

Actualizar a VMware Identity Manager 2.9.1

VMware Identity Manager 2.9.1

vmware[®]

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware en:

<https://docs.vmware.com/es/>

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. Todos los derechos reservados. [Copyright e información de marca registrada.](#)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.: + 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Actualizar a VMware Identity Manager 2.9.1	5
1 Acerca de la actualización a VMware Identity Manager 2.9.1	7
Actualizar un clúster	8
2 Actualizar VMware Identity Manager en línea	9
Requisitos previos para la actualización online	9
Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager	10
Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager	10
Realizar una actualización en línea	11
3 Actualizar VMware Identity Manager sin conexión	13
Requisitos previos para la actualización sin conexión	13
Preparar un servidor web local para la actualización sin conexión	13
Configurar el dispositivo y realizar una actualización sin conexión	14
4 Configurar opciones tras la actualización	17
5 Resolver problemas de actualización	19
Consultar los registros de errores de la actualización	19
Restaurar instantáneas de VMware Identity Manager	19
Recopilar un paquete de archivos de registro	20
Índice	21

Actualizar a VMware Identity Manager 2.9.1

En *Actualizar a VMware Identity Manager 2.9.1*, se describe la forma de actualizar a VMware Identity Manager 2.9.1 desde una versión anterior.

Si prefiere hacer una instalación nueva, consulte *Instalar y configurar VMware Identity Manager*. Recuerde que en una nueva instalación no se conservan las configuraciones existentes.

Para obtener información sobre cómo utilizar la instancia actualizada de VMware Identity Manager, consulte la *guía del administrador* de VMware Identity Manager.

Público objetivo

Esta información está dirigida a todos los que instalen, actualicen y configuren VMware Identity Manager. La información está escrita para administradores de sistemas Windows o Linux con experiencia y que estén familiarizados con la tecnología de máquinas virtuales.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario con términos que quizá usted desconozca. Para consultar las definiciones de términos tal como se utilizan en la documentación técnica de VMware, visite <http://www.vmware.com/es/support/pubs>.

Acerca de la actualización a VMware Identity Manager 2.9.1

1

Son compatibles las siguientes rutas y escenarios de actualización.

Rutas de actualización compatibles

Son compatibles las siguientes rutas de actualización:

- De la versión 2.6 y posteriores a 2.9.1

NOTA: La última versión publicada fue 2.8.1. No se ha publicado la versión 2.9 de forma externa.

Conexión a Internet

Puede actualizar VMware Identity Manager en línea o sin conexión.

De forma predeterminada, el dispositivo de VMware Identity Manager utiliza el sitio web de VMware para el procedimiento de actualización, para lo que se necesita que el dispositivo tenga conexión a Internet. También se debe configurar el proxy para el dispositivo, si corresponde.

Si el dispositivo virtual no dispone de conexión a Internet, se puede realizar la actualización sin conexión. Para realizar una actualización sin conexión, se debe descargar el paquete de actualización de My VMware y configurar un servidor web local para alojar el archivo de actualización.

Escenarios de actualización

- Si se ha implementado un solo dispositivo de VMware Identity Manager, se debe actualizar en línea o sin conexión de la manera descrita en [Capítulo 2, "Actualizar VMware Identity Manager en línea,"](#) página 9 o [Capítulo 3, "Actualizar VMware Identity Manager sin conexión,"](#) página 13.

NOTA: Se producirá algún tiempo de inactividad, ya que durante la actualización se detendrán todos los servicios. Planifique el momento de la actualización teniéndolo en cuenta.

- Si se han implementado varios dispositivos virtuales de VMware Identity Manager en un clúster para conmutación por error o alta disponibilidad, consulte ["Actualizar un clúster,"](#) página 8.
- Para actualizar VMware Identity Manager sin tiempo de inactividad en un escenario de implementación de un centro de datos múltiple, consulte "Actualizar VMware Identity Manager sin tiempo de inactividad" en *Instalar y configurar VMware Identity Manager*.

Actualizar un clúster

Si se han implementado varios dispositivos virtuales VMware Identity Manager en un clúster para disponer de conmutación por error o alta disponibilidad, se pueden actualizar los nodos de uno en uno. Durante la actualización se producirán períodos de inactividad, por lo que se debe planificar el momento adecuado para la actualización.

Procedimiento

- 1 Realice snapshots de la base de datos y los nodos de VMware Identity Manager.
- 2 Elimine todos los nodos excepto uno del equilibrador de carga.
- 3 Actualice el nodo que sigue conectado al equilibrador de carga.

Siga el proceso para realizar una actualización con o sin conexión como se describe en [Capítulo 2, “Actualizar VMware Identity Manager en línea,”](#) página 9 o en [Capítulo 3, “Actualizar VMware Identity Manager sin conexión,”](#) página 13.

IMPORTANTE: Durante el proceso de actualización se producirán períodos de inactividad.

- 4 Después de actualizar el nodo, déjelo conectado al equilibrador de carga.
De esta forma se asegura que el servicio VMware Identity Manager esté disponible mientras se actualizan los otros nodos.
- 5 Actualice los nodos de uno en uno.
- 6 Compruebe que RabbitMQ no se ejecute en el modo de clúster en los nodos actualizados.

En la versión 2.9.1, la agrupación en clústeres de RabbitMQ se encuentra deshabilitada.

- a Inicie sesión en un nodo actualizado a la vez.
- b Ejecute el siguiente comando:

```
rabbitmqctl cluster_status
```

El comando debería devolver un estado similar al siguiente para cada nodo:

```
sva-1:~ # rabbitmqctl cluster_status
Cluster status of node 'rabbitmq@sva-1' ...
[{"nodes", [{"disc", ["rabbitmq@sva-1"]}]},
 {"running_nodes", ["rabbitmq@sva-1"]},
 {"cluster_name", <<"rabbitmq@sva-1.hs.trcint.com">>},
 {"partitions", []},
 {"alarms", [{"rabbitmq@sva-1", []}]}
```

- 7 Después de actualizar todos los nodos, vuelva a agregarlos al equilibrador de carga.

Actualizar VMware Identity Manager en línea

2

El dispositivo virtual de VMware Identity Manager se puede actualizar en línea. Para la actualización en línea, el dispositivo virtual se debe poder conectar a Internet.

Este capítulo cubre los siguientes temas:

- [“Requisitos previos para la actualización online,”](#) página 9
- [“Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager,”](#) página 10
- [“Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager,”](#) página 10
- [“Realizar una actualización en línea,”](#) página 11

Requisitos previos para la actualización online

Antes de actualizar el dispositivo virtual de VMware Identity Manager en línea, debe realizar estas tareas previas.

- Compruebe que dispone de al menos 2,5 GB de espacio en el disco en la partición raíz primaria del dispositivo virtual.
- Realice una instantánea del dispositivo virtual como copia de seguridad. Para obtener información sobre cómo realizar instantáneas, consulte la documentación de vSphere.
- Si utiliza una base de datos externa, realice una instantánea o una copia de seguridad de la base de datos.
- Verifique que VMware Identity Manager esté configurado correctamente.
- Verifique que el dispositivo virtual pueda resolver y acceder a la dirección vapp-updates.vmware.com en el puerto 80 mediante HTTP.
- Si para el acceso HTTP saliente se necesita un servidor proxy HTTP, configure los valores del servidor proxy para el dispositivo virtual. Consulte [“Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager,”](#) página 10.
- Confirme que existe una actualización de VMware Identity Manager. Ejecute el comando correspondiente para comprobar si hay actualizaciones. Consulte [“Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager,”](#) página 10.

Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager

Si el dispositivo virtual de VMware Identity Manager puede conectarse a Internet, puede comprobar la disponibilidad de las actualizaciones en línea desde el mismo dispositivo.

Procedimiento

- 1 Inicie la sesión en el dispositivo virtual como usuario raíz.
- 2 Ejecute el comando siguiente para comprobar si existe una actualización en línea.

```
/usr/local/horizon/update/updatemgr.hzn check
```

Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager

El dispositivo virtual de VMware Identity Manager accede a los servidores de actualización de VMware a través de Internet. Si su configuración de red proporciona acceso a Internet con un proxy HTTP, debe modificar la configuración del dispositivo.

Habilite su proxy para gestionar solo el tráfico de Internet. Para asegurar que el proxy esté configurado correctamente, establezca el parámetro de tráfico interno en la opción `no-proxy` dentro del dominio.

NOTA: Los servidores proxy que requieren autenticación no son compatibles.

Prerequisitos

- Compruebe que dispone de la contraseña raíz del dispositivo virtual.
- Compruebe que dispone de la información del servidor proxy. Tenga en cuenta que los servidores proxy que requieren autenticación no son compatibles.

Procedimiento

- 1 Inicie sesión en el dispositivo virtual de VMware Identity Manager como usuario root.
- 2 Introduzca `YaST` en la línea de comandos para ejecutar la utilidad `YaST`.
- 3 En el panel izquierdo, seleccione **Servicios de red** y, a continuación, **Proxy**.
- 4 Introduzca las URL del servidor proxy en los campos de **URL del proxy HTTP** y **URL del proxy HTTPS**.
- 5 Seleccione **Finalizar** y salga de la utilidad `YaST`.
- 6 Reinicie el servidor Tomcat en el dispositivo virtual de VMware Identity Manager para utilizar la nueva configuración del proxy.

```
service horizon-workspace restart
```

Los servidores de actualización de VMware ya están disponibles para el dispositivo virtual de VMware Identity Manager.

Realizar una actualización en línea

Si su dispositivo virtual de VMware Identity Manager dispone de conexión a Internet, puede actualizarlo en línea.

Prerequisitos

- Compruebe que cumple los requisitos previos que aparecen en la lista de [“Requisitos previos para la actualización online,”](#) página 9.
- Compruebe que el dispositivo virtual esté encendido y en funcionamiento.

Procedimiento

- 1 Inicie sesión en el dispositivo virtual de VMware Identity Manager como usuario root.
- 2 Ejecute el comando siguiente `updatemgr.hzn`.
`/usr/local/horizon/update/updatemgr.hzn updateinstaller`
- 3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.
`/usr/local/horizon/update/updatemgr.hzn check`
- 4 Ejecute el comando siguiente para actualizar el dispositivo.
`/usr/local/horizon/update/updatemgr.hzn update`
Los mensajes que se generen durante la actualización se guardan en el archivo `update.log` en `/opt/vmware/var/log/update.log`.
- 5 Vuelva a ejecutar el comando `updatemgr.hzn check` para comprobar que no existe ninguna actualización más reciente.
`/usr/local/horizon/update/updatemgr.hzn check`
- 6 Compruebe la versión del dispositivo actualizado.
`vami cli version --appliance`
Se mostrará la nueva versión.
- 7 Reinicie el dispositivo virtual.
`reboot`

Se completó la actualización.

Tenga en cuenta que es posible que las funciones de búsqueda y autocompletar en la consola de administración no se encuentren disponibles por 15 o 20 minutos tras el inicio del dispositivo virtual. Esto depende de la versión desde la que se realice la actualización. En la versión 2.7, la búsqueda de índices se transfirió a Elasticsearch, un motor de búsqueda y análisis integrado en el dispositivo de VMware Identity Manager. El proceso de migración puede durar entre 15 y 20 minutos después del inicio del dispositivo virtual.

Tenga también en cuenta que para que funcionen la búsqueda y la función de autocompletar, la auditoría no debe estar deshabilitada. Puede comprobar la configuración de la auditoría en la página **Catálogo > Configuración > Auditoría**.

Actualizar VMware Identity Manager sin conexión

3

Si el dispositivo virtual de VMware Identity Manager no se puede conectar a Internet para su actualización, se puede realizar una actualización sin conexión. Se debe configurar un directorio de actualización en un servidor web local y configurar el dispositivo para utilizarlo para la actualización.

Este capítulo cubre los siguientes temas:

- “Requisitos previos para la actualización sin conexión,” página 13
- “Preparar un servidor web local para la actualización sin conexión,” página 13
- “Configurar el dispositivo y realizar una actualización sin conexión,” página 14

Requisitos previos para la actualización sin conexión

Antes de actualizar sin conexión el dispositivo virtual de VMware Identity Manager, realice estas tareas obligatorias previas.

- Compruebe que dispone de al menos 2,5 GB de espacio en el disco en la partición raíz primaria del dispositivo virtual.
- Realice una instantánea del dispositivo virtual como copia de seguridad. Para obtener información sobre cómo realizar instantáneas, consulte la documentación de vSphere.
- Si utiliza una base de datos externa, realice una instantánea o una copia de seguridad de la base de datos.
- Verifique que VMware Identity Manager esté configurado correctamente.
- Confirme que existe una actualización de VMware Identity Manager. Compruebe si hay actualizaciones en el sitio de My VMware en my.vmware.com.
- Prepare un servidor web local para alojar el archivo de actualización. Consulte “Preparar un servidor web local para la actualización sin conexión,” página 13.

Preparar un servidor web local para la actualización sin conexión

Antes de iniciar la actualización sin conexión, se debe configurar el servidor web local creando una estructura de directorios que incluya un subdirectorío para el dispositivo virtual VMware Identity Manager.

Prerequisitos

- Obtenga el archivo `identity-manager-2.9.x.x-buildNumber-updaterepo.zip`. Vaya a my.vmware.com y acceda a la página de descarga del producto VMware Identity Manager para descargar el archivo.

- Si utiliza un servidor web IIS, configúrelo para que admita caracteres especiales en los nombres de archivo. Para ello, acceda a la sección **Filtrado de solicitudes** y seleccione la opción **Permitir doble escape**.

Procedimiento

- 1 Cree un directorio en el servidor web en `http://SuServidorWeb/VM/` y copie en él el archivo descargado.
- 2 Verifique que el servidor web incluya los tipos mime para `.sig` (texto/simple) y `.sha256` (texto/simple). Si estos tipos de mime, el servidor no podrá comprobar si hay actualizaciones.

- 3 Descomprima el archivo.

El contenido extraído del archivo ZIP será proporcionado por `http://SuServidorWeb/VM/`.

El contenido extraído del archivo contiene los siguientes subdirectorios `/manifest` y `/package-pool`.

- 4 Ejecute el comando siguiente `updateLocal.hzn` para comprobar que en la URL hay contenido de actualización válido.

```
/usr/local/horizon/update/updateLocal.hzn checkurl http://YourWebServer/VM
```

Configurar el dispositivo y realizar una actualización sin conexión

Configure el dispositivo de VMware Identity Manager para indicarle al servidor web local que realice una actualización sin conexión. A continuación, actualice el dispositivo.

Prerequisitos

[“Preparar un servidor web local para la actualización sin conexión,”](#) página 13.

Procedimiento

- 1 Inicie sesión en el dispositivo de VMware Identity Manager como usuario raíz.
- 2 Ejecute el siguiente comando para configurar un repositorio de actualización que utilice un servidor web local.

```
/usr/local/horizon/update/updateLocal.hzn seturl http://YourWebServer/VM/
```

NOTA: Para deshacer los cambios de la configuración y restablecer la opción de realizar una actualización en línea, puede ejecutar el siguiente comando.

```
/usr/local/horizon/update/updateLocal.hzn setdefault
```

- 3 Realice la actualización.
 - a Ejecute el comando siguiente `updateMgr.hzn`.


```
/usr/local/horizon/update/updateMgr.hzn updateinstaller
```
 - b Ejecute el comando siguiente.


```
/usr/local/horizon/update/updateMgr.hzn update
```

Los mensajes que se generen durante la actualización se guardan en el archivo `update.log` en `/opt/vmware/var/log/update.log`.
 - c Vuelva a ejecutar el comando `updateMgr.hzn check` para comprobar que no existe ninguna actualización más reciente.

```
/usr/local/horizon/update/updateMgr.hzn check
```

- d Compruebe la versión del dispositivo actualizado.

```
vami cli version --appliance
```

El comando debe mostrar la nueva versión.

- e Reinicie el dispositivo virtual.

Por ejemplo, desde la línea del comando, ejecute el siguiente comando.

```
reboot
```

Se completó la actualización.

Tenga en cuenta que es posible que las funciones de búsqueda y autocompletar en la consola de administración no se encuentren disponibles por 15 o 20 minutos tras el inicio del dispositivo virtual. Esto depende de la versión desde la que se realice la actualización. En la versión 2.7, la búsqueda de índices se transfirió a Elasticsearch, un motor de búsqueda y análisis integrado en el dispositivo de VMware Identity Manager. El proceso de migración puede durar entre 15 y 20 minutos después del inicio del dispositivo virtual.

Tenga también en cuenta que para que funcionen la búsqueda y la función de autocompletar, la auditoría no debe estar deshabilitada. Puede comprobar la configuración de la auditoría en la página **Catálogo > Configuración > Auditoría**.

Configurar opciones tras la actualización

4

Después de actualizar a VMware Identity Manager 2.9.1, configure estas opciones.

- Cambios de sincronización masiva en VMware Identity Manager 2.9.1

En la versión 2.8.1, la sincronización masiva se realizaba con 4 subprocesos por CPU a través de un parámetro de configuración global en la base de datos que se denominaba `bulkSyncThreadLimitPerCPU=4`.

En la versión 2.9.1, el número de subprocesos para realizar la sincronización masiva no se basa en CPU. Es un número absoluto, que es igual al número de CPU en un nodo de forma predeterminada.

Si sincroniza grandes cantidades de usuarios y grupos, y advierte que la sincronización es lenta después de la actualización, puede establecer el parámetro de configuración global denominado `bulkSyncSharedThreadCount` para especificar el número de subprocesos.

Establezca el valor de subprocesos en la base de datos mediante la REST API siguiente y reinicie los nodos para que los cambios surtan efecto.

Solicitud de HTTP:

Operation: PUT

URI: `bulkSyncSharedThreadCount`

Encabezados HTTP:

Content-Type: `application/vnd.vmware.horizon.manager.systemconfigparameter+json`

Accept: `application/vnd.vmware.horizon.manager.systemconfigparameter+json`

Authorization: HZN <operator token>

Cuerpo de la solicitud (con 8 subprocesos como ejemplo):

```
{
  "name": "bulkSyncSharedThreadCount",
  "values": {
    "values": [
      "8"
    ]
  }
}
```

- Si tiene configurado un clúster de VMware Identity Manager para la conmutación por error con dos nodos, se recomienda actualizarlo a tres nodos. Esto se debe a una limitación de Elasticsearch, un motor de búsqueda y análisis integrado en el dispositivo de VMware Identity Manager. Puede seguir utilizando dos nodos, pero debe tener en cuenta las limitaciones relacionadas con Elasticsearch. Para obtener más información, consulte el apartado sobre cómo configurar los errores y la redundancia en *Instalar y configurar VMware Identity Manager*.

- Habilite la nueva interfaz de usuario del portal.
 - a En la consola de administración, haga clic en la flecha de la pestaña **Catálogo** y seleccione **Configuración**.
 - b Seleccione **Nueva interfaz del portal de usuario final** en el panel de la izquierda y haga clic en **Habilitar nueva interfaz del portal**.
- De forma predeterminada, el protocolo de seguridad de la capa de transporte (TLS) 1.0 se encuentra deshabilitado en VMware Identity Manager 2.9.1. Se admiten TLS 1.1 y 1.2.

Los errores en productos externos pueden producirse cuando TLS 1.0 está deshabilitado. Le recomendamos que actualice sus otras configuraciones de productos para utilizar TLS 1.1 o 1.2. Sin embargo, si la versión de productos como Horizon, Horizon Cloud, Citrix o los equilibradores de carga depende de TLS 1.0, puede habilitar TLS 1.0 en VMware Identity Manager mediante las instrucciones en el [artículo 2144805 de la base de conocimientos](#).

Resolver problemas de actualización

Para resolver problemas de actualización, revise los archivos de registro. Si VMware Identity Manager no se inicia, se puede restaurar una instancia anterior a partir de una instantánea.

Este capítulo cubre los siguientes temas:

- [“Consultar los registros de errores de la actualización,”](#) página 19
- [“Restaurar instantáneas de VMware Identity Manager,”](#) página 19
- [“Recopilar un paquete de archivos de registro,”](#) página 20

Consultar los registros de errores de la actualización

Revise los registros de errores ocurridos durante la actualización para resolverlos. Los archivos de registro de la actualización están en el directorio `/opt/vmware/var/log`.

Problema

Al acabar la actualización, VMware Identity Manager no se inicia y los errores aparecen en los registros de errores.

Origen

Errores ocurridos durante la actualización.

Solución

- 1 Inicie sesión en el dispositivo virtual VMware Identity Manager.
- 2 Vaya al directorio `/opt/vmware/var/log`.
- 3 Abra el archivo `update.log` y revise los mensajes de error.
- 4 Resuelva los errores y vuelva a ejecutar el comando de actualización. El comando de actualización continuará desde el punto en que se detuvo.

NOTA: Alternativamente, puede revertir a una snapshot y ejecutar de nuevo la actualización.

Restaurar instantáneas de VMware Identity Manager

Si VMware Identity Manager no se inicia correctamente después de una actualización, se puede restaurar una instancia anterior.

Problema

Después actualizar VMware Identity Manager, no se inicia correctamente. Se revisaron los registros de errores de actualización y se ejecutó de nuevo el comando de actualización, pero no se resolvió el problema.

Origen

Ocurrieron errores durante el proceso de actualización.

Solución

- ◆ Restaure una de las instantáneas realizadas como copia de seguridad de la instancia original de VMware Identity Manager y de la base de datos externa, si corresponde. Para obtener información, consulte la documentación de vSphere.

Recopilar un paquete de archivos de registro

Puede recopilar un paquete de archivos de registro. El paquete se obtiene de la página de configuración de dispositivos de VMware Identity Manager.

El paquete incluye los siguientes archivos de registro.

Tabla 5-1. Archivos de registro

Componente	Ubicación del archivo de registro	Descripción
Registros de Apache Tomcat (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat registra los mensajes que no se registran en otros archivos de registro.
Registros del configurador (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	Solicitudes que recibe el configurador del cliente REST y de la interfaz web.
Registros del conector (connector.log)	/opt/vmware/horizon/workspace/logs/connector.log	Un registro de cada solicitud recibida desde la interfaz web. Cada entrada del registro incluye también la URL, la marca de hora y las excepciones de la solicitud. No se registra ninguna acción de sincronización.
Registros del servicio (horizon.log)	/opt/vmware/horizon/workspace/logs/horizon.log	El registro del servicio registra la actividad que tiene lugar en el dispositivo VMware Identity Manager, como la actividad relacionada con autorizaciones, usuarios y grupos.
Registros del catálogo unificado (greenbox_web.log)	/opt/vmware/horizon/workspace/logs/greenbox_web.log	Registros de actividad relacionada con el catálogo unificado.

Procedimiento

- 1 Inicie la sesión en la página de configuración del dispositivo VMware Identity Manager en <https://identitymanagerURL:8443/cfg/logs>.
- 2 Haga clic en **Preparar paquete de registro**.
- 3 Descargue el paquete.

Índice

A

actualización en línea **9, 11**
actualización sin conexión **13**
actualizar **7**

C

clúster, actualizar **8**
comprobar actualización en línea **10**
configurar opciones **17**

E

errores **19**
errores de actualización **19**

G

glosario **5**

I

indicar al servidor web local **14**
instantáneas **19**

N

nueva interfaz de usuario del portal **17**

P

paquete de registro **20**
preparar el servidor web local **13**
proxy HTTP **10**
público objetivo **5**

R

recopilar paquete de registro **20**
registros de errores **19**
requisitos previos para la actualización en línea **9**
requisitos previos para la actualización sin conexión **13**
restaurar instantánea **19**

S

servidor proxy **10**
servidor web local **14**
solucionar problemas **19**

