Red Hat Enterprise Linux 8

Actualización de RHEL 7 a RHEL 8

Instrucciones para una actualización in situ de Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8

Last Updated: 2021-02-26

Red Hat Enterprise Linux 8 Actualización de RHEL 7 a RHEL 8

Instrucciones para una actualización in situ de Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

Legal Notice

Resumen

Este documento proporciona instrucciones sobre cómo realizar una actualización in situ de Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 utilizando la utilidad Leapp. Durante la actualización in situ, el sistema operativo RHEL 7 existente es reemplazado por una versión RHEL 8.

Table of Contents

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO

Red Hat se compromete a sustituir el lenguaje problemático en nuestro código, documentación y propiedades web. Estamos empezando con estos cuatro términos: maestro, esclavo, lista negra y lista blanca. Debido a la enormidad de este esfuerzo, estos cambios se implementarán gradualmente a lo largo de varias versiones próximas. Para más detalles, consulte el mensaje de nuestro CTO Chris Wright .

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT

Agradecemos su opinión sobre nuestra documentación. Por favor, díganos cómo podemos mejorarla. Para ello:

- Para comentarios sencillos sobre pasajes concretos:
  1. Asegúrese de que está viendo la documentación en el formato *Multi-page HTML*. Además, asegúrese de ver el botón **Feedback** en la esquina superior derecha del documento.
  2. Utilice el cursor del ratón para resaltar la parte del texto que desea comentar.
  3. Haga clic en la ventana emergente **Add Feedback** que aparece debajo del texto resaltado.
  4. Siga las instrucciones mostradas.
- Para enviar comentarios más complejos, cree un ticket de Bugzilla:
  1. Vaya al sitio web de Bugzilla.
  2. Como componente, utilice **Documentation**.
  3. Rellene el campo **Description** con su sugerencia de mejora. Incluya un enlace a la(s) parte(s) pertinente(s) de la documentación.
  4. Haga clic en **Submit Bug**.

CAPÍTULO 1. PLANIFICAR UNA ACTUALIZACIÓN

An in-place upgrade is the recommended and supported way to migrate your system to the next major version of RHEL.

Debe tener en cuenta lo siguiente antes de actualizar a RHEL 8:

- **Operating system** - El sistema operativo es actualizado por la utilidad **Leapp** bajo las siguientes condiciones:
  - La variante de servidor instalada del **latest available RHEL 7 version**, que actualmente es:
    - **RHEL 7.9** en las arquitecturas Intel de 64 bits, IBM POWER 8 (little endian) e IBM Z
    - **RHEL 7.6** en arquitecturas que **require kernel version 4.14**: ARM de 64 bits, IBM POWER 9 (little endian), o IBM Z (estructura A)
      Consulte Rutas de actualización in situ compatibles con Red Hat Enterprise Linux para obtener más información.
  - Se cumplen los requisitos mínimos de hardware para RHEL 8
  - Se proporciona acceso al contenido actualizado de RHEL 7.9 y RHEL 8.2; consulte Preparación de un sistema RHEL 7 para la actualización , paso 1 para obtener más detalles.
- **Applications** - Puede migrar las aplicaciones instaladas en su sistema utilizando **Leapp**. Sin embargo, en ciertos casos, tiene que crear actores personalizados, que especifican las acciones que debe realizar **Leapp** durante la actualización, por ejemplo, reconfigurar una aplicación o instalar un controlador de hardware específico. Para obtener más información, consulte Cómo gestionar la migración de sus aplicaciones personalizadas y de terceros. Tenga en cuenta que los actores personalizados no son soportados por Red Hat.
- **Security** - Debe evaluar este aspecto antes de la actualización y tomar medidas adicionales cuando el proceso de actualización se complete. Considere especialmente lo siguiente:
  - Antes de la actualización, defina el estándar de seguridad que debe cumplir su sistema y comprenda los cambios de seguridad en RHEL 8 .
  - Durante el proceso de actualización, la utilidad **Leapp** establece el modo SELinux como permisivo.
  - No se admiten las actualizaciones in situ de los sistemas en modo FIPS.
  - Una vez finalizada la actualización, vuelva a evaluar y aplicar sus políticas de seguridad. Para obtener información sobre la aplicación de políticas de seguridad que se han desactivado durante la actualización o que se han introducido recientemente en RHEL 8, consulte Aplicación de políticas de seguridad .
- **Storage and file systems**- Siempre debes hacer una copia de seguridad de tu sistema antes de actualizarlo. Por ejemplo, puede utilizar la utilidad Relax-and-Recover (ReaR), las instantáneas de LVM, la división de RAID o una instantánea de la máquina virtual.
- **Downtime** - El proceso de actualización puede durar desde varios minutos hasta varias horas.
- **Satellite** - Si gestiona sus hosts a través de Satellite, puede actualizar varios hosts simultáneamente de RHEL 7 a RHEL 8 utilizando la interfaz web de Satellite. Para más información, consulte Actualización de hosts de RHEL 7 a RHEL 8 .

- **Public Clouds** - La actualización in situ es compatible con instancias bajo demanda en Amazon Web Services (AWS) y Microsoft Azure, utilizando Red Hat Update Infrastructure (RHUI) .
- **Known limitations** - Entre las limitaciones conocidas de **Leapp** se encuentran actualmente:
  - El cifrado de todo el disco o de una partición, o el cifrado del sistema de archivos no puede utilizarse actualmente en un sistema destinado a una actualización in situ.
  - No se puede utilizar ningún tipo de montaje de almacenamiento en red como partición del sistema (por ejemplo, iSCSI o NFS).
  - La actualización in situ no es actualmente compatible con las instancias bajo demanda en las restantes nubes públicas (Huawei Cloud, Alibaba Cloud, Google Cloud) que utilizan Red Hat Update Infrastructure pero no Red Hat Subscription Manager para una suscripción a RHEL.

Véase también Problemas conocidos.

Puede utilizar **Red Hat Insights** para determinar cuál de los sistemas que ha registrado en Insights se encuentra en una ruta de actualización compatible con RHEL 8. Para ello, navegue hasta la recomendación del Asesor correspondiente en Insights, active la recomendación en el menú desplegable *Actions* e inspeccione la lista bajo el encabezado *Affected systems*. Tenga en cuenta que la recomendación del Asesor sólo tiene en cuenta la versión menor de RHEL 7 y no realiza una evaluación previa a la actualización del sistema.

CAPÍTULO 2. PREPARACIÓN DE UN SISTEMA RHEL 7 PARA LA ACTUALIZACIÓN

Este procedimiento describe los pasos necesarios antes de realizar una actualización in situ a RHEL 8 mediante la utilidad **Leapp**.

Si no tiene previsto utilizar Red Hat Subscription Manager durante el proceso de actualización, siga las instrucciones de Actualización a RHEL 8 sin Red Hat Subscription Manager .

Requisitos previos

- El sistema cumple las condiciones indicadas en Planificación de una actualización .

Procedimiento

1. Asegúrese de que su sistema se ha registrado correctamente en Red Hat Content Delivery Network (CDN) o en Red Hat Satellite 6.5 o posterior mediante Red Hat Subscription Manager.

IMPORTANTE

Si su sistema está registrado en el Servidor Satélite, asegúrese de que éste cumple las siguientes condiciones:

a. Satellite tiene un manifiesto de suscripción con los repositorios de RHEL 8 importados. Para más información, consulte el capítulo *Managing Subscriptions* en el *Content Management Guide* para la versión particular de Red Hat Satellite , por ejemplo, para la versión 6.8.

b. Los siguientes repositorios están habilitados y sincronizados con las últimas actualizaciones, y publicados en Satellite:

- Red Hat Enterprise Linux 7 Server RPMs x86_64 **7** o Red Hat Enterprise Linux 7 Server RPMs x86_64 **7.9**
- Red Hat Enterprise Linux 7 Server - Extras (RPMs)
- Red Hat Enterprise Linux 8 para x86_64 - AppStream RPMs x86_64 **8.2**
- Red Hat Enterprise Linux 8 para x86_64 - BaseOS RPMs x86_64 **8.2**
  Para más información, consulte el capítulo *Importing Red Hat Content* en el sitio web *Content Management Guide* para la versión particular de Red Hat Satellite, por ejemplo, para la versión 6.8.

c. El host de contenido pertenece a uno de los siguientes:

- Una vista de contenido que contiene los repositorios RHEL 7 y RHEL 8 mencionados anteriormente.
- La vista de contenido de la organización por defecto y el entorno del ciclo de vida de la biblioteca.
  Para más información, consulte el capítulo *Managing Content Views* en el sitio web *Content Management Guide* para la versión particular de Red Hat Satellite, por ejemplo, para la versión 6.8.

2. Compruebe que tiene conectada la suscripción a Red Hat Enterprise Linux Server :

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name:   Red Hat Enterprise Linux Server
Product ID:     69
Version:        7.9
Arch:           x86_64
Status:         Subscribed
```

Debería ver *Server* en el nombre del producto y *Subscribed* como estado.

3. Asegúrese de que tiene activados los repositorios adecuados. Los siguientes comandos enumeran los repositorios para la arquitectura Intel de 64 bits; para otras arquitecturas, consulte los repositorios de RHEL 7 .

   a. Habilitar el repositorio Base:

   ```
   # subscription-manager repos --enable rhel-7-server-rpms
   ```

   b. Habilite el repositorio de Extras donde **Leapp** y sus dependencias están disponibles:

   ```
   # subscription-manager repos --enable rhel-7-server-extras-rpms
   ```

   NOTA

   También puede tener habilitados los repositorios Opcional o Suplementario; vea su lista en los repositorios de RHEL 7. En tal caso, **Leapp** habilita el RHEL 8 CodeReady Linux Builder o los repositorios RHEL 8 Supplementary, respectivamente.

4. Configure el Red Hat Subscription Manager para que consuma el último contenido de RHEL 7:

   ```
   # subscription-manager release --unset
   ```

5. Opcional: Si desea utilizar repositorios personalizados, configúrelos según las instrucciones en Configuración de repositorios personalizados .

6. Si utiliza el complemento **yum-plugin-versionlock** para bloquear los paquetes a una versión específica, borre el bloqueo ejecutando:

   ```
   # yum versionlock clear
   ```

   Consulte ¿Cómo restringir yum para que instale o actualice un paquete a una versión específica fija? para obtener más información.

7. Asegúrese de que tiene la configuración regional del sistema en **en_US.UTF-8**:

   ```
   $ cat /etc/locale.conf
   ```

   Si la configuración regional es diferente, siga las instrucciones en ¿Cómo cambiar la configuración regional del sistema en RHEL7?

8. Si está actualizando utilizando Red Hat Update Infrastructure (RHUI) en una nube pública, complete las siguientes tareas para asegurarse de que su sistema está listo para la actualización.

   a. Para AWS, active el repositorio de Red Hat Update Infrastructure 3 Client Configuration Server 7 e instale los paquetes RHUI necesarios.

      i. Para arquitecturas no ARM:

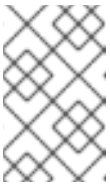
      ```
      # yum-config-manager --enable rhui-client-config-server-7
      # yum -y install rh-amazon-rhui-client leapp-rhui-aws
      ```

      ii. Para la arquitectura ARM:

      ```
      # yum-config-manager --enable rhui-client-config-server-7-arm
      # yum -y install rh-amazon-rhui-client-arm leapp-rhui-aws
      ```

   b. Para Microsoft Azure, active los RPMs de Microsoft Azure para el repositorio de Red Hat Enterprise Linux 7 e instale los paquetes RHUI necesarios.

   ```
   # yum-config-manager --enable rhui-microsoft-azure-rhel7
   # yum -y install rhui-azure-rhel7 leapp-rhui-azure
   ```

   NOTA

   Si ha bloqueado la máquina virtual (VM) de Azure a una versión menor, elimine el bloqueo de la versión. Para obtener más información, consulte Cambiar una máquina virtual RHEL 7.x a una versión no EUS .

9. Si gestiona contenedores en Docker, recree esos contenedores con las imágenes de contenedor apropiadas utilizando Podman y luego adjunte cualquier volumen en uso. Para más información, consulte ¿Cómo puedo migrar mis contenedores Docker a Podman antes de pasar de Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8?

10. Actualice todos los paquetes a la última versión de RHEL 7:

    ```
    # yum update
    ```

11. Reinicia el sistema:

    ```
    # reboot
    ```

12. Instale la utilidad **Leapp**:

    ```
    # yum install leapp leapp-repository
    ```

    Tenga en cuenta que actualmente necesita la versión 0.11.1 o posterior del paquete **leapp** y la versión 0.12.0 o posterior del paquete **leapp-repository**.

13. Descargue los archivos de datos adicionales necesarios (cambios en los paquetes RPM y asignación de repositorios RPM) adjuntos al artículo de la base de conocimientos Datos requeridos por la utilidad Leapp para una actualización in situ de RHEL 7 a RHEL 8 y colóquelos

en el directorio **/etc/leapp/files/**. Esto es necesario para una actualización exitosa. Tenga en cuenta que actualmente necesita los archivos de datos del archivo **leapp-data12.tar.gz** o posterior.

NOTA

Si está actualizando en una nube pública utilizando RHUI y no tiene una suscripción a Red Hat o una cuenta en el Portal del Cliente de Red Hat, cree una suscripción de desarrollador de RHEL sin coste para poder acceder al artículo de la base de conocimientos y descargar los paquetes de datos necesarios. Para obtener más información, consulte ¿Cómo puedo obtener una suscripción de desarrollador de Red Hat Enterprise Linux sin coste o renovarla?

14. Asegúrese de que tiene cualquier gestión de la configuración (como **Salt**, **Chef**, **Puppet**, **Ansible**) deshabilitada o adecuadamente reconfigurada para no intentar restaurar el sistema RHEL 7 original.

15. Asegúrese de que su sistema no utiliza más de una tarjeta de interfaz de red (NIC) con un nombre basado en el prefijo utilizado por el kernel (**eth**). Para obtener instrucciones sobre cómo migrar a otro esquema de nomenclatura antes de una actualización in situ a RHEL 8, consulte Cómo realizar una actualización in situ a RHEL 8 cuando se utilizan nombres de NIC del kernel en RHEL 7.

16. Asegúrese de tener una copia de seguridad completa del sistema o una instantánea de la máquina virtual. Debería poder devolver su sistema al estado anterior a la actualización si sigue los procedimientos estándar de recuperación de desastres en su entorno. Por ejemplo, puede utilizar la utilidad Relax-and-Recover (ReaR). Para obtener más información, consulte la documentación de ReaR y ¿Qué es Relax and Recover (ReaR) y cómo puedo utilizarlo para la recuperación de desastres? Como alternativa, puede utilizar las instantáneas LVM, o la división de RAID. En caso de actualizar una máquina virtual, puede crear una instantánea de toda la VM.

CAPÍTULO 3. REVISIÓN DEL INFORME PREVIO A LA ACTUALIZACIÓN

Para evaluar la capacidad de actualización de su sistema, inicie el proceso de preactualización mediante el comando **leapp preupgrade**. Durante esta fase, la utilidad **Leapp** recopila datos sobre el sistema, evalúa la capacidad de actualización y genera un informe de preactualización.

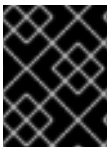
El informe previo a la actualización está disponible tanto en el archivo **/var/log/leapp/leapp-report.txt** como en la consola web. El informe resume los posibles problemas y propone soluciones recomendadas. El informe también le ayuda a decidir si es posible o aconsejable proceder a la actualización.

En ciertas configuraciones, **Leapp** genera preguntas de verdadero/falso para determinar cómo proceder. Todas las preguntas se almacenan en **/var/log/leapp/answerfile** y en el informe previo a la actualización en el mensaje **Missing required answers in the answer file**. **Leapp** inhibe la actualización si no se proporcionan respuestas a todas las preguntas.

Tiene dos opciones a la hora de evaluar la capacidad de actualización en la fase previa a la misma:

a. Revise el informe previo a la actualización en el archivo generado **leapp-report.txt** y resuelva manualmente los problemas notificados mediante la interfaz de línea de comandos.

b. Utilice la consola web para revisar el informe, aplicar correcciones automáticas cuando estén disponibles y solucionar los problemas restantes utilizando las sugerencias de corrección.



IMPORTANTE

Durante la fase de preactualización, **Leapp** no simula todo el proceso de actualización in situ ni descarga todos los paquetes RPM.

La revisión de un informe de preactualización también es útil si decide o necesita volver a desplegar un sistema RHEL 8 sin el proceso de actualización in situ.

3.1. EVALUACIÓN DE LA CAPACIDAD DE ACTUALIZACIÓN DESDE LA LÍNEA DE COMANDOS

Identifique los posibles problemas de actualización durante la fase previa a la misma mediante la interfaz de línea de comandos.

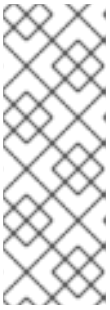
Requisitos previos

- Se han completado los pasos indicados en Preparación de un sistema RHEL 7 para la actualización.

Procedimiento

1. En su sistema RHEL 7, realice la fase de preactualización:

```
# leapp preupgrade
```



NOTA

Si va a utilizar repositorios personalizados del directorio **/etc/yum.repos.d/** para la actualización, habilite los repositorios seleccionados como sigue:

```
# leapp preupgrade --enablerepo repository_id1 --enablerepo repository_id2...
```

Si vas a actualizar sin RHSM o usando RHUI, añade la opción **--no-rhsm**.

2. Responda a cada una de las preguntas requeridas por **Leapp** por cualquiera de los siguientes métodos:

   a. Ejecute el comando **leapp answer**, especificando la pregunta a la que responde y su respuesta confirmada.

   ```
   # leapp answer --section question_section.confirm=answer
   ```

   Por ejemplo, para confirmar una respuesta **True** a la pregunta **Disable pam_pkcs11 module in PAM configuration?**, ejecute el siguiente comando:

   ```
   # leapp answer --section remove_pam_krb5_module_check.confirm=True
   ```

   b. Edite manualmente el archivo **/var/log/leapp/answerfile**, descomente la línea **confirm** del archivo borrando el símbolo **#**, y confirme su respuesta como **True** o **False**; vea Leapp answerfile.

1. Examine el informe en el archivo **/var/log/leapp/leapp-report.txt** y resuelva manualmente todos los problemas notificados antes de proceder a la actualización in situ.

3.2. EVALUACIÓN DE LA CAPACIDAD DE ACTUALIZACIÓN Y APLICACIÓN DE CORRECCIONES AUTOMÁTICAS A TRAVÉS DE LA CONSOLA WEB

Identificar los posibles problemas en la fase previa a la actualización y cómo aplicar correcciones automáticas mediante la consola web.

Requisitos previos

- Se han completado los pasos indicados en Preparación de un sistema RHEL 7 para la actualización.

Procedimiento

1. Instale el complemento **cockpit-leapp**:

   ```
   # yum install cockpit-leapp
   ```

2. Vaya a la consola web en su navegador e inicie sesión como **root** o como un usuario configurado en el archivo **/etc/sudoers**. Para obtener más información sobre la consola web, consulte Administración de sistemas mediante la consola web de RHEL 7 .

3. En su sistema RHEL 7, realice la fase de preactualización desde la interfaz de línea de comandos o desde el terminal de la consola web:

```
# leapp preupgrade
```

NOTA

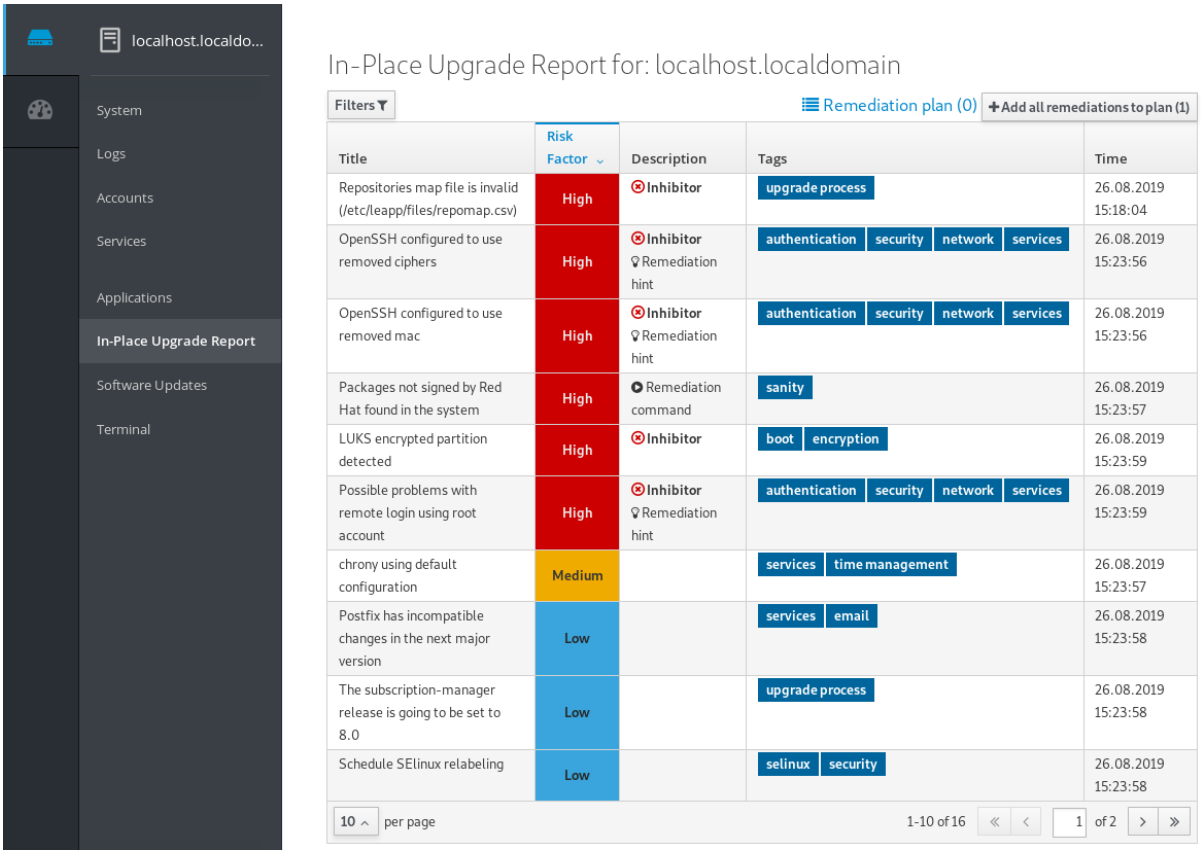
Si va a utilizar repositorios personalizados del directorio **/etc/yum.repos.d/** para la actualización, habilite los repositorios seleccionados como sigue:

```
# leapp preupgrade --enablerepo repository_id1 --enablerepo repository_id2...
```

Si vas a actualizar sin RHSM o usando RHUI, añade la opción **--no-rhsm**.

4. En la consola web, seleccione **Informe de actualización in situ** en el menú de la izquierda.

Figura 3.1. Informe de actualización en la consola web



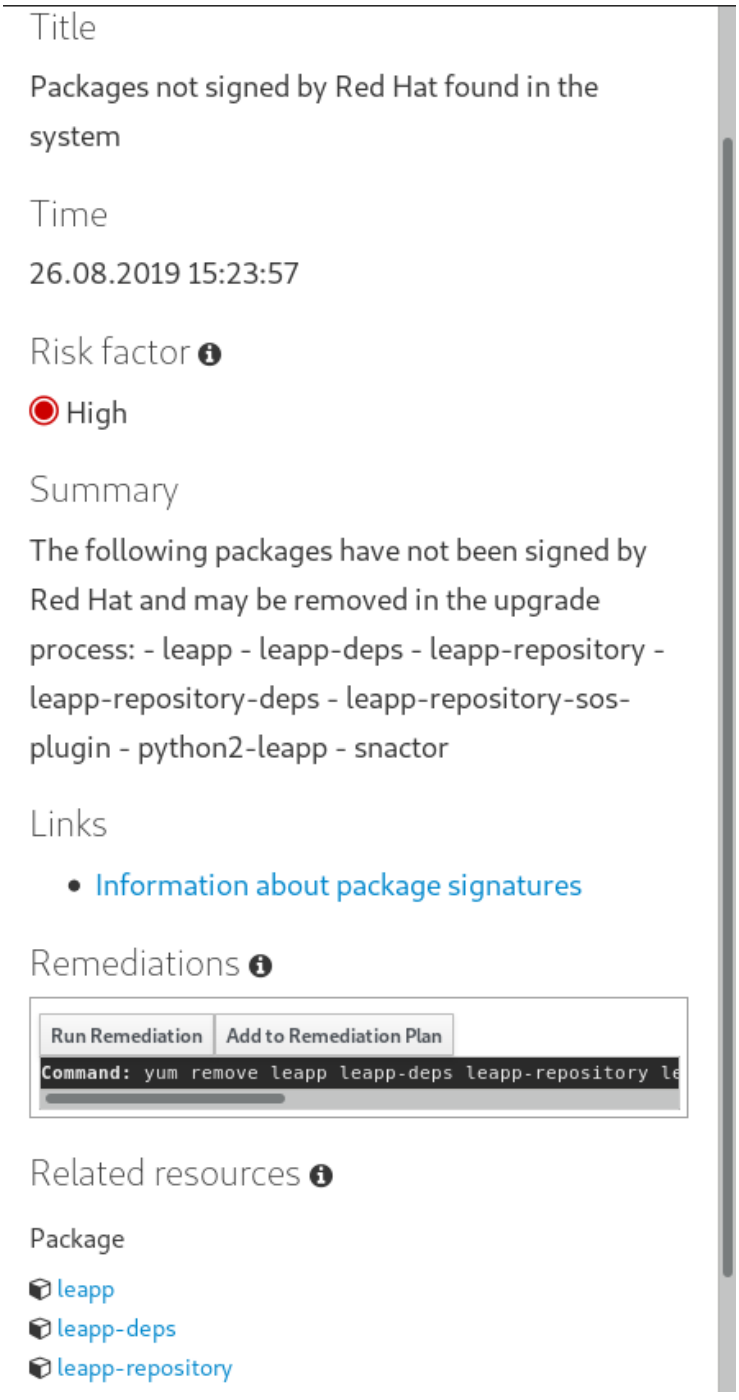
La tabla del informe ofrece una visión general de los problemas encontrados, su evaluación de riesgo y las soluciones (si están disponibles).

- Factor de riesgo:
  - Alto: es muy probable que el estado del sistema se deteriore
  - Medio: puede afectar tanto al sistema como a las aplicaciones
  - Baja: no debería afectar al sistema, pero puede tener un impacto en las aplicaciones
- Inhibidor: inhibe (detiene) el proceso de actualización, de lo contrario el sistema podría quedar inutilizado, inaccesible o disfuncional
- Remediación - una solución procesable para un problema reportado:

- Comando de remediación - puede ser ejecutado directamente a través de la consola web
- Sugerencia de solución: instrucciones sobre cómo resolver el problema manualmente

5. Examine el contenido del informe. Puede ordenar la tabla haciendo clic en una cabecera. Para abrir un panel detallado, haga clic en una fila seleccionada.

Figura 3.2. Panel de detalles



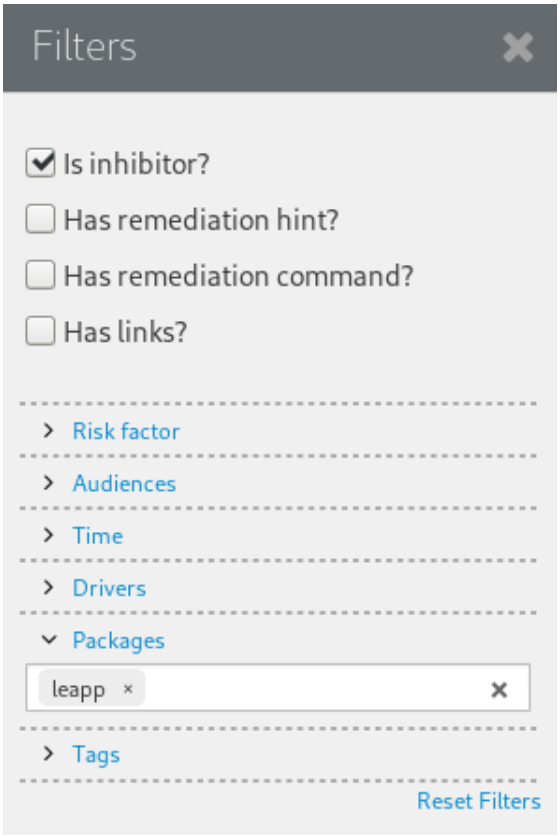
El panel de detalles muestra la siguiente información adicional:

- Resumen del problema y enlaces a los artículos de la base de conocimientos que describen el problema con más detalle
- Correcciones: puede ejecutar o programar una corrección automática (si está disponible), y ver sus resultados cuando se aplique

- Recursos del sistema afectados: paquetes, repositorios, archivos (configuración, datos), discos, volúmenes

6. Si lo desea, puede filtrar los resultados. Haga clic en el botón **Filtros** en la esquina superior izquierda sobre el informe y aplique un filtro basado en sus preferencias. Las categorías de filtros se aplican conjuntamente.

Figura 3.3. Filtros



7. Seleccione los problemas a los que desea aplicar una corrección automática. Tiene dos opciones:

   a. Elija elementos individuales haciendo clic en el botón **Añadir al plan de corrección** en el panel de detalles. También puede ejecutar directamente las correcciones individuales haciendo clic en **Ejecutar corrección** en el panel de detalles.

   b. Seleccione todos los elementos para los que se dispone de una corrección haciendo clic en el botón **Añadir todas las correcciones al plan** en la esquina superior derecha sobre el informe.

8. Revise y responda las preguntas requeridas por **Leapp** en la consola web. Cada pregunta sin responder aparece como un título de **Missing required answers in the answer file** en el informe de actualización. Seleccione un título para responder a la pregunta:

   a. Para confirmar la respuesta predeterminada **True**, seleccione **Añadir al plan de corrección** para ejecutar la corrección más tarde o **Ejecutar corrección** para ejecutar la corrección inmediatamente.

   b. Para seleccionar la respuesta no predeterminada en su lugar, realice una de las siguientes acciones:

      i. Ejecute el comando **leapp answer**, especificando la pregunta a la que responde y su respuesta confirmada.

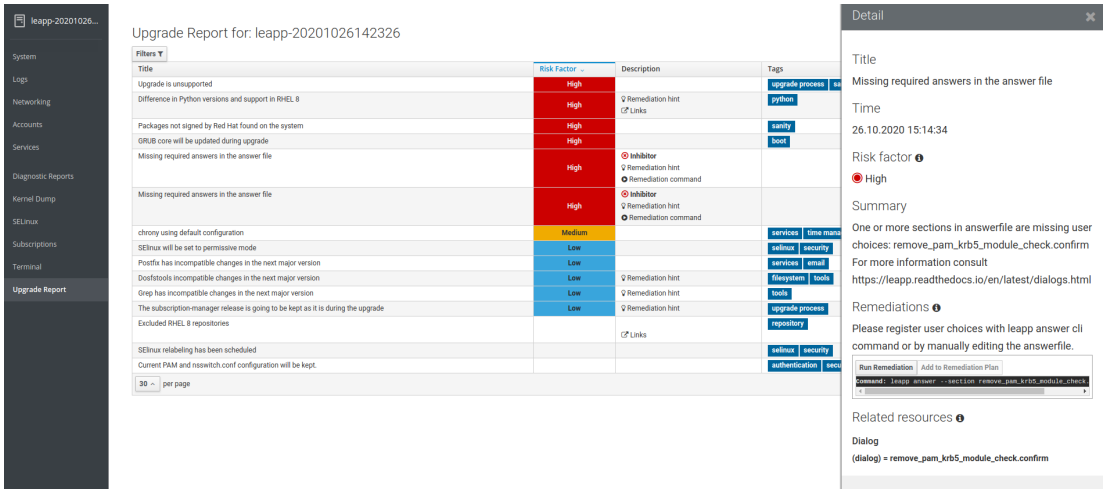
```
# leapp answer --section question_section.confirm=answer
```

Por ejemplo, para confirmar una respuesta **False** a la pregunta **Disable pam_pkcs11 module in PAM configuration?**, ejecute el siguiente comando:

```
# leapp answer --section remove_pam_krb5_module_check.confirm=False
```

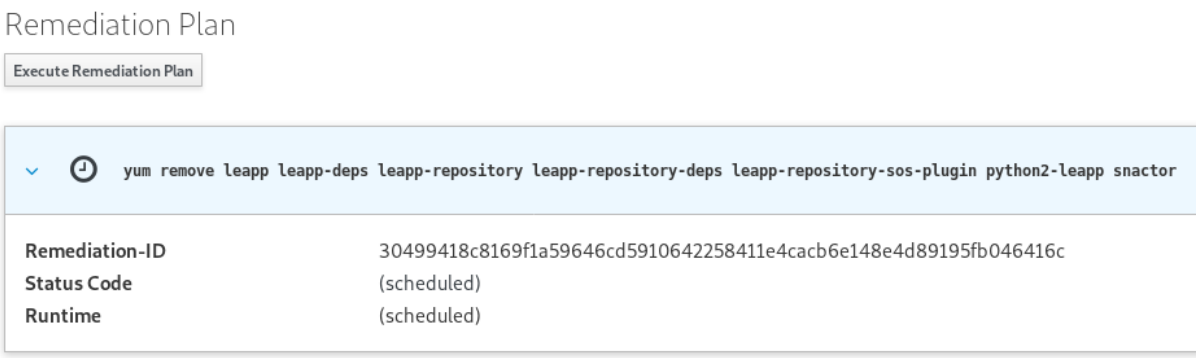
ii. Edite manualmente el archivo **/var/log/leapp/answerfile**, descomente la línea **confirm** del archivo borrando el símbolo **#**, y confirme su respuesta como **True** o **False**; vea el ejemplo del archivo de respuesta de Leapp .

Figura 3.4. Pregunta pendiente de Leapp



9. Abra el plan de corrección haciendo clic en el enlace **Plan de corrección** en la esquina superior derecha sobre el informe. El plan de corrección ofrece una lista de todas las correcciones ejecutadas o programadas.

Figura 3.5. Plan de remediación



10. Procese todas las correcciones programadas haciendo clic en **Ejecutar plan de corrección**. Se muestra la siguiente información para cada entrada de corrección:

- Una identificación única de la reparación
- Estado de salida del comando
- Tiempo transcurrido de la reparación ejecutada
- Salida estándar
- Error estándar

11. Después de ejecutar las correcciones seleccionadas, vuelva a generar el informe previo a la actualización mediante el comando **leapp preupgrade**, examine el nuevo informe y tome medidas de corrección adicionales si es necesario.

CAPÍTULO 4. REALIZACIÓN DE LA ACTUALIZACIÓN DE RHEL 7 A RHEL 8

Actualice a RHEL 8 utilizando la utilidad **Leapp**.

Requisitos previos

- Se han completado los pasos indicados en Preparación de un sistema RHEL 7 para la actualización, incluida una copia de seguridad completa del sistema.
- Se han completado los pasos indicados en Revisión del informe previo a la actualización y se han resuelto todos los problemas notificados.

Procedimiento

1. En su sistema RHEL 7, inicie el proceso de actualización:

```
# leapp upgrade
```

NOTA

Si va a utilizar repositorios personalizados del directorio **/etc/yum.repos.d/** para la actualización, habilite los repositorios seleccionados como sigue:

```
# leapp upgrade --enablerepo repository_id1 --enablerepo repository_id2...
```

Si vas a actualizar sin RHSM o usando RHUI, añade la opción **--no-rhsm**.

Al inicio del proceso de actualización, **Leapp** realiza la fase de preactualización descrita en Revisión del informe de preactualización

Si el sistema es actualizable, **Leapp** descarga los datos necesarios y prepara una transacción RPM para la actualización.

Si su sistema no cumple los parámetros para una actualización fiable, **Leapp** termina el proceso de actualización y proporciona un registro que describe el problema y una solución recomendada en el archivo **/var/log/leapp/leapp-report.txt**. Para obtener más información, consulte Solución de problemas.

2. Reinicie manualmente el sistema:

```
# reboot
```

En esta fase, el sistema arranca en una imagen de disco RAM inicial basada en RHEL 8, initramfs. **Leapp** actualiza todos los paquetes y se reinicia automáticamente en el sistema RHEL 8.

También puede ejecutar el comando **leapp upgrade** con la opción **--reboot** y saltarse este paso manual.

Si se produce un fallo, investigue los registros como se describe en Solución de problemas.

3. Inicie sesión en el sistema RHEL 8 y verifique su estado como se describe en Verificación del estado posterior a la actualización del sistema RHEL 8.

4. Realice las tareas posteriores a la actualización como se describe en Realización de tareas posteriores a la actualización. Especialmente, reevalúe y vuelva a aplicar sus políticas de seguridad.

CAPÍTULO 5. VERIFICACIÓN DEL ESTADO POSTERIOR A LA ACTUALIZACIÓN DEL SISTEMA RHEL 8

Este procedimiento enumera los pasos de verificación que se recomienda realizar tras una actualización in situ a RHEL 8.

Requisitos previos

- El sistema se ha actualizado siguiendo los pasos descritos en Realización de la actualización de RHEL 7 a RHEL 8 y ha podido iniciar sesión en RHEL 8.

Procedimiento

Una vez completada la actualización, determine si el sistema está en el estado requerido, como mínimo:

- Compruebe que la versión actual del sistema operativo es Red Hat Enterprise Linux 8:

```
# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.2 (Ootpa)
```

- Compruebe la versión del núcleo del sistema operativo:

```
# uname -r
4.18.0-193.el8.x86_64
```

  Tenga en cuenta que **.el8** es importante.

- Si está utilizando el Red Hat Subscription Manager:
  - Verifique que se ha instalado el producto correcto:

```
# subscription-manager list --installed
+-------------------------------------------+
    Installed Product Status
+-------------------------------------------+
Product Name: Red Hat Enterprise Linux for x86_64
Product ID:   479
Version:      8.2
Arch:         x86_64
Status:       Subscribed
```

  - Compruebe que la versión de lanzamiento se establece en 8.2 inmediatamente después de la actualización:

```
# subscription-manager release
Release: 8.2
```

- Compruebe que los servicios de red están operativos, por ejemplo, intente conectarse a un servidor mediante SSH.

- Compruebe el estado posterior a la actualización de sus aplicaciones. En algunos casos, es posible que tenga que realizar la migración y los cambios de configuración manualmente. Por ejemplo, para migrar sus bases de datos, siga las instrucciones de la documentación de los servidores de bases de datos de RHEL 8.

CAPÍTULO 6. REALIZACIÓN DE TAREAS POSTERIORES A LA ACTUALIZACIÓN

Este procedimiento enumera las principales tareas que se recomienda realizar tras una actualización in situ a RHEL 8.

Requisitos previos

- El sistema se ha actualizado siguiendo los pasos descritos en Realización de la actualización de RHEL 7 a RHEL 8 y ha podido iniciar sesión en RHEL 8.
- Se ha verificado el estado de la actualización in situ siguiendo los pasos descritos en Verificación del estado posterior a la actualización del sistema RHEL 8.

Procedimiento

Después de realizar la actualización, complete las siguientes tareas:

1. Asegúrese de que su sistema sigue siendo compatible después de la actualización in situ. Con la disponibilidad general de RHEL 8.3, actualice su sistema a RHEL 8.3 o a RHEL 8.2 Extended Update Support (EUS).
   a. Actualice el sistema a RHEL 8.3:
      i. Desactive Red Hat Subscription Manager para consumir el último contenido de RHEL 8.3:

      ```
      # subscription-manager release --unset
      ```

      ii. Actualice su sistema a la última versión de RHEL 8.3:

      ```
      # yum update
      ```

   b. Actualice el sistema a RHEL 8.2 EUS:
      i. Habilitar los repositorios EUS de RHEL 8:

      ```
      # subscription-manager repos --enable repository_id1 --enable repository_id2 ..
      ```

      Sustituya *repository_id** por los ID de los repositorios EUS disponibles con su suscripción. Habilite al menos los repositorios BaseOS y AppStream. Por ejemplo, en la arquitectura Intel 64:

      ```
      # subscription-manager repos --enable  rhel-8-for-x86_64-baseos-eus-rpms --enable rhel-8-for-x86_64-appstream-eus-rpms
      ```

      ii. Actualice su sistema a la última versión de RHEL 8.2.EUS

      ```
      # yum update
      ```

2. Si ha actualizado utilizando RHUI en AWS o Microsoft Azure y su certificación de software no está disponible en una versión menor posterior, bloquee su sistema en una versión menor compatible con su certificación.

```
# echo '8.x' > /etc/yum/vars/releasever
```

3. Reevalúe y vuelva a aplicar sus políticas de seguridad. Especialmente, cambie el modo de SELinux a enforcing. Para más detalles, consulte Aplicación de políticas de seguridad.

CAPÍTULO 7. APLICACIÓN DE POLÍTICAS DE SEGURIDAD

Durante el proceso de actualización in situ, algunas políticas de seguridad deben permanecer desactivadas. Además, RHEL 8 introduce un nuevo concepto de políticas criptográficas en todo el sistema y también los perfiles de seguridad pueden contener cambios entre las versiones principales. Esta sección le guiará a la hora de asegurar sus sistemas RHEL actualizados.

7.1. CAMBIAR EL MODO DE SELINUX A FORZOSO

Durante el proceso de actualización in situ, la utilidad **Leapp** establece el modo SELinux como permisivo. Cuando el sistema se actualiza con éxito, hay que cambiar manualmente el modo SELinux a enforcing.

Requisitos previos

- El sistema se ha actualizado y usted ha realizado los pasos de verificación descritos en Verificación del estado posterior a la actualización del sistema RHEL 8 .

Procedimiento

1. Asegúrese de que no hay denegaciones de SELinux, por ejemplo, utilizando la utilidad **ausearch**:

```
# ausearch -m AVC,USER_AVC -ts boot
```

   Tenga en cuenta que el paso anterior sólo cubre el escenario más común. Para comprobar todas las posibles denegaciones de SELinux, consulte la sección Identificación de denegaciones de SELinux en el título Uso de SELinux, que proporciona un procedimiento completo.

2. Abra el archivo **/etc/selinux/config** en un editor de texto de su elección, por ejemplo:

```
# vi /etc/selinux/config
```

3. Configure la opción **SELINUX=enforcing**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

4. Guarde el cambio y reinicie el sistema:

```
# reboot
```

Pasos de verificación

1. Después de reiniciar el sistema, confirme que el comando **getenforce** devuelve **Enforcing**:

```
$ getenforce
Enforcing
```

Recursos adicionales

- Solución de problemas relacionados con SELinux
- Cambio de estados y modos de SELinux

7.2. ESTABLECIMIENTO DE POLÍTICAS CRIPTOGRÁFICAS EN TODO EL SISTEMA

Las políticas criptográficas son un componente del sistema que configura los subsistemas criptográficos principales, que abarcan los protocolos TLS, IPSec, SSH, DNSSec y Kerberos.

Después de una instalación exitosa o de un proceso de actualización in situ, la política criptográfica de todo el sistema se establece automáticamente en **DEFAULT**. El nivel de política criptográfica de todo el sistema **DEFAULT** ofrece una configuración segura para los modelos de amenaza actuales.

Para ver o cambiar la política criptográfica actual de todo el sistema, utilice la herramienta update-crypto-policies:

```
$ update-crypto-policies --show
DEFAULT
```

Por ejemplo, el siguiente comando cambia el nivel de política criptográfica de todo el sistema a **FUTURE**, que debería resistir cualquier ataque futuro a corto plazo:

```
# update-crypto-policies --set FUTURE
Setting system policy to FUTURE
```

RHEL 8.2 también introduce la personalización de las políticas criptográficas de todo el sistema. Para obtener más detalles, consulte las secciones Personalización de políticas criptográficas de todo el sistema con modificadores de políticas y Creación y configuración de una política criptográfica personalizada de todo el sistema.

Recursos adicionales

- Uso de políticas criptográficas en todo el sistema
- **update-crypto-policies(8)** página de manual.

7.3. REMEDIAR EL SISTEMA A UNA LÍNEA DE BASE DE SEGURIDAD

El paquete OpenSCAP proporciona correcciones para que su sistema cumpla con las líneas de base de seguridad, como PCI-DSS, OSPP o ACSC E8. Utilice los pasos del siguiente procedimiento para cambiar la configuración de su sistema para que se ajuste al perfil PCI-DSS.

IMPORTANTE

Red Hat no proporciona ningún método automatizado para revertir los cambios realizados por las correcciones de seguridad. Las remediaciones son compatibles con los sistemas RHEL en la configuración por defecto. Si su sistema ha sido alterado después de la instalación, la ejecución de la remediación podría hacer que no cumpla con el perfil de seguridad requerido.

Requisitos previos

- El paquete **scap-security-guide** está instalado en su sistema RHEL 8.

Procedimiento

1. Utilice el comando **oscap** con la opción **--remediate**:

```
# oscap xccdf eval --profile pci-dss --remediate /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

   Puede sustituir *pci-dss* en el ejemplo anterior por un perfil requerido por su escenario.

2. Reinicie su sistema:

```
# reboot
```

Pasos de verificación

1. Evaluar el sistema de cómo cumple con el perfil PCI-DSS, y guardar los resultados en el archivo *pcidss_report.html*:

```
$ oscap xccdf eval --report pcidss_report.html --profile pci-dss /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

Recursos adicionales

- Escanear el sistema para comprobar el cumplimiento de la seguridad y las vulnerabilidades
- **scap-security-guide(8)** página de manual
- **oscap(8)** páginas de manual

CAPÍTULO 8. SOLUCIÓN DE PROBLEMAS

Puede consultar los siguientes consejos para solucionar los problemas de actualización de RHEL 7 a RHEL 8.

8.1. RECURSOS PARA LA RESOLUCIÓN DE PROBLEMAS

Puede consultar los siguientes recursos para la resolución de problemas.

Console output

Por defecto, la utilidad **Leapp** sólo imprime en la consola los mensajes de nivel de registro de error y crítico. Para cambiar el nivel de registro, utilice las opciones **--verbose** o **--debug** con el comando **leapp upgrade**.

- En el modo *verbose*, **Leapp** imprime mensajes de información, advertencia, error y crítica.
- En el modo *debug*, **Leapp** imprime mensajes de depuración, información, advertencia, error y crítica.

Logs

- El archivo **/var/log/leapp/leapp-upgrade.log** enumera los problemas encontrados durante la fase de initramfs.
- El directorio **/var/log/leapp/dnf-debugdata/** contiene datos de depuración de transacciones. Este directorio sólo está presente si el comando **leapp upgrade** se ejecuta con la opción **--debug**.
- El sitio web **/var/log/leapp/answerfile** contiene las preguntas que debe responder **Leapp**.
- La utilidad **journalctl** proporciona registros completos.

Reports

- El archivo **/var/log/leapp/leapp-report.txt** enumera los problemas encontrados durante la fase previa a la actualización. El informe también está disponible en la consola web, véase Evaluación de la capacidad de actualización y aplicación de correcciones automáticas a través de la consola web.

8.2. CONSEJOS PARA LA RESOLUCIÓN DE PROBLEMAS

Puede consultar los siguientes consejos para la resolución de problemas.

Pre-upgrade phase

- Compruebe que su sistema cumple todas las condiciones indicadas en Planificación de una actualización.
- Asegúrese de haber seguido todos los pasos descritos en Preparación de un sistema RHEL 7 para la actualización por ejemplo, su sistema no utiliza más de una tarjeta de interfaz de red (NIC) con un nombre basado en el prefijo utilizado por el kernel (**eth**).
- Asegúrese de haber respondido a todas las preguntas requeridas por **Leapp** en el archivo **/var/log/leapp/answerfile**. Si falta alguna respuesta, **Leapp** impide la actualización. Ejemplo de preguntas:

- ¿Desactivar el módulo pam_pkcs11 en la configuración de PAM?
- ¿Desactivar el módulo pam_krb5 en la configuración de PAM?
- Configurar PAM y nsswitch.conf con la siguiente llamada authselect?

- Asegúrese de que ha resuelto todos los problemas identificados en el informe previo a la actualización, situado en **/var/log/leapp/leapp-report.txt**. Para ello, también puede utilizar la consola web, como se describe en Evaluación de la capacidad de actualización y aplicación de soluciones automáticas a través de la consola web.

Ejemplo 8.1. Perfil de respuesta de la fuga

El siguiente es un ejemplo de un archivo **/var/log/leapp/answerfile** sin editar que tiene una pregunta sin responder:

```
[remove_pam_pkcs11_module_check]
# Title:          None
# Reason:         Confirmation
# ================== remove_pam_pkcs11_module_check.confirm ==================
# Label:          Disable pam_pkcs11 module in PAM configuration? If no, the upgrade process will be interrupted.
# Description:    PAM module pam_pkcs11 is no longer available in RHEL-8 since it was replaced by SSSD.
# Type:           bool
# Default:        None
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
# confirm =
```

El campo **Label** especifica la pregunta que requiere una respuesta. En este ejemplo, la pregunta es **Disable pam_pkcs11 module in PAM configuration?**

Para responder a la pregunta, descomente la línea **confirm** e introduzca una respuesta de **True** o **False**. En este ejemplo, la respuesta seleccionada es **True**:

```
[remove_pam_pkcs11_module_check]
...
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
confirm = True
```

Download phase

- Si se produce un problema durante la descarga de los paquetes RPM, examine los datos de depuración de transacciones ubicados en el directorio **/var/log/leapp/dnf-debugdata/**.

initramfs phase

- Durante esta fase, los posibles fallos le redirigen al shell de Dracut. Comprueba el registro del Diario:

```
# journalctl
```

Alternativamente, reinicie el sistema desde el shell de Dracut utilizando el comando **reboot** y compruebe el archivo **/var/log/leapp/leapp-upgrade.log**.

Post-upgrade phase

- Si su sistema parece haberse actualizado con éxito pero arranca con el antiguo kernel de RHEL 7, reinicie el sistema y compruebe la versión del kernel de la entrada por defecto en GRUB.
- Asegúrese de haber seguido los pasos recomendados en Verificación del estado del sistema RHEL 8 después de la actualización.
- Si su aplicación o un servicio deja de funcionar o se comporta de forma incorrecta después de haber cambiado SELinux al modo de refuerzo, busque las denegaciones utilizando el comando **ausearch**, **journalctl**, o **dmesg** para buscar las denegaciones:

```
# ausearch -m AVC,USER_AVC -ts boot
# journalctl -t setroubleshoot
# dmesg | grep -i -e selinux -e type=1400
```

Los problemas más comunes son causados por un etiquetado incorrecto. Consulte Solución de problemas relacionados con SELinux para obtener más detalles.

8.3. PROBLEMAS CONOCIDOS

Los siguientes son problemas conocidos que puede encontrar al actualizar de RHEL 7 a RHEL 8.

- Actualmente, la agrupación de redes no funciona cuando la actualización in situ se realiza mientras Network Manager está desactivado o no está instalado.
- Si utiliza un proxy HTTP, Red Hat Subscription Manager debe estar configurado para utilizar dicho proxy, o el comando **subscription-manager** debe ser ejecutado con la opción **--proxy <hostname>**. De lo contrario, la ejecución del comando **subscription-manager** falla. Si utiliza la opción **--proxy** en lugar del cambio de configuración, el proceso de actualización falla porque **Leapp** no puede detectar el proxy. Para evitar que ocurra este problema, edite manualmente el archivo **rhsm.conf** como se describe en Cómo configurar el proxy HTTP para la gestión de suscripciones de Red Hat. (BZ#1689294)
- Si su sistema RHEL 7 está instalado en un número de unidad lógica (LUN) FCoE y está conectado a una tarjeta de red que utiliza el controlador **bnx2fc**, el LUN no se detecta en RHEL 8 después de la actualización. En consecuencia, el sistema actualizado no puede arrancar. (BZ#1718147)
- Si su sistema RHEL 7 utiliza un controlador de dispositivo proporcionado por Red Hat pero que no está disponible en RHEL 8, **Leapp** inhibe la actualización. Sin embargo, si el sistema RHEL 7 utiliza un controlador de dispositivo de terceros que no está incluido en la lista de controladores eliminados (ubicada en **/etc/leapp/repos.d/system_upgrade/el7toel8/actors/kernel/checkkerneldrivers/files/removed_drivers.txt**), **Leapp** no detecta dicho controlador y procede con la actualización. En consecuencia, el sistema podría no arrancar después de la actualización.
- No se puede realizar una actualización in situ cuando se utilizan los módulos de Samba **winbind** y **wins** en el archivo **/etc/nsswitch.conf** en este momento. La transacción de actualización falla con los siguientes mensajes de error y **Leapp** inhibe la actualización:

```
upgrade[469]: STDERR:
upgrade[469]: Error in PREIN scriptlet in rpm package unbound-libs
```

```
upgrade[469]: Error: Transaction failed
upgrade[469]: Container el8userspace failed with error code 1.
unbound-libs has a PREIN failure
```

Para solucionar este problema, configure el sistema para que sólo utilice proveedores locales para las bases de datos **user**, **groups** y **hosts** durante la actualización:

1. Abra el archivo de configuración del sistema **/etc/nsswitch.conf** y busque las entradas que contengan las cadenas **winbind** o **wins**.
2. Si encuentra estas entradas, cree una copia de seguridad de **/etc/nsswitch.conf**.
3. Edite **/etc/nsswitch.conf** y elimine **winbind** o **wins** de las entradas que los contienen.
4. Realiza una actualización in situ.
5. Después de la actualización, añada las cadenas **winbind** y **wins** a las entradas respectivas en **/etc/nsswitch.conf**, según los requisitos de configuración de su sistema. (BZ#1410154)

- La utilidad **Leapp** no cambia la configuración de autenticación personalizada durante el proceso de actualización. Si utilizó la utilidad obsoleta **authconfig** para configurar la autenticación en su sistema RHEL 7, es posible que la autenticación en RHEL 8 no funcione correctamente. Para asegurarse de que su configuración personalizada funciona correctamente en el sistema RHEL 8, vuelva a configurar su sistema RHEL 8 con la utilidad **authselect**.

IMPORTANTE

Durante la actualización in situ, se eliminan los módulos de autenticación enchufables (PAM) obsoletos **pam_krb5** o **pam_pkcs11**. En consecuencia, si la configuración de PAM en su sistema RHEL 7 contiene los módulos **pam_krb5** o **pam_pkcs11** y si estos módulos tienen los valores de control **required** o **requisite**, la realización de la actualización in situ podría provocar el bloqueo del sistema. Para solucionar este problema, reconfigure su sistema RHEL 7 para que no utilice **pam_krb5** o **pam_pkcs11** antes de iniciar el proceso de actualización.

- En los sistemas IBM Z, **Leapp** siempre espera que haya un disco DASD conectado. En consecuencia, si el archivo **/etc/dasd.conf** no existe, la actualización in situ falla. Para solucionar este problema, cree un archivo **dasd.conf** vacío utilizando el comando **touch > /etc/dasd.conf**. (BZ#1783248)

- Si el nombre de un paquete de terceros (no firmado por Red Hat) instalado en su sistema es el mismo que el de un paquete proporcionado por Red Hat, la actualización in situ falla. Para evitar este problema, elija una de las siguientes opciones antes de actualizar:

  a. Eliminar el paquete de terceros

  b. Sustituya el paquete de terceros por el paquete proporcionado por Red Hat

- Durante una actualización in situ, el paquete **docker** se elimina sin previo aviso. Si utiliza contenedores en RHEL, migre a Podman antes de actualizar a RHEL 8. Para obtener instrucciones, consulte ¿Cómo puedo migrar mis contenedores Docker a Podman antes de pasar de Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8?(BZ#1858711)

- Por motivos de seguridad, se ha eliminado la compatibilidad con los tipos de cifrado Single-DES (DES) y Triple-DES (3DES) en RHEL 8.3.0. Sin embargo, RHEL 7 Identity Management (IdM)

sigue siendo compatible con el cifrado 3DES.
La actualización de un entorno IdM de RHEL 7 a RHEL 8 es posible porque ambas versiones de RHEL prefieren tipos de cifrado AES más fuertes por defecto:

Versión de IdM	Tipos de encriptación por defecto	Otros tipos de cifrado admitidos
RHEL 7	**aes256-cts** **aes128-cts**	**camellia256-cts** **camellia128-cts** **des3-hmac** **arcfour-hmac**
RHEL 8	**aes256-cts** **aes128-cts**	**aes256-sha2** **aes128-sha2** **camellia256-cts** **camellia128-cts** **arcfour-hmac** [a]

[a] El cifrado RC4 ha sido obviado y deshabilitado por defecto en RHEL 8, ya que se considera menos seguro que los nuevos tipos de cifrado AES-128 y AES-256. Para obtener más información sobre cómo habilitar el soporte de RC4 para la compatibilidad con los entornos de Active Directory heredados, consulte Garantizar el soporte de los tipos de cifrado comunes en AD y RHEL.

Si ha configurado manualmente un Centro de Distribución Kerberos (KDC) que no sea IdM, algún servicio o algún usuario para que **only** utilice el cifrado DES o 3DES, es posible que experimente interrupciones del servicio después de actualizar a los últimos paquetes Kerberos en RHEL 8, como por ejemplo:

- Errores de autenticación de Kerberos
- **unknown enctype** errores de codificación
- Los KDC con claves maestras de base de datos cifradas con DES (**K/M**) no se inician

Red Hat recomienda que no utilice el cifrado DES o 3DES en su entorno. Para obtener más información sobre la recodificación de las entidades de crédito de Kerberos para utilizar tipos de cifrado más potentes, consulte Retirar DES en la documentación de MIT Kerberos.

8.4. OBTENCIÓN DE AYUDAS

Puede abrir un caso de asistencia, seleccionar *RHEL 8* como producto y proporcionar un **sosreport** de su sistema.

- Para generar un **sosreport** en su sistema, ejecute:

```
# sosreport
```

Tenga en cuenta que puede dejar el ID del caso vacío.

Para más detalles sobre la generación de un sosreport, vea la solución ¿Qué es un sosreport y cómo crear uno en Red Hat Enterprise Linux?

Para más información sobre cómo abrir y gestionar un caso de asistencia en el Portal del Cliente, consulte el artículo ¿Cómo abrir y gestionar un caso de asistencia en el Portal del Cliente?

CAPÍTULO 9. INFORMACIÓN RELACIONADA

Puede consultar el siguiente material didáctico:

- Capacidades y límites de la tecnología Red Hat Enterprise Linux
- Consideraciones para adoptar RHEL 8
- Personalización de la actualización in situ de Red Hat Enterprise Linux
- ¿Cómo puedo actualizar de Red Hat Enterprise Linux 6 a Red Hat Enterprise Linux 7?
- Actualización de RHEL 6 a RHEL 8
- Cómo pasar de CentOS u Oracle Linux a RHEL
- Actualización de hosts de RHEL 7 a RHEL 8 en Red Hat Satellite
- Documentación de Red Hat Insights

APÉNDICE A. REPOSITORIOS DE RHEL 7

Antes de la actualización, asegúrese de que tiene habilitados los repositorios adecuados, tal y como se describe en el paso 3 del procedimiento en Preparación de un sistema RHEL 7 para la actualización .

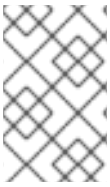
Si planea utilizar Red Hat Subscription Manager durante la actualización, debe **must enable** los siguientes repositorios antes de la actualización utilizando el **subscription-manager repos --enable *repository_id*** comando:

Arquitectura	Repositorio	ID del depósito
Intel de 64 bits	Base	**rhel-7-server-rpms**
	Extras	**rhel-7-server-extras-rpms**
ARM de 64 bits	Base	**rhel-7-for-arm-64-rpms**
	Extras	**rhel-7-for-arm-64-extras-rpms**
IBM POWER8 (little endian)	Base	**rhel-7-for-power-le-rpms**
	Extras	**rhel-7-for-power-le-extras-rpms**
IBM POWER9 (little endian)	Base	**rhel-7-for-power-9-rpms**
	Extras	**rhel-7-for-power-9-extras-rpms**
IBM Z	Base	**rhel-7-for-system-z-rpms**
	Extras	**rhel-7-for-system-z-extras-rpms**
IBM Z (Estructura A)	Base	**rhel-7-for-system-z-a-rpms**
	Extras	**rhel-7-for-system-z-a-extras-rpms**

Usted **can enable** los siguientes repositorios antes de la actualización utilizando el **subscription-manager repos --enable *repository_id*** comando:

Arquitectura	Repositorio	ID del depósito
Intel de 64 bits	Opcional	**rhel-7-server-optional-rpms**

Arquitectura	Repositorio	ID del depósito
	Complemento	**rhel-7-server-supplementary-rpms**
ARM de 64 bits	Opcional	**rhel-7-for-arm-64-optional-rpms**
	Complemento	N/A
IBM POWER8 (little endian)	Opcional	**rhel-7-for-power-le-optional-rpms**
	Complemento	**rhel-7-for-power-le-supplementary-rpms**
IBM POWER9 (little endian)	Opcional	**rhel-7-for-power-9-optional-rpms**
	Complemento	**rhel-7-for-power-9-supplementary-rpms**
IBM Z	Opcional	**rhel-7-for-system-z-optional-rpms**
	Complemento	**rhel-7-for-system-z-supplementary-rpms**
IBM Z (Estructura A)	Opcional	**rhel-7-for-system-z-a-optional-rpms**
	Complemento	N/A



NOTA

Si ha habilitado un repositorio RHEL 7 Optional o RHEL 7 Supplementary antes de una actualización in situ, **Leapp** habilita los repositorios RHEL 8 CodeReady Linux Builder o RHEL 8 Supplementary, respectivamente.

Si decide utilizar repositorios personalizados, habilítelos según las instrucciones en Configuración de repositorios personalizados.