de Symantec Endpoint Protection Manager

Si sufre un desastre, recupere los archivos que fueron asegurados después de la instalación inicial. A continuación, abra el archivo Backup.txt que contiene las contraseñas, los ID del dominio y así sucesivamente.

Acerca de identificar el equipo nuevo o reconstruido

Si tuvo un error de hardware catastrófico, es posible que sea necesario reconstruir el equipo. Si reconstruye el equipo, debe asignarle la dirección IP y el nombre del host originales. Esta información se debe encontrar en el archivo Backup.txt.

Reinstalación de Symantec Endpoint Protection Manager

La tarea clave que debe realizarse cuando se reinstala Symantec Endpoint Protection Manager es escribir el nombre de la clave previamente compartida que usted utilizó al instalar Symantec Endpoint Protection Manager que falló.

Para reinstalar Symantec Endpoint Protection Manager

1. Inserte el CD de instalación, Comience a instalar Symantec Endpoint Protection Manager.
2. En el Panel de bienvenida, marque "Instalar mi primer sitio".
3. Haga clic en **Siguiente**
4. Siga con la instalación hasta que se le solicite la **Clave Previamente Compartida**.
5. En el **panel de información del sitio > cuadros de Contraseña de cifrado**, escriba el "nombre de la contraseña" del archivo de texto.
 - **Nota:** Si está realizando la restauración sin una copia de respaldo de la base de datos, la restauración fallará si no escribe la contraseña correctamente.
6. Haga clic en **Siguiente**.
7. Cuando se le solicite, reconstruya el mismo tipo de base de datos.
8. Continúe con la instalación hasta que aparezca el panel que indica que finalizó la configuración del Asistente para la instalación del servidor de administración.
9. En el panel Configuración completada, debajo de "¿Desea ejecutar el Asistente para migración y distribución ahora?", marque **No**.
10. Haga clic en **Finalizar**.

Restauración del certificado de servidor

El certificado del servidor es un almacén de claves Java que contiene el certificado público y los pares de claves pública y privada. Es necesario escribir la contraseña que contiene el archivo de Backup.txt. La contraseña está también en el archivo server_marca de hora.xml.

Para restaurar el certificado de servidor

1. Inicie sesión en la consola.
2. Haga clic en **Administrador**.
3. Haga clic en **Servidores**, debajo de Tareas
4. Debajo de "Ver servidores", amplíe **Sitio local**
5. Haga clic en el **nombre del equipo que identifica el sitio del local**.
6. Haga clic en **Administrar certificado del servidor**, debajo de "Tareas".
7. En el panel de bienvenida, haga clic en **Siguiente**.
8. En el panel de administración del certificado del servidor, marque **Actualizar el certificado de servidor**.
9. Haga clic en **Siguiente**.
10. Debajo de "Seleccione el tipo de certificado que desea importar", marque **Almacén de claves JKS**.
11. Haga clic en **Siguiente**.
 - **Nota:** Si ha implementado uno de los otros tipos de certificado, seleccione ese tipo.
12. En el panel "Almacén de claves JKS", haga clic en **Examinar**.
13. Busque y seleccione el archivo de almacén de claves almacén de claves_marca de fech.jks que incluyó en la copia de seguridad.
14. Haga clic en **Aceptar**.
15. Abra su "archivo de texto de la recuperación después de un desastre".
16. Seleccione y copie la **contraseña del almacén de claves**.
17. Active el cuadro de diálogo **Almacén de claves JKS**.
18. Pegue la **contraseña del almacén de claves** en los cuadros "Almacén de claves" y Clave.
 - **Nota:** El único mecanismo de pegado admitido es Ctrl + V.

19. Haga clic en **Siguiente**.
 - **Nota:** Si recibe un mensaje de error que diga que hay un archivo no válido de almacén de claves, probablemente haya escrito contraseñas no válidas. Reintente copiar y pegar la contraseña. (Este mensaje de error es engañoso)
20. En el panel Completa, haga clic en **Finalizar**.
21. Cierre la sesión en la Consola.
22. Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas > Servicios**.
23. En la ventana Servicios, haga clic con el botón secundario en **Symantec Endpoint Protection Manager**.
24. Haga clic en **Detener**.
 - **Nota:** No cierre la ventana Servicios hasta que haya finalizado la recuperación después de un desastre y restablezca las comunicaciones de los clientes.
25. Haga clic con el botón secundario en **Symantec Endpoint Protection Manager**.
26. Haga clic en Inicio.
 - **Nota:** Detener e iniciar Symantec Endpoint Protection Manager restaura completamente el certificado.

Restauración de comunicaciones de los clientes

Si tiene acceso a una copia de respaldo de la base de datos, es posible restaurarla y reanudar las comunicaciones de los clientes. La ventaja sobre la restauración con una copia de respaldo de la base de datos es que los clientes reaparecen en sus grupos y están sujetos a las políticas originales. Si no tiene acceso a una copia de respaldo de la base de datos, es posible aún recuperar las comunicaciones con sus clientes, pero éstos aparecen en el grupo temporal. Es posible entonces reconstruir la estructura del grupo y de las políticas.

Restauración de las comunicaciones de los clientes con una copia de respaldo de la base de datos

No es posible restaurar una base de datos en un equipo que ejecute un servicio activo de Symantec Endpoint Protection Manager, por lo tanto, es necesario detenerlo e iniciarlo algunas veces.

Para restaurar las comunicaciones de los clientes con una copia de respaldo de la base de datos

1. Si cerró la ventana Servicios, haga clic en **Inicio Configuración > Panel de control > Herramientas administrativas > Servicios**.
2. En la ventana Servicios, haga clic con el botón secundario en **Symantec Endpoint Protection Manager**.
3. Haga clic en **Detener**.
 - **Nota:** No cierre la ventana Servicios hasta que haya terminado este procedimiento.
4. Cree el siguiente directorio: \\Archivos de programa\Symantec\Symantec Endpoint Protection Manager\data\backup
5. Copie el archivo de la copia de respaldo de la base de datos en el directorio.
 - **Nota:** De forma predeterminada, el archivo de la copia de respaldo de la base de datos lleva el nombre fecha_marca de fecha.zip.

6. Haga clic en **Inicio > Programas > Symantec Endpoint Protection Manager** Copia de respaldo y restauración de la base de datos .
7. En el cuadro de diálogo Copia de respaldo y restauración de la base de datos, haga clic en Restaurar.
8. En el cuadro de diálogo Restaurar sitio, seleccione el archivo de copia de respaldo que copió en el directorio de copia de respaldo.
9. Haga clic en **Aceptar**.
 - **Nota:** El tiempo de la restauración de base de datos varía y depende del tamaño de la base de datos.
10. Cuando aparece la indicación de mensaje, haga clic en **Aceptar**.
11. Haga clic en **Salir**.
12. Haga clic en **Inicio > Programas > Symantec Endpoint Protection Manager > Asistente para la configuración del servidor de administración**.
13. En el panel de bienvenida, marque Volver a **configurar el servidor de administración**.
14. Haga clic en **Siguiente**.
15. En el panel Información de servidor, modifique los valores de la entrada de información, si fuera necesario, para que coincida con las entradas de información anteriores y, luego, haga clic en **Siguiente**.
16. En el panel Elección del servidor de bases de datos, active el tipo de base de datos para que coincida con el tipo anterior y, luego, haga clic en **Siguiente**.
17. En el panel Información de la base de datos, modifique e inserte los valores de la entrada de información para que coincida con las entradas de información anteriores, y luego haga clic en **Siguiente**.
 - **Nota:** La configuración dura varios minutos.
18. En el cuadro de diálogo Configuración finalizada, haga clic en **Finalizar**.
19. Inicie sesión en la Consola de Symantec Endpoint Protection Manager.
20. Haga clic con el botón secundario en sus **grupos**.
21. Haga clic en **Ejecutar comando** en el **grupo Actualizar contenido**.
22. Si los clientes no responden después de una hora, reinicie los clientes.

Restauración de las comunicaciones de los clientes sin una copia de respaldo de la base de datos

Para cada dominio que utilice, es necesario crear un nuevo dominio y reinsertar el mismo ID del dominio en la base de datos.

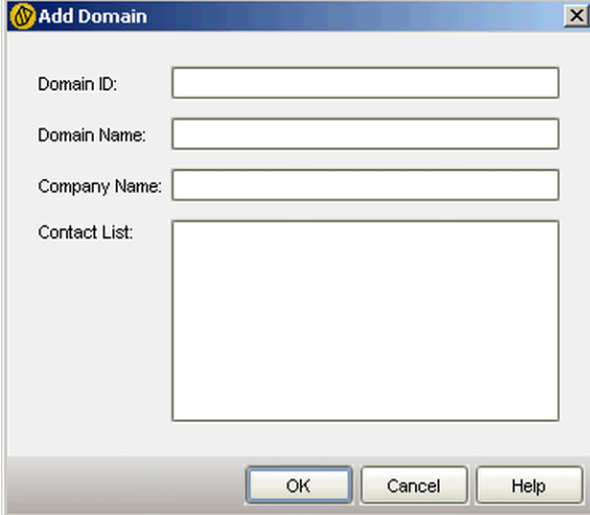
Estos ID del dominio están en el archivo de texto de recuperación después de un desastre (si alguien los escribió en este archivo). El dominio Sistema es el dominio predeterminado.

Se recomienda crear un nombre de dominio que sea idéntico al nombre de dominio anterior. Para reconstruir el dominio (predeterminado) del sistema, agregue algún valor, por ejemplo: `_2` (System_2). Después de restaurar dominios, es posible entonces eliminar el dominio anterior del sistema, y cambiar el nombre del nuevo dominio a Sistema.

Para restaurar las comunicaciones de los clientes sin una copia de respaldo de la base de datos

1. Inicie sesión en la **Consola de Symantec Endpoint Protection Manager**.
2. En la consola, haga clic en **Administrador**.
3. En el panel Administrador del sistema, haga clic en **Dominios**.
4. En la esquina superior derecha, haga clic en **Acerca**.

5. Mantenga presionadas las teclas **Mayús + Ctrl + Alt** y haga un clic a la **izquierda del botón Aceptar** en el cuadro de diálogo "Acerca" de, tres veces rápidamente.
6. Haga clic en **Aceptar**.
7. Debajo de Tareas, haga clic en **Agregar dominio**.



The image shows a Windows-style dialog box titled "Add Domain". It features a title bar with a yellow icon and a close button. The main area contains four input fields: "Domain ID:", "Domain Name:", "Company Name:", and "Contact List:". The "Contact List" field is a larger text area. At the bottom, there are three buttons: "OK", "Cancel", and "Help".

8. Abra el archivo de texto de recuperación después de un desastre.
9. Seleccione y copie el **ID del dominio**.
10. Seleccione el cuadro de diálogo **Agregar dominio** y pegue el **ID del dominio** en el cuadro "ID del dominio"
 - **Nota:** Si no aparece el cuadro ID del dominio, repita los pasos 4, 5, 6 y 7 hasta que aparezca el cuadro. Ctrl + V es el único mecanismo de pegado admitido.
11. Haga clic en **Aceptar**.
(Opcional) Repita los pasos 7, 8 y 9 para cada dominio que desee recuperar.
12. Debajo de Tareas, haga clic en **Administrar dominio**.
13. Reinicie todos los equipos cliente. Los equipos aparecen en el grupo Temporal.
 - (Opcional) si usted utiliza sólo un dominio, elimine el dominio predeterminado Sistema sin usar y cambie el nombre del dominio creado recientemente a Sistema.