Explicación sobre Leapp

Leapp es una herramienta que cuenta con soporte y que permite actualizar de forma integrada y con confianza el sistema de una versión principal de Red Hat® Enterprise Linux® a otra, y así aprovechar sus funciones nuevas sin tener que reinstalarlo.

Motivos por los que debería actualizar el sistema

Las actualizaciones permiten garantizar el mantenimiento de la continuidad empresarial ya que los clientes aprovechan el soporte, las mejoras, las correcciones y los parches más recientes de los productos, junto con las funciones innovadoras que ofrece cada versión principal nueva de Red Hat Enterprise Linux.

Las mejoras de la plataforma en cuanto al rendimiento disminuyen el costo total de propiedad, influyen en la productividad y le aseguran aprovechar al máximo su inversión en tecnología.

Red Hat Enterprise Linux funciona con un ciclo predecible de versiones principales de tres años, y la suscripción es válida para cualquiera de las versiones actuales compatibles. Por ello, tiene acceso a la tecnología innovadora más reciente, la cual puede aprovechar a medida que están disponibles las versiones nuevas. Todas las versiones principales de Red Hat Enterprise Linux cuentan con diez años de soporte, el cual se divide en dos fases.

En la primera, que tiene lugar los cinco años posteriores a la disponibilidad general (GA), se ofrece soporte completo. Se agregan funciones nuevas, se ofrece compatibilidad con hardware reciente y se corrigen problemas y fallas. En la segunda fase de cinco años, se inicia el soporte de mantenimiento de la versión, en la cual se siguen publicando los errores de seguridad graves o importantes y otras mejoras de correcciones de errores y funciones seleccionadas. Luego del ciclo de vida común de 10 años, los clientes pueden adquirir el complemento Extended Life Cycle Support para obtener dos años adicionales de soporte, incluidos los parches para los errores graves o importantes de seguridad. Consulte la página del ciclo de vida de Red Hat Enterprise Linux para obtener más información.

Los clientes obtienen múltiples funciones nuevas cuando actualizan Red Hat Enterprise Linux, por ejemplo:

- Las bases de datos, los tiempos de ejecución de lenguajes y otras aplicaciones, que se renuevan durante la fase de soporte completo de una versión principal de RHEL cuando se actualiza el sistema de software mediante los flujos de aplicaciones.
- Las herramientas de contenedores de Red Hat Enterprise Linux, como Podman, Buildah y Skopeo, que respaldan su diseño, implementación y gestión.
- La ejecución activa de parches en el kernel (kpatch) para aplicarlos en los puntos vulnerables y las exposiciones comunes (CVE) graves e importantes sin reiniciar el sistema.

Obtenga la lista de verificación de "Las razones principales para adoptar Red Hat Enterprise Linux".

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

- Las herramientas que se basan en la tecnología extendida Berkeley Packet Filter (eBPF) para supervisar el rendimiento del sistema en pos de obtener información sobre él rápidamente.
- La compatibilidad con Flatpak para ejecutar las aplicaciones que suelen ser de escritorio.
- La función cgroup2 que ofrece funcionalidades mejoradas para regular la cantidad de recursos que utilizan los procesos.

También se ofrecen varias mejoras en cuanto a la automatización y la gestión, como la interfaz mejorada de la consola web, que simplifica las tareas de administración.

En el caso de la automatización, se incluyen:

- Nuevas funciones del sistema para Red Hat Enterprise Linux, con la tecnología de Red Hat Ansible® Automation Platform, para automatizar la gestión según sea necesario.
- Red Hat Insights, que forma parte de todas las suscripciones de Red Hat Enterprise Linux, para analizar el sistema de forma preventiva en busca de puntos vulnerables, omisiones de las funciones y otros criterios predefinidos.

Para los clientes cuyo principal objetivo es aprovechar al máximo el sistema de hardware, cabe destacar que Red Hat Enterprise Linux 9 ofrece un mayor rendimiento que las versiones 7 y 8. Estos son algunos de los cambios que lo hacen posible:

- Nuevos elevadores del disco para el kernel
- Nuevos perfiles de rendimiento adaptados

Consulte la Actualización de RHEL 6 a RHEL 8 para obtener información sobre el producto.

Explicación sobre Leapp y razones para usar la herramienta

No es tarea sencilla actualizar los servidores, pero Red Hat Enterprise Linux incluye Leapp, una herramienta compatible para gestionar el proceso, la cual proporciona una forma universal para adoptar la siguiente versión principal de RHEL. La herramienta permite que los clientes conserven la suscripción original (que se encuentra conectada al sistema), las configuraciones del sistema y los repositorios personalizados, como también las aplicaciones de terceros.

Dado que las versiones 7 y 8 de Red Hat Enterprise Linux incluyen Leapp, puede actualizar el sistema operativo de la versión 7.9 a la 8. Además, la herramienta también le servirá para pasar de la versión 8 a la 9 de RHEL.

En cambio, si utiliza Red Hat Enterprise Linux 6, deberá recurrir a otras herramientas para obtener la versión 7 de RHEL antes de actualizar el sistema a las versiones 8 o 9 con Leapp.

En la siguiente tabla le presentamos las ventajas de actualizar el servidor con Leapp.

Actualización integrada con Leapp	Reinstalación
Se mantiene la configuración.	Se debe crear una copia de seguridad de los datos de configuración y luego reiniciarlos.
Las máquinas conservan los datos de la suscripción actual.	Se debe adquirir la suscripción para las máquinas mediante subscription-manager.
Tiene un impacto positivo en la productividad gracias a la automatización.	Implica tiempo y costos adicionales.

Funcionamiento

Para que pueda actualizar el sistema con éxito, es esencial que conozca el funcionamiento de Leapp. La herramienta consta de un proceso de dos fases: el análisis de la capacidad de actualización y la actualización propiamente dicha. También se debe reiniciar el sistema luego de realizarla, por lo cual es importante que considere este paso al momento de la planificación.

Si un solo host utiliza Leapp, el análisis de la capacidad de actualización se basa en aspectos que debe tener en cuenta sobre ella y se descargan como metadatos desde *cloud.redhat.com*.

En caso de que los hosts estén conectados a Red Hat Satellite, este se encarga de distribuir los metadatos a los servidores que usan Leapp. Posteriormente se puede llevar a cabo el análisis según sea necesario con el plugin de Leapp para Red Hat Satellite.

El análisis de la capacidad de actualización genera un informe que posiblemente incluya temas que debe solucionar antes de llevar a cabo el proceso.

Leapp utiliza diversos programas Python como parte del flujo de trabajo, los cuales se denominan actores y pueden implementar cambios en el sistema.

Consulte "Using Red Hat Satellite to upgrade with Leapp".

Por ejemplo, **CheckOSRelease** es un actor que comprobará si la versión secundaria actual de Red Hat Enterprise Linux es compatible. En caso de que no lo sea, impedirá el proceso de actualización.

Si existe un aspecto sobre la actualización que debe considerar y que no se aborda mediante los actores con los que cuenta la herramienta, puede escribir uno propio y personalizarlo para que lo solucione, lo impida o le envíe información al respecto. Luego puede incorporarlo al flujo de trabajo de Leapp.

Leapp se integra con Red Hat Insights para analizar el conjunto de sistemas registrados, y así definir las máquinas que reúnen los requisitos par actualizarse.

Puede ejecutar la actualización con Leapp a través de la línea de comandos o Red Hat Satellite.

Limitaciones

Antes de comenzar a actualizar el servidor, debe conocer algunas limitaciones importantes que tendrá al usar Leapp:

- Solo se puede utilizar para actualizar de una versión principal de Red Hat Enterprise Linux a la siguiente.
- No funcionará si el sistema utiliza el cifrado del disco para el sistema de archivos de superusuario.
- Los dispositivos VDO deben convertirse para que los administre el gestor de volúmenes lógicos (LVM).
- Las rutas múltiples basadas en la red o los montajes del almacenamiento de red, como iSCSI o los sistemas de archivos de la red (NFS), no pueden utilizarse para la partición del sistema.
- Las instancias por solicitud en la nube pública que utilizan Red Hat Update Infrastructure (no es lo mismo que Red Hat Subscription Manager) no pueden actualizarse con Leapp.

Primeros pasos para comenzar la actualización

Veamos en qué consiste la actualización de la versión Red Hat Enterprise Linux 7 a la versión 8. El flujo de trabajo para pasar de la versión 8 a la 9 de RHEL sería parecido. Asegúrese de haber actualizado el sistema a Red Hat Enterprise Linux 7.9 con el comando **yum update:**

```
[root@leapp7to8 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.9 (Maipo)
```

Se debe instalar el paquete **leapp**. Asegúrese de que la máquina se encuentre suscrita a la red de distribución de contenidos (CDN) de Red Hat o al servidor de Satellite, con el canal Extras de RHEL 7 habilitado. Puede verificarlo mediante el comando:

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-7-server-extras-rpms
Repo Name: Red Hat Enterprise Linux 7 Server - Extras (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/7Server/$basearch/extras/os
Enabled:   1


Repo ID:   rhel-7-server-rpms
Repo Name: Red Hat Enterprise Linux 7 Server (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/$releasever/$basearch/os
Enabled:   1
```

Si el repositorio rhel-7-server-extras-rpms no se encuentra habilitado, puede activarlo con el código:

```
[root@leapp7to8 ~]# subscription-manager repos --enable
rhel-7-server-extras-rpm
```

Ya puede instalar Leapp en Red Hat Enterprise Linux 7 con el comando:

```
[root@leapp7to8 ~]# yum install -y leapp
```

Si actualiza desde la versión 8 a la 9 de Red Hat Enterprise Linux, consulte los siguientes pasos para instalar la herramienta Leapp de actualización integrada. Antes de adquirir la versión 9, probablemente tendrá que actualizar los servidores de RHEL 8. Consulte la página Supported in-place upgrade paths for Red Hat Enterprise Linux para obtener más información.

```
[root@leapp8to9 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.6 (Ootpa)
```

En el repositorio **rhel-8-for-x86_64-appstream-rpms** encontrará los paquetes **leapp** y **leapp-upgrade-el8toel9** que debe instalar con el comando:

```
[root@leapp8to9 ~]# yum install -y leapp leapp-upgrade-el8toel9
```

Si ya llevó a cabo una actualización integrada de RHEL 7 a RHEL 8, elimine el directorio **/root/tmp_leapp_py3** en caso de que forme parte de su sistema:

```
[root@leapp8to9 ~]# rm -rf /root/tmp_leapp_py3
```

Cuando haya instalado los paquetes de actualización integrada de Leapp para la versión de Red Hat Enterprise Linux, deberá analizar el servidor con **leapp preupgrade** antes de actualizar el sistema para identificar los posibles inconvenientes. El sistema no se modifica y crea archivos importantes que delinearán el proceso de actualización.

```
[root@leappXtoY ~]# leapp preupgrade
```

Luego de ejecutar el comando preupgrade, probablemente vea un resultado similar al siguiente:

```
…
 output omitted
…


============================================================
                    UPGRADE INHIBITED
============================================================
```

```
Upgrade has been inhibited due to the following problems:
    1. Inhibitor: Use of NFS detected. Upgrade can’t proceed
Consult the pre-upgrade report for details and possible remediation.

============================================================
                    UPGRADE INHIBITED
============================================================

Debug output written to /var/log/leapp/leapp-preupgrade.log

============================================================
                           REPORT
============================================================

A report has been generated at /var/log/leapp/leapp-report.json
A report has been generated at /var/log/leapp/leapp-report.txt

============================================================
                       END OF REPORT
============================================================

Answerfile has been generated at /var/log/leapp/answerfile
```

Archivos importantes:

/var/log/leapp/leapp-report.txt	Información legible y comprensible del informe de Leapp sobre la actualización
/var/log/leapp/leapp-report.json	Equivalente al formato JSON
/var/log/leapp/leapp-preupgrade.log	Resultado de depuración del comando leapp preupgrade
/var/log/leapp/answerfile	Respuesta a las preguntas del comando leapp preupgrade

El informe sobre el análisis de la capacidad de actualización se almacena en **/var/log/leapp/leapp-report.txt** y puede incluir aspectos importantes de los que debería encargarse antes de actualizar el sistema. Estos quizás precisen que usted proporcione información, la cual puede brindar si sigue las instrucciones que figuran en el informe.

Abordaje de los aspectos que deben tenerse en cuenta en el análisis de Leapp previo a la actualización

Es probable que tenga que encargarse de varios temas del informe que genera Leapp antes de la actualización en el archivo /var/log/leapp/leapp-report.txt. El ***inhibitor*** (inhibidor) es un obstáculo del que debe encargarse antes de continuar con la actualización, sino Leapp no podrá llevarla a cabo en el sistema.

El ***risk factor*** (factor de riesgo) indica el impacto que tienen los aspectos que debe considerar para la actualización según los siguientes niveles:

High (Alto)	Es muy probable que conduzca a un mal resultado.
Medium (Medio)	Podría afectar tanto al sistema como a las aplicaciones.
Low (Bajo)	No debería afectar al sistema, pero podría repercutir en las aplicaciones.
Info (Informativo)	Es meramente informativo, y no debería repercutir ni en el sistema ni en las aplicaciones.

El ***title*** (título) delimita los elementos en el informe de Leapp previo a la actualización y el summary brinda más información al respecto.

El ***summary*** (resumen) incluye una breve descripción del inconveniente detectado que debe abordarse.

La ***remediation*** (corrección) es una solución viable al problema informado. Estas son las más comunes:

- La edición de un archivo de configuración.
- La ejecución de un comando que cambie el comportamiento del sistema.
- La resolución mediante un archivo de respuesta de Leapp.
- La resolución que repercute en el software de modularidad de la biblioteca Software Collections de Red Hat Enterprise Linux 7, como Python, PHP, Node.js, PostgreSQL, etc.
- El desmontaje temporario de las exportaciones del NFS.

En esta sección se muestran ejemplos de aspectos sobre la actualización que debería abordar, y que poseen factor de riesgo alto y medio. Sus estructuras incluyen:

- El mensaje que aparece en el informe de Leapp, en el fragmento de ejemplo.
- El subsistema de software afectado.
- La explicación del problema informado.
- Las medidas que debería tomar.
- Las consecuencias de no abordar el problema informado.

Los sistemas pueden mostrar distintos aspectos para tener en cuenta según la versión de RHEL que actualice y su configuración.

Ejemplo 1: inhibidor de alto riesgo que implica cambios temporales en el sistema

En este ejemplo se presenta un problema inhibidor que se considera de alto riesgo en el informe de la evaluación previa. Si no se soluciona, la actualización de Leapp que se ejecute en el sistema presentará errores y el sistema quedará con la versión actual. Además de mostrar el mensaje, también analizaremos cómo resolver el problema en el sistema.

```
Risk Factor: high (inhibitor)
Title: Use of NFS detected. Upgrade can't proceed
Summary: NFS is currently not supported by the inplace upgrade.
We have found NFS usage at the following locations:
- One or more NFS entries in /etc/fstab
- Currently mounted NFS shares

Remediation: [hint] Disable NFS temporarily for the upgrade if possible.
Key: 9881b25faceeeaa7a6478bcdac29afd7f6baaaed
```

¿Qué ocurre si no me ocupo de este aviso?

Se trata de un inhibidor, por lo que impedirá que la actualización siga su curso hasta que tome las medidas correspondientes. El factor de riesgo es alto porque se espera que solo se efectúen cambios en el servidor local, pero no en los recursos compartidos del NFS.

¿En qué subsistema impacta?

Influye en los montajes del NFS.

¿Qué implica esto?

Los montajes del NFS no se pueden utilizar durante la actualización, por lo que se los debe desmontar y deshabilitar hasta que el proceso haya finalizado.

¿Cómo debo proceder?

Edite /etc/fstab para que los recursos compartidos del NFS aparezcan como comentarios de forma temporal y desmonte los que actualmente se encuentran montados. Detenga y deshabilite autofs.service de forma temporal. Las entradas del NFS y autofs.service pueden habilitarse nuevamente cuando la actualización haya finalizado.

```
[root@leapp8to9 ~]# systemctl disable –now autofs.service
```

Ejemplo 2: inhibidor de alto riesgo que requiere cambios en un archivo de configuración actual

Aplica en gran medida a la actualización de Red Hat Enterprise Linux 7 a la versión 8.

```
Risk Factor: high (inhibitor)

Title: Possible problems with remote login using root account

Summary: OpenSSH configuration file does not explicitly state the
option PermitRootLogin in sshd_config file, which will default in
Red Hat Enterprise Linux8 to “prohibit-password”.

Remediation: [hint] If you depend on remote root logins using
passwords, consider setting up a different user for remote
administration or adding “PermitRootLogin yes” to sshd_config.

Key: 3d21e8cc9e1c09dc60429de7716165787e99515f
```

¿Qué ocurre si no me ocupo de este aviso?

Se trata de un inhibidor, por lo que impedirá que la actualización siga su curso. También cabo señalar que al ser un factor de riesgo alto, no podrá iniciar sesión en su servidor con Secure Shell (SSH) de forma remota si no lo aborda correctamente.

¿En qué subsistema impacta?

Afecta al servidor de SSH (sshd.service).

¿Qué implica esto?

El fragmento de código indica que el funcionamiento del servidor de SSH cambia drásticamente entre las versiones 7 y 8 de Red Hat Enterprise Linux. De forma predeterminada, está deshabilitada la autenticación del superusuario mediante contraseña en RHEL 8. En Red Hat Enterprise Linux 7, el valor predeterminado implícito para PermitRootLogin es yes, pero en RHEL 8 es prohibit-password.

Dentro de /etc/ssh/sshd_config aparece una directiva de configuración implícita en forma de comentario, pero en realidad no lo es. Está allí para comunicarle los valores predeterminados de la directiva.

¿Cómo debo proceder?

Asegúrese de poder iniciar sesión como otro usuario, indistintamente de si utiliza o no una contraseña.

Debe establecer de forma explícita un valor para PermitRootLogin dentro de /etc/ssh/sshd_config. Puede ser "yes" para permitir que el superusuario inicie sesión a través de SSH o "no" para evitar que lo haga. Lo importante es que lo establezca de forma expresa.

Las páginas de manual de Linux son una fuente de información adicional extraordinaria. Utilice el comando **man sshd_config** y busque la cadena *PermitRootLogin* para obtener más información sobre la directiva de configuración.

Ejemplo 3: inhibidor de alto riesgo que requiere el uso del archivo de respuesta de Leapp

Este problema en particular aplica en gran medida a la actualización de Red Hat Enterprise Linux 7 a la versión 8. La característica particular de este ejemplo es que se debe corregir el problema con el archivo de respuesta de Leapp, en el cual los datos se pueden trasladar de forma automática a la herramienta.

```
Risk Factor: high (inhibitor)

Title: Missing required answers in the answer file

Summary: One or more sections in answerfile are missing user choices:
remove_pam_pkcs11_module_check.confirm

For more information consult https://leapp.readthedocs.io/en/latest/
dialogs.html

Remediation: [hint] Please register user choices with leapp answer cli
command or by manually editing the answerfile.

[command] leapp answer --section remove_pam_pkcs11_module_check.
confirm=True

Key: d35f6c6b1b1fa6924ef442e3670d90fa92f0d54b
```

¿Qué ocurre si no me ocupo de este aviso?

Se trata de un inhibidor, por lo que impedirá que la actualización siga su curso hasta que autorice la eliminación del módulo pam_pkcs11. El factor de riesgo es alto porque es probable que los valores del control *requisite o required* estén asociados con el módulo pam_pkcs11 en la configuración de PAM, y si elimina este módulo en Red Hat Enterprise Linux 8 el sistema podría bloquearlo.

Este punto sobre la actualización **solo** podría solucionarse con el uso del archivo de respuesta de Leapp.

¿En qué subsistema impacta?

Influye en la autenticación (pam).

¿Qué implica esto?

El fragmento de código indica que el módulo pam_pkcs11 se elimina de Red Hat Enterprise Linux 8 y ahora esta función la provee sssd.

¿Cómo debo proceder?

Edite /var/log/leapp/answerfile de la siguiente manera:

```
[remove_pam_pkcs11_module_check]

confirm = True
```

O ejecute el siguiente comando para editar el archivo de respuesta /var/log/leapp/answerfile:

```
leapp answer --section
remove_pam_pkcs11_module_check.confirm=true
```

También debe comprobar que pueda utilizar otros métodos para autenticarse que no dependan del módulo pam_pkcs11.

Puede hacerlo al ejecutar **grep pam_pkcs11 /etc/pam.d/***.

Acceda al laboratorio práctico managing software from an application stream

Ejemplo 4: aspecto no inhibidor de alto riesgo que afecta a los programas Python después de la actualización

Este ejemplo aplica en gran medida a las máquinas que se actualizan de Red Hat Enterprise Linux 7 a la versión 8. A diferencia de los anteriores, no se trata de un inhibidor, por lo cual la herramienta Leapp llevará a cabo la actualización incluso si el problema identificado no se soluciona. El administrador del sistema definirá si es necesario resolver el inconveniente. También determinará si la máquina utiliza aplicaciones basadas en Python 2 y si son compatibles con Python 3, la versión que ofrece el sistema operativo actualizado.

```
Risk Factor: high

Title: Difference in Python versions and support in Red Hat Enterprise
Linux 8

Summary: In Red Hat Enterprise Linux 8, there is no ‘python’
command. Python 3 (backward incompatible) is the primary Python
version and Python 2 is available with limited support and
limited set of packages. Read more here: https://access.redhat.
com/documentation/en-us/red_hat_enterprise_linux/8/html-single/
configuring_basic_system_settings/#using-python3

Remediation: [hint] Please run “alternatives --set python /usr/bin/
python3” after upgrade

Key: 0c98585b1d8d252eb540bf61560094f3495351f5
```

¿Qué ocurre si no me ocupo de este aviso?

Como no se trata de un inhibidor, el comando de actualización de Leapp podrá seguir su curso a pesar de que no solucione el inconveniente. El factor de riesgo es alto porque el comando (/usr/bin/python) de Python sin versión no está disponible en Red Hat Enterprise Linux 8 de forma predeterminada. No será posible ejecutar el intérprete de Python de forma directa (por ejemplo, desde una terminal) ni de forma indirecta (en la cual otro proceso ejecuta el comando por usted).

¿En qué subsistema impacta?

Influye en Python y en las aplicaciones que dependen del comando /usr/bin/python sin versión.

¿Qué implica esto?

Si bien se descontinúa el uso de Python 2 en favor de Python 3, todavía puede instalarlo mediante los flujos de aplicaciones. El repositorio de los flujos ofrece varios módulos de Python que puede instalar en simultáneo con el servidor. Siempre debe indicar la versión del programa, indistintamente de si lo implementa, lo invoca o interactúa con él. El comando Python sin versión no está disponible de forma predeterminada, pero si quisiera podría configurarlo.

¿Cómo debo proceder?

Puede ejecutar el siguiente comando para asegurarse de que /usr/bin/python3 se utilice como la versión predeterminada de Python:

```
alternatives --set python /usr/bin/python3
```

En las aplicaciones que requieran Python 2 específicamente, debe indicarse /usr/bin/python2. También puede utilizar el siguiente comando para establecer esa versión como predeterminada:

```
alternatives --set python /usr/bin/python2
```

Ejemplo 5: aspecto no inhibidor de riesgo medio

Este ejemplo aplica en gran medida a la actualización de Red Hat Enterprise Linux 7 a la versión 8.

```
Risk Factor: medium

Title: chrony using default configuration

Summary: default chrony configuration in Red Hat Enterprise Linux8
uses leapsectz directive, which cannot be used with leap smearing
NTP servers, and uses a single pool directive instead of four server
directives

Key: c4222ebd18730a76f6bc7b3b66df898b106e6554
```

¿Qué ocurre si no me ocupo de este aviso?

Como no se trata de un inhibidor, la actualización de Leapp podrá seguir su curso. El factor de riesgo es medio porque los clientes del protocolo Network Time Protocol (NTP) que estén configurados para obtener la hora de varios servidores recibirán distintos horarios al momento de la adición del tiempo si no implementan la técnica de extensión del tiempo (leap smear) o si dichas técnicas son distintas. Esto puede generar que dejen de actualizar los relojes o que cambien entre los servidores de forma aleatoria.

¿En qué subsistema impacta?

Influye en la sincronización del tiempo mediante chrony.

¿Qué implica esto?

Chrony implementa la sincronización del tiempo con NTP. En Red Hat Enterprise Linux 8, la directiva de grupo se utiliza de forma predeterminada para referirse a un conjunto de servidores NTP que tienen las mismas funciones. El uso de múltiples directivas de servidor que se refieren a los servidores NTP con diferentes funciones podría generar que se corrompa la sincronización del tiempo.

¿Cómo debo proceder?

En /etc/chrony.conf, elimine las directivas *leapsectz* y *leapfile* y utilice allí la directiva de grupo en lugar de la de servidor. Esto garantizará que se utilicen los servidores NTP con las mismas funciones.

Si desea sincronizar el horario del sistema con servidores definidos de forma expresa, asegúrese de que estos tengan las mismas funciones.

Obtenga la lista de verificación de "Las razones principales para adoptar Red Hat Enterprise Linux".

Ya estoy en condiciones de actualizar el sistema

Luego de que haya abordado los inconvenientes que se detectaron en el informe previo a la actualización, es recomendable que ejecute el comando **leapp preupgrade** nuevamente. Luego vuelva a consultar el archivo del informe para asegurarse de no haber omitido nada que le impida realizar la actualización con éxito.

Cuando el sistema esté preparado para actualizarse, ejecute el comando **leapp upgrade** o **leapp upgrade --reboot**.

El comando **leapp upgrade** ingresa el proceso de actualización en cola, y para finalizarlo tendrá que reiniciar el sistema repetidas veces. Es importante que considere esto en sus planes. Luego del primer inicio, puede seguir utilizando la versión actual de Red Hat Enterprise Linux.

El comando **leapp upgrade reboot** reinicia el servidor de forma automática.

Primer inicio: el cargador de arranque inicia de forma automática un entorno de actualización especial, dentro del cual se actualizará el servidor, con la entrada del menú **Red Hat Enterprise Linux-Upgrade-Initramfs**. Debe hacer una copia de seguridad en caso de que quiera restaurar la actualización y seguir utilizando la versión principal anterior de Red Hat Enterprise Linux.

Segundo inicio: las etiquetas de SELinux se restablecerán y el servidor se reiniciará una vez más.

Tercer inicio: puede corroborar la actualización y disfrutar la experiencia nueva con Red Hat Enterprise Linux.

Valide la versión de Red Hat Enterprise Linux que utiliza en la actualidad:

```
[root@leapp7to8 ~]# rpm -q redhat-release
redhat-release-8.6-0.1.el8.x86_64
```

```
[root@leapp8to9 ~]# rpm -q redhat-release
redhat-release-9.0-2.17.el9.x86_64
```

Si actualiza Red Hat Enterprise Linux de la versión 7 a la 8, seguramente espera ver un repositorio denominado *rhel-8-server-rpms*, pero en realidad RHEL 8 cuenta con dos repositorios: *rhel-8-for-x86_64-baseos-rpms* que ofrece el conjunto principal de funciones subyacentes del SO y *rhel-8-for-x86_64-appstream-rpms* que incluye aplicaciones del espacio de usuario, lenguajes del tiempo de ejecución y bases de datos adicionales que respaldan múltiples cargas de trabajo y casos prácticos. Puede comprobarlo de la siguiente manera:

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-8-for-x86_64-appstream-rpms
```

Consulte what is BOOM and how to install it?

Para obtener más información sobre la gestión de las actualizaciones del sistema con instantáneas

```
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/x86_64/
appstream/os
Enabled:   1


Repo ID:   rhel-8-for-x86_64-baseos-rpms
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/x86_64/
baseos/os
Enabled:   1
```

Luego de que se haya actualizado y reiniciado el sistema, debe revisar **/var/log/leapp/leapp-report.txt** , que ahora posee el informe posterior a la actualización, el cual podría contener puntos adicionales de los que debería encargarse.

Recomendaciones

Antes de que comience el proceso, posiblemente quiera analizar las siguientes recomendaciones.

sosreport

Tenga presente que puede generar un informe sosreport para que le brindemos soporte si lo necesita.

1. Utilice **yum install sos** para asegurarse de que el paquete sos esté instalado.
2. Genere el informe con el comando **sosreport**.
3. Copie el archivo tar que genero de **/var/tmp/** a una ubicación segura si necesita el soporte de Red Hat Support.

Asegúrese de tener una copia de seguridad

En caso de que se produzca algún imprevisto que no le permita operar el sistema ni acceder a los datos, es fundamental que pueda recuperarse de forma oportuna y continuar las operaciones. Las copias de seguridad de los datos facilitan el proceso de recuperación, por lo cual ya debería tenerlas listas. Pero cabe destacar que debe realizarlas antes de utilizar Leapp para actualizar los servidores.

Utilice las herramientas que ya posee para implementar una estrategia de copia de seguridad.

- Defina los datos que son importantes para que el servidor funcione.
- Haga una copia de seguridad de los datos en una ubicación segura fuera del servidor que está actualizando.
- Pruébela para asegurarse de que los datos se hayan copiado de forma correcta.
- Compruebe que puede restablecer los datos de la copia de seguridad.
- Valide el plan de recuperación ante desastres para asegurarse de estar completamente listo para afrontar una posible pérdida del servidor.

Use Red Hat Insights

Red Hat Insights sirve para determinar si cumple con los requisitos para la actualización.

Aproveche Red Hat Satellite Server

Red Hat Satellite Server puede sacar provecho del plugin de Leapp para analizar y actualizar los sistemas que reúnan los requisitos según sea necesario.

Utilice la consola web

Tenga en cuenta que el uso de la consola web simplificará el proceso de actualización, dado que presenta el informe previo en un formato legible.

Debe asegurarse de que los paquetes cockpit y cockpit-leapp estén instalados con **yum install cockpit cockpit-leapp**.

Luego recurra a **systemctl enable --now cockpit.socket** para activar el socket cockpit.

Agregue el puerto de la consola web al firewall mediante **firewall-cmd --add-port 9090/tcp** y luego compruebe que la regla se haya incorporado de forma permanente a su configuración con **firewall-cmd --add-port 9090/tcp --permanent**.

Ahora inicie sesión en la consola web en *https://your_server_name:9090*

Requisitos del repositorio de Satellite

Si utiliza Satellite Server para gestionar los paquetes, compruebe que los siguientes repositorios estén disponibles:

- rhel-7-server-rpms
- rhel-7-server-extras-rpms
- rhel-8-for-x86_64-baseos-rpms
- rhel-8-for-x86_64-appstream-rpms

yum versionlock

Si utilizó el comando yum versionlock para fijar paquetes a una versión en particular, elimínelos mediante **yum versionlock clear**.

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800

es.redhat.com
#F31715_0822