Red Hat Enterprise Linux 8

Atualização de RHEL 7 para RHEL 8

Instruções para uma atualização no local de Red Hat Enterprise Linux 7 para Red Hat Enterprise Linux 8

Last Updated: 2021-02-26

Red Hat Enterprise Linux 8 Atualização de RHEL 7 para RHEL 8

Instruções para uma atualização no local de Red Hat Enterprise Linux 7 para 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.

Nota Legal

Resumo

Este documento fornece instruções sobre como realizar uma atualização no local de Red Hat Enterprise Linux 7 para Red Hat Enterprise Linux 8 usando o utilitário Saltar. Durante o upgrade no local, o sistema operacional RHEL 7 existente é substituído por uma versão RHEL 8.

Índice

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO

A Red Hat tem o compromisso de substituir a linguagem problemática em nosso código, documentação e propriedades da web. Estamos começando com estes quatro termos: master, slave, blacklist e whitelist. Por causa da enormidade deste esforço, estas mudanças serão implementadas gradualmente ao longo de vários lançamentos futuros. Para mais detalhes, veja a mensagem de nosso CTO Chris Wright.

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT

Agradecemos sua contribuição em nossa documentação. Por favor, diga-nos como podemos melhorá-la. Para fazer isso:

- Para comentários simples sobre passagens específicas:
  1. Certifique-se de que você está visualizando a documentação no formato *Multi-page HTML*. Além disso, certifique-se de ver o botão **Feedback** no canto superior direito do documento.
  2. Use o cursor do mouse para destacar a parte do texto que você deseja comentar.
  3. Clique no pop-up **Add Feedback** que aparece abaixo do texto destacado.
  4. Siga as instruções apresentadas.
- Para enviar comentários mais complexos, crie um bilhete Bugzilla:
  1. Ir para o site da Bugzilla.
  2. Como Componente, use **Documentation**.
  3. Preencha o campo **Description** com sua sugestão de melhoria. Inclua um link para a(s) parte(s) relevante(s) da documentação.
  4. Clique em **Submit Bug**.

CAPÍTULO 1. PLANEJANDO UMA ATUALIZAÇÃO

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

Você deve considerar o seguinte antes de atualizar para a RHEL 8:

- **Operating system** - O sistema operacional é atualizado pela concessionária **Leapp** sob as seguintes condições:
  - A variante Servidor instalada do **latest available RHEL 7 version**, que atualmente é:
    - **RHEL 7.9** sobre as arquiteturas 64-bit Intel, IBM POWER 8 (little endian), e IBM Z
    - **RHEL 7.6** sobre arquiteturas que **require kernel version 4.14**: 64-bit ARM, IBM POWER 9 (little endian), ou IBM Z (Estrutura A)
      Veja Caminhos de atualização suportados no local para o Red Hat Enterprise Linux para mais informações.
  - Os requisitos mínimos de hardware para RHEL 8 foram cumpridos
  - Acesso ao conteúdo atualizado RHEL 7.9 e RHEL 8.2 fornecido; veja Preparando um sistema RHEL 7 para a atualização, passo 1 para detalhes.
- **Applications** - Você pode migrar as aplicações instaladas em seu sistema usando **Leapp**. No entanto, em certos casos, é necessário criar atores personalizados, que especificam ações a serem realizadas por **Leapp** durante a atualização, por exemplo, reconfigurando uma aplicação ou instalando um driver de hardware específico. Para mais informações, consulte Manuseio da migração de suas aplicações personalizadas e de terceiros. Observe que os atores personalizados não são suportados pela Red Hat.
- **Security** - Você deve avaliar este aspecto antes da atualização e tomar medidas adicionais quando o processo de atualização estiver concluído. Considere especialmente o seguinte:
  - Antes da atualização, defina o padrão de segurança que seu sistema precisa para cumprir e compreender as mudanças de segurança no RHEL 8 .
  - Durante o processo de atualização, o utilitário **Leapp** define o modo SELinux como permissivo.
  - As atualizações no local dos sistemas no modo FIPS não são suportadas.
  - Após a atualização estar concluída, reavalie e reaplique suas políticas de segurança. Para informações sobre a aplicação de políticas de segurança que foram desativadas durante a atualização ou recentemente introduzidas no RHEL 8, consulte Aplicando políticas de segurança.
- **Storage and file systems**- Você deve sempre fazer backup de seu sistema antes da atualização. Por exemplo, você pode usar o utilitário Relax-and-Recover (ReaR), snapshots de LVM, divisão RAID ou um instantâneo de máquina virtual.
- **Downtime** - O processo de atualização pode levar de vários minutos a várias horas.
- **Satellite** - Se você administra seus hosts através do Satellite, você pode atualizar vários hosts simultaneamente do RHEL 7 para o RHEL 8 usando o Satellite web UI. Para mais informações, consulte Atualização de hosts da RHEL 7 para a RHEL 8 .

- **Public Clouds** - A atualização no local é suportada para instâncias sob demanda em Amazon Web Services (AWS) e Microsoft Azure, usando a Infra-estrutura de Atualização da Red Hat (RHUI).

- **Known limitations** - Notáveis limitações conhecidas do **Leapp** atualmente incluem:

  - A criptografia de todo o disco ou de uma partição, ou a criptografia do sistema de arquivos atualmente não pode ser usada em um sistema destinado a uma atualização no local.

  - Nenhum caminho múltiplo baseado em rede e nenhum tipo de montagem de armazenamento em rede pode ser usado como partição do sistema (por exemplo, iSCSI, ou NFS).

  - A atualização no local não é atualmente suportada para instâncias sob demanda nas nuvens públicas remanescentes (Huawei Cloud, Alibaba Cloud, Google Cloud) que utilizam a infraestrutura de atualização da Red Hat mas não o Gerente de Assinaturas da Red Hat para uma assinatura RHEL.

Veja também Questões Conhecidas.

Você pode usar **Red Hat Insights** para determinar qual dos sistemas que você registrou no Insights está em um caminho de atualização suportado para o RHEL 8. Para isso, navegue até a recomendação do respectivo Conselheiro no Insights, habilite a recomendação no menu suspenso *Actions*, e inspecione a lista sob o título *Affected systems*. Observe que a recomendação do Assessor considera apenas a versão menor da RHEL 7 e não realiza uma avaliação de pré-atualização do sistema.

CAPÍTULO 2. PREPARANDO UM SISTEMA RHEL 7 PARA A ATUALIZAÇÃO

Este procedimento descreve as etapas necessárias antes de realizar uma atualização no local para o RHEL 8 usando o utilitário **Leapp**.

Se você não planeja usar o Red Hat Subscription Manager durante o processo de atualização, siga as instruções em Upgrade to RHEL 8 sem o Red Hat Subscription Manager .

Pré-requisitos

- O sistema atende às condições listadas em Planejamento de uma atualização.

Procedimento

1. Certifique-se de que seu sistema foi registrado com sucesso na Red Hat Content Delivery Network (CDN) ou no Red Hat Satellite 6.5 ou posterior usando o Gerente de Assinaturas da Red Hat.

IMPORTANTE

Se seu sistema estiver registrado no Satellite Server, certifique-se de que o Satellite atenda às seguintes condições:

a. A Satellite tem um manifesto de assinatura com os repositórios RHEL 8 importados. Para mais informações, veja o capítulo *Managing Subscriptions* no *Content Management Guide* para a versão particular do Red Hat Satellite, por exemplo, para a versão 6.8.

b. Os seguintes repositórios são habilitados e sincronizados com as últimas atualizações, e publicados no Satellite:

- Red Hat Enterprise Linux 7 Server RPMs x86_64 **7** ou Red Hat Enterprise Linux 7 Server RPMs x86_64 **7.9**
- Servidor Red Hat Enterprise Linux 7 - 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 mais informações, veja o capítulo *Importing Red Hat Content* no *Content Management Guide* para a versão particular do Red Hat Satellite, por exemplo, para a versão 6.8.

c. O hospedeiro de conteúdo pertence a um dos seguintes:

- Uma Vista de Conteúdo contendo os repositórios RHEL 7 e RHEL 8 acima.
- A Visão de Conteúdo Padrão da Organização e o ambiente do ciclo de vida da Biblioteca.
  Para mais informações, veja o capítulo *Managing Content Views* no *Content Management Guide* para a versão particular do Red Hat Satellite, por exemplo, para a versão 6.8.

2. Verifique se você tem a assinatura do Red Hat Enterprise Linux Server anexada:

```
# 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
```

   Você deve ver *Server* no nome do produto e *Subscribed* como o status.

3. Assegure-se de ter os repositórios apropriados habilitados. Os seguintes comandos listam os repositórios para a arquitetura Intel de 64 bits; para outras arquiteturas, veja os repositórios RHEL 7.

   a. Habilitar o repositório Base:

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

   b. Habilitar o repositório Extras onde **Leapp** e suas dependências estão disponíveis:

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

NOTA

Você também pode ter os repositórios Opcionais ou Suplementares habilitados; veja a lista deles nos repositórios RHEL 7. Em tal caso, **Leapp** habilita o Construtor Linux CodeReady da RHEL 8 ou os repositórios Suplementares da RHEL 8, respectivamente.

4. Defina o Red Hat Subscription Manager para consumir o mais recente conteúdo RHEL 7:

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

5. Opcional: Se você quiser usar repositórios personalizados, configure-os de acordo com as instruções em Configuração de repositórios personalizados.

6. Se você usar o plug-in **yum-plugin-versionlock** para bloquear pacotes para uma versão específica, limpe a trava executando:

```
# yum versionlock clear
```

   Veja Como restringir o yum para instalar ou atualizar um pacote para uma versão de pacote específico fixo? para mais informações.

7. Certifique-se de ter o sistema locale configurado para **en_US.UTF-8**:

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

   Se o locale for diferente, siga as instruções em Como mudar o locale do sistema no RHEL7?

8. Se você estiver atualizando usando a Red Hat Update Infrastructure (RHUI) em uma nuvem pública, complete as seguintes tarefas para garantir que seu sistema esteja pronto para a atualização.

   a. Para AWS, habilite o repositório do Red Hat Update Infrastructure 3 Client Configuration Server 7 e instale os pacotes RHUI necessários.

      i. Para arquiteturas não-ARM:

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

      ii. Para a arquitetura ARM:

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

   b. Para o Microsoft Azure, habilite os RPMs do Microsoft Azure para o repositório Red Hat Enterprise Linux 7 e instale os pacotes RHUI necessários.

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

   NOTA

   Se você trancou a máquina virtual Azure (VM) para um lançamento menor, remova o bloqueio da versão. Para mais informações, consulte Mudar uma RHEL 7.x VM de volta para não-EUA.

9. Se você administra containers no Docker, recrie esses containers com as imagens apropriadas usando Podman e depois anexe qualquer volume em uso. Para mais informações, veja Como faço para migrar meus containers do Docker para o Podman antes de mudar do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8?

10. Atualizar todos os pacotes para a última versão do RHEL 7:

    ```
    # yum update
    ```

11. Reinicie o sistema:

    ```
    # reboot
    ```

12. Instale o utilitário **Leapp**:

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

    Observe que atualmente você precisa da versão 0.11.1 ou posterior do pacote **leapp** e da versão 0.12.0 ou posterior do pacote **leapp-repository**.

13. Baixar arquivos de dados adicionais necessários (mudanças no pacote RPM e mapeamento do repositório RPM) anexados ao artigo Knowledgebase Dados requeridos pelo utilitário Leapp para uma atualização no local de RHEL 7 para RHEL 8 e colocá-los no diretório

/etc/leapp/files/. Isto é necessário para um upgrade bem sucedido. Observe que atualmente são necessários arquivos de dados do arquivo **leapp-data12.tar.gz** ou posterior.

NOTA

Se você estiver atualizando em uma nuvem pública usando a RHUI e não tiver uma assinatura Red Hat ou conta no Portal do Cliente Red Hat, crie uma assinatura de desenvolvedor RHEL sem custos para que você possa acessar o artigo da Base de Conhecimento e fazer o download dos pacotes de dados necessários. Para mais informações, veja Como posso obter uma assinatura de desenvolvedor Red Hat Enterprise Linux sem custos ou renová-la?

14. Certifique-se de ter qualquer gerenciamento de configuração (como **Salt**, **Chef**, **Puppet**, **Ansible**) desativado ou adequadamente reconfigurado para não tentar restaurar o sistema RHEL 7 original.

15. Certifique-se de que seu sistema não utilize mais de uma placa de interface de rede (NIC) com um nome baseado no prefixo utilizado pelo kernel (**eth**). Para instruções sobre como migrar para outro esquema de nomes antes de uma atualização no local para o RHEL 8, veja Como realizar uma atualização no local para o RHEL 8 ao usar nomes NIC do kernel no RHEL 7.

16. Certifique-se de ter um backup completo do sistema ou uma foto da máquina virtual. Você deve ser capaz de levar seu sistema ao estado de pré-atualização se seguir os procedimentos padrão de recuperação de desastres dentro de seu ambiente. Por exemplo, você pode usar o utilitário Relax-and-Recover (ReaR). Para mais informações, veja a documentação do ReaR e o que é Relax-and-Recover (ReaR) e como posso utilizá-lo para a recuperação de desastres? Alternativamente, você pode usar snapshots LVM, ou divisão RAID. Em caso de atualização de uma máquina virtual, você pode criar um instantâneo de toda a VM.

CAPÍTULO 3. REVISÃO DO RELATÓRIO DE PRÉ-ATUALIZAÇÃO

Para avaliar a possibilidade de atualização de seu sistema, inicie o processo de pré-atualização através do comando **leapp preupgrade**. Durante esta fase, o utilitário **Leapp** coleta dados sobre o sistema, avalia a possibilidade de atualização e gera um relatório de pré-atualização.

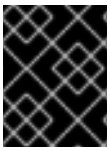
O relatório de pré-atualização está disponível tanto no arquivo **/var/log/leapp/leapp-report.txt** quanto no console web. O relatório resume os problemas potenciais e propõe soluções recomendadas. O relatório também o ajuda a decidir se é possível ou aconselhável proceder com a atualização.

Em certas configurações, **Leapp** gera perguntas verdadeiro/falso para determinar como proceder. Todas as perguntas são armazenadas em **/var/log/leapp/answerfile** e no relatório de pré-atualização na mensagem **Missing required answers in the answer file**. **Leapp** inibe a atualização se você não fornecer respostas a todas as perguntas.

Você tem duas opções ao avaliar a possibilidade de atualização na fase de pré-atualização:

a. Reveja o relatório de pré-atualização no arquivo **leapp-report.txt** gerado e resolva manualmente os problemas relatados usando a interface de linha de comando.

b. Use o console web para revisar o relatório, aplicar remediações automáticas quando disponíveis e corrigir os problemas restantes usando as dicas de remediação sugeridas.



IMPORTANTE

Durante a fase de pré-atualização, **Leapp** não simula todo o processo de atualização no local nem baixa todos os pacotes de RPM.

A revisão de um relatório de pré-atualização é útil também se você decidir ou precisar reimplantar um sistema RHEL 8 sem o processo de atualização no local.

3.1. AVALIANDO A POSSIBILIDADE DE ATUALIZAÇÃO A PARTIR DA LINHA DE COMANDO

Identificar problemas potenciais de atualização durante a fase de pré-atualização usando a interface de linha de comando.

Pré-requisitos

- As etapas listadas em Preparação de um sistema RHEL 7 para a atualização foram concluídas.

Procedimento

1. Em seu sistema RHEL 7, realize a fase de pré-atualização:

```
# leapp preupgrade
```

NOTA

Se você vai usar repositórios personalizados do diretório **/etc/yum.repos.d/** para a atualização, habilite os repositórios selecionados da seguinte forma:

```
# salto de pré-atualização --enablerepo repository_id1 --enablerepo
repository_id2...
```

Se você for atualizar sem a RHSM ou usando a RHUI, adicione a opção **--no-rhsm**.

2. Fornecer respostas a cada pergunta exigida por **Leapp** através de um dos seguintes métodos:

   a. Execute o comando **leapp answer**, especificando a pergunta a que você está respondendo e sua resposta confirmada.

   ```
   #resposta saltitante --secção question_section.confirm=answer
   ```

   Por exemplo, para confirmar uma resposta a **True** à pergunta **Disable pam_pkcs11 module in PAM configuration?**, execute o seguinte comando:

   ```
   # resposta pulo --section remove_pam_krb5_module_check.confirm=True
   ```

   b. Edite manualmente o arquivo **/var/log/leapp/answerfile**, descomente a linha **confirm** do arquivo deletando o símbolo **#**, e confirme sua resposta como **True** ou **False**; veja o arquivo de respostas do Leapp.

1. Examinar o relatório no arquivo **/var/log/leapp/leapp-report.txt**, e resolver manualmente todos os problemas relatados antes de proceder com a atualização no local.

3.2. AVALIANDO A POSSIBILIDADE DE ATUALIZAÇÃO E APLICANDO REMEDIAÇÕES AUTOMATIZADAS ATRAVÉS DO CONSOLE WEB

Identificar problemas potenciais na fase de pré-atualização e como aplicar remediações automatizadas usando o console web.

Pré-requisitos

- As etapas listadas em Preparação de um sistema RHEL 7 para a atualização foram concluídas.

Procedimento

1. Instale o plug-in **cockpit-leapp**:

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

2. Navegue até o console web em seu navegador e faça o login como **root** ou como um usuário configurado no arquivo **/etc/sudoers**. Veja Sistemas de gerenciamento usando o console web RHEL 7 para mais informações sobre o console web.

3. Em seu sistema RHEL 7, realize a fase de pré-atualização a partir da interface da linha de comando ou a partir do terminal do console web:

```
# leapp preupgrade
```

NOTA

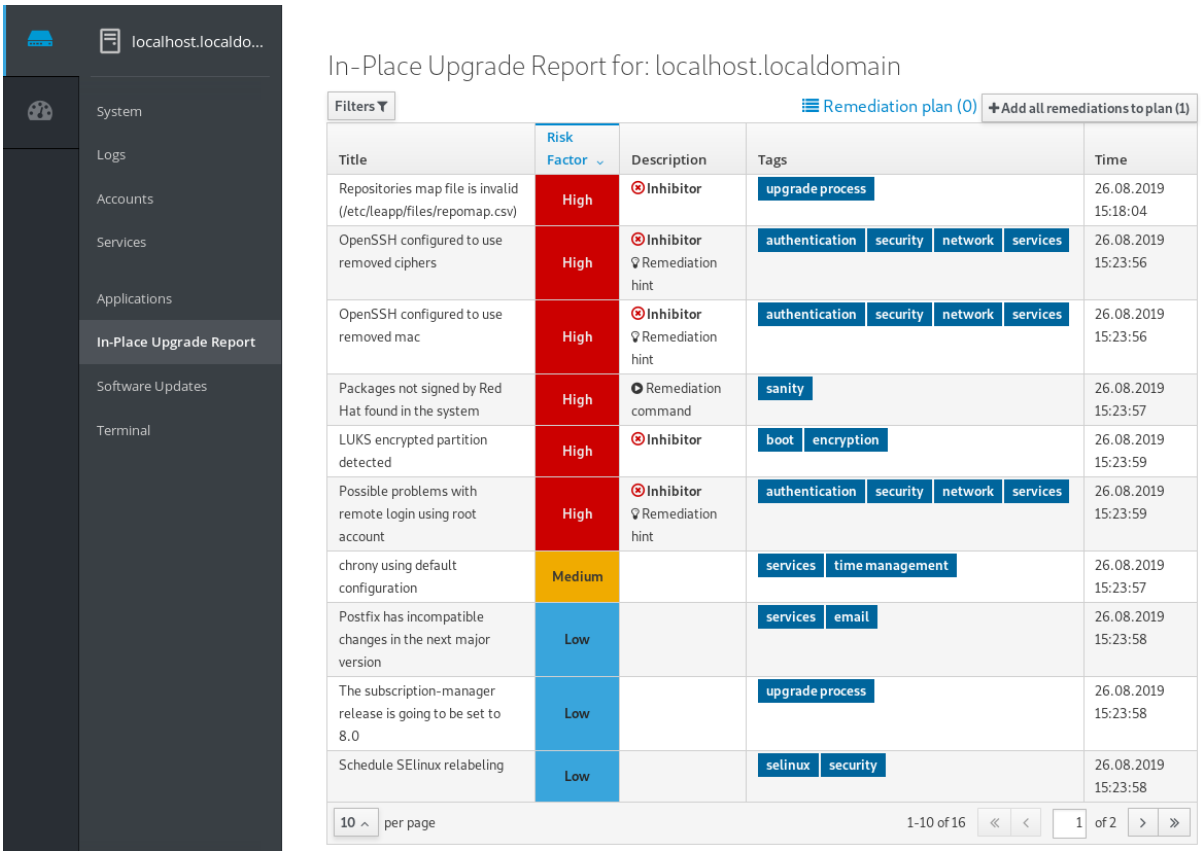
Se você vai usar repositórios personalizados do diretório **/etc/yum.repos.d/** para a atualização, habilite os repositórios selecionados da seguinte forma:

```
# salto de pré-atualização --enablerepo repository_id1 --enablerepo repository_id2...
```

Se você for atualizar sem a RHSM ou usando a RHUI, adicione a opção **--no-rhsm**.

4. No console web, selecione **In-place Upgrade Report** no menu à esquerda.

Figura 3.1. Relatório de atualização in loco no console web



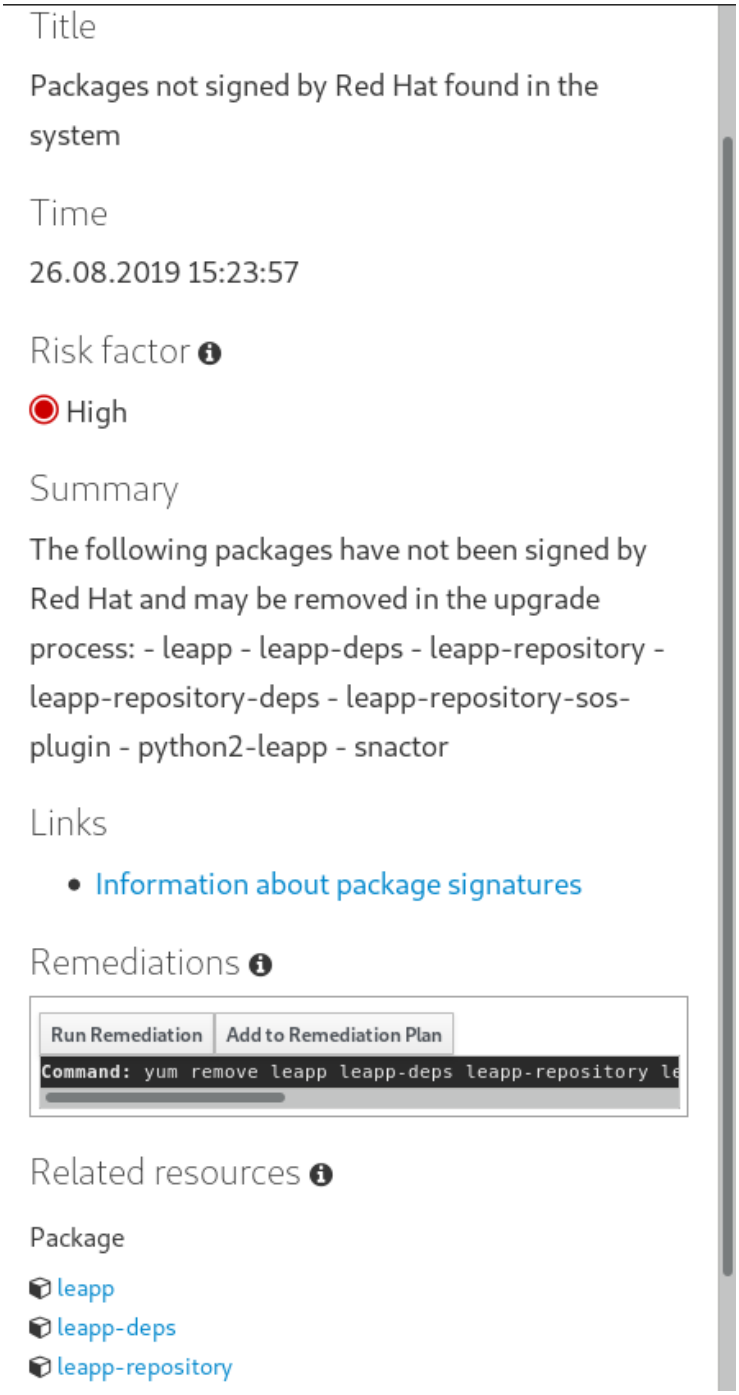
A tabela do relatório fornece uma visão geral dos problemas encontrados, sua avaliação de risco e remediações (se disponíveis).

- Fator de risco:
  - Alto - muito provável que resulte em um estado de sistema deteriorado
  - Médio - pode impactar tanto o sistema quanto as aplicações
  - Baixo - não deve ter impacto no sistema, mas pode ter um impacto nas aplicações
- Inibidor - inibirá (parada dura) o processo de atualização, caso contrário o sistema pode se tornar inabalável, inacessível, ou disfuncional

- Remediação - uma solução acionável para um problema relatado:
  - Comando de remediação - pode ser executado diretamente através do console web
  - Dica de remediação - instruções sobre como resolver o problema manualmente

5. Examine o conteúdo do relatório. Você pode ordenar a tabela clicando em um cabeçalho. Para abrir um painel de detalhes, clique em uma linha selecionada.

Figura 3.2. Painel de detalhes



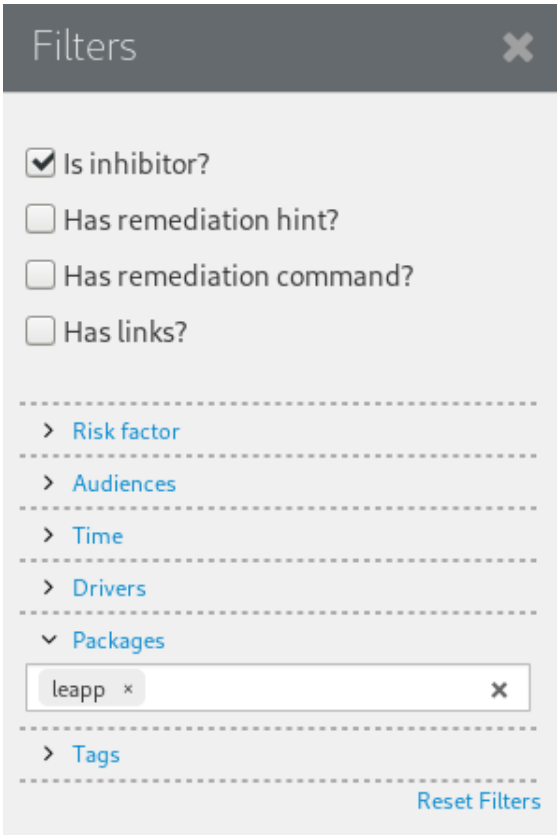
O painel de detalhes exibe as seguintes informações adicionais:

- Resumo do problema e links para artigos da Knowledgebase descrevendo o problema em mais detalhes

- Remediações - você pode executar ou agendar uma remediação automática (se disponível), e ver seus resultados quando aplicada
- Recursos do sistema afetados: pacotes, repositórios, arquivos (configuração, dados), discos, volumes

6. Opcionalmente, filtrar os resultados. Clique no botão **Filtros** no canto superior esquerdo acima do relatório e aplique um filtro com base em suas preferências. As categorias de filtros são aplicadas em conjunto umas com as outras.

Figura 3.3. Filtros



7. Selecione as questões para as quais você deseja aplicar uma remediação automatizada. Você tem duas opções:

   a. Escolha itens individuais clicando no botão **Adicionar ao Plano de Remediação** no painel de detalhes. Alternativamente, você pode executar remediações individuais diretamente clicando em **Executar Remediação** no painel de detalhes.

   b. Selecione todos os itens para os quais uma remediação está disponível, clicando no botão **Adicionar todas as remediações para planejar** no canto superior direito acima do relatório.

8. Reveja e responda as perguntas exigidas por **Leapp** no console web. Cada pergunta não respondida aparece como um título **Missing required answers in the answer file** no Relatório de Atualização. Selecione um título para responder à pergunta:

   a. Para confirmar a resposta padrão **True**, selecione **Adicionar ao Plano de Remediação** para executar a remediação mais tarde ou **Executar Remediação** para executar a remediação imediatamente.

   b. Para selecionar a resposta não inadimplente, execute uma das seguintes ações:

i. Execute o comando **leapp answer**, especificando a pergunta a que você está respondendo e sua resposta confirmada.

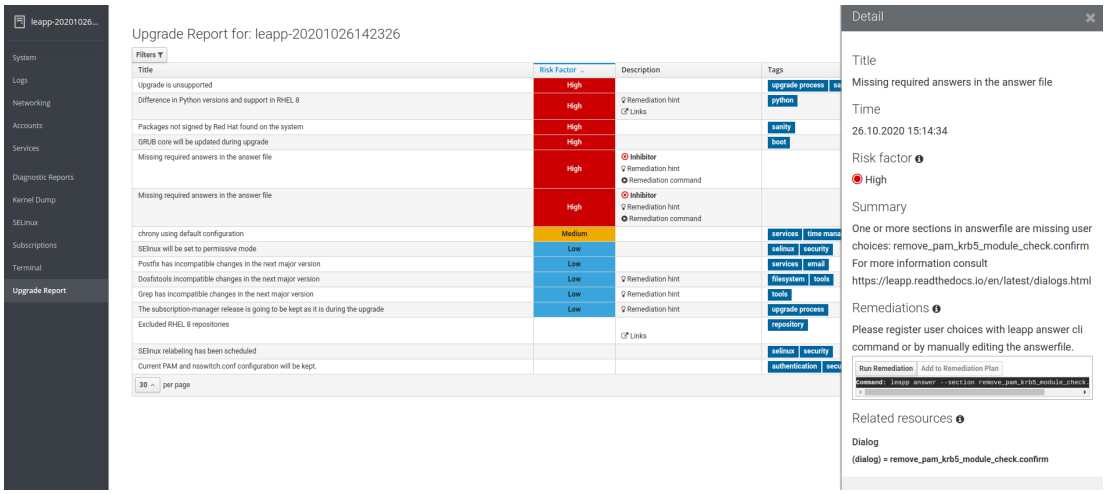
```
#resposta saltitante --secção question_section.confirm=answer
```

Por exemplo, para confirmar uma resposta a **False** à pergunta **Disable pam_pkcs11 module in PAM configuration?**, execute o seguinte comando:

```
# resposta pulo --section remove_pam_krb5_module_check.confirm=False
```

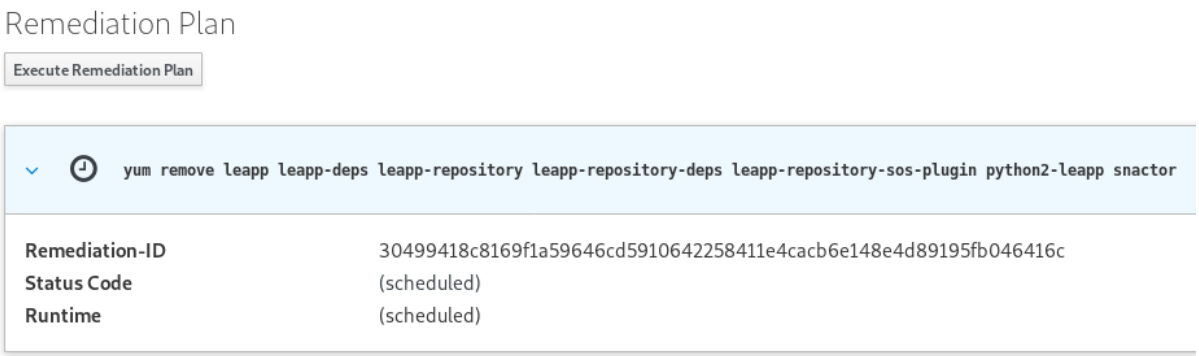
ii. Edite manualmente o arquivo **/var/log/leapp/answerfile**, descomente a linha **confirm** do arquivo deletando o símbolo **#**, e confirme sua resposta como **True** ou **False**; veja o exemplo do arquivo de respostas do Leapp .

Figura 3.4. Falta de resposta à pergunta Salto sem resposta



9. Abra o plano de remediação clicando no link **Plano de remediação** no canto superior direito acima do relatório. O plano de remediação fornece uma lista de todas as remediações executadas ou programadas.

Figura 3.5. Plano de remediação



10. Processe todas as remediações programadas clicando em **Executar Plano de Remediação**. As seguintes informações são exibidas para cada entrada de remediação:

- Uma identificação única da remediação
- Status da saída do comando
- Tempo transcorrido da remediação executada

- Saída padrão
- Erro padrão

11. Após executar as remediações selecionadas, gerar novamente o relatório de pré-atualização usando o comando **leapp preupgrade**, examinar o novo relatório e tomar medidas adicionais de remediação, se necessário.

CAPÍTULO 4. REALIZANDO A ATUALIZAÇÃO DA RHEL 7 PARA RHEL 8

Atualização para RHEL 8 usando o utilitário **Leapp**.

Pré-requisitos

- As etapas listadas em Preparação de um sistema RHEL 7 para a atualização foram concluídas, incluindo um backup completo do sistema.
- As etapas listadas em Revisão do relatório de pré-atualização foram concluídas e todos os problemas relatados resolvidos.

Procedimento

1. Em seu sistema RHEL 7, inicie o processo de atualização:

```
# leapp upgrade
```

NOTA

Se você vai usar repositórios personalizados do diretório **/etc/yum.repos.d/** para a atualização, habilite os repositórios selecionados da seguinte forma:

```
# salto de atualização --enablerepo repository_id1 --enablerepo
repository_id2...
```

Se você for atualizar sem a RHSM ou usando a RHUI, adicione a opção **--no-rhsm**.

No início do processo de atualização, **Leapp** executa a fase de pré-atualização descrita em Revisão do relatório de pré-atualização

Se o sistema for atualizável, **Leapp** faz o download dos dados necessários e prepara uma transação RPM para a atualização.

Se seu sistema não atender aos parâmetros para uma atualização confiável, **Leapp** encerra o processo de atualização e fornece um registro descrevendo o problema e uma solução recomendada no arquivo **/var/log/leapp/leapp-report.txt**. Para mais informações, consulte Solução de problemas .

2. Reinicialize o sistema manualmente:

```
# reboot
```

Nesta fase, o sistema inicia em uma imagem de disco RAM inicial baseada no RHEL 8, initramfs. **Leapp** atualiza todos os pacotes e reinicia automaticamente para o sistema RHEL 8.

Alternativamente, você pode executar o comando **leapp upgrade** com a opção **--reboot** e pular esta etapa do manual.

Se ocorrer uma falha, investigar os logs conforme descrito em Solução de Problemas.

3. Faça login no sistema RHEL 8 e verifique seu estado conforme descrito em Verificação do estado pós-atualização do sistema RHEL 8.

4. Tarefas completas de pós-atualização conforme descrito em Execução de tarefas de pós-atualização. Especialmente, reavaliar e reaplicar suas políticas de segurança.

CAPÍTULO 5. VERIFICANDO O ESTADO PÓS-ATUALIZAÇÃO DO SISTEMA RHEL 8

Este procedimento lista as etapas de verificação recomendadas para realizar após uma atualização no local para o RHEL 8.

Pré-requisitos

- O sistema foi atualizado seguindo os passos descritos em Execução da atualização de RHEL 7 para RHEL 8 e foi possível fazer o login no RHEL 8.

Procedimento

Após a atualização, determinar se o sistema está no estado exigido, pelo menos:

- Verificar se a versão atual do sistema operacional é o Red Hat Enterprise Linux 8:

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

- Verifique a versão do núcleo do SO:

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

  Note que **.el8** é importante.

- Se você estiver usando o Red Hat Subscription Manager:
  - Verificar se o produto correto está instalado:

```
# 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
```

  - Verificar se a versão de lançamento está definida para 8.2 imediatamente após a atualização:

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

- Verifique se os serviços de rede estão operacionais, por exemplo, tente se conectar a um servidor usando SSH.

- Verifique o status de pós-atualização de suas aplicações. Em alguns casos, pode ser necessário realizar mudanças de migração e configuração manualmente. Por exemplo, para migrar seus bancos de dados, siga as instruções na documentação do RHEL 8 Database Server .

CAPÍTULO 6. REALIZAÇÃO DE TAREFAS DE PÓS-ATUALIZAÇÃO

Este procedimento lista as principais tarefas recomendadas para executar após uma atualização no local para o RHEL 8.

Pré-requisitos

- O sistema foi atualizado seguindo os passos descritos em Execução da atualização de RHEL 7 para RHEL 8 e foi possível fazer o login no RHEL 8.
- O status da atualização no local foi verificado seguindo os passos descritos em Verificação do status pós atualização do sistema RHEL 8.

Procedimento

Após a realização da atualização, completar as seguintes tarefas:

1. Assegure-se de que seu sistema permaneça apoiado após a atualização no local. Com a disponibilidade geral do RHEL 8.3, atualize seu sistema para o RHEL 8.3 ou para o RHEL 8.2 Extended Update Support (EUS).
   a. Atualizar o sistema para RHEL 8.3:
      i. Gerente de Assinaturas da Red Hat não definido para consumir o mais recente conteúdo RHEL 8.3:

      ```
      # liberação do gerenciador de assinaturas --unset
      ```

      ii. Atualize seu sistema para a última versão RHEL 8.3:

      ```
      # yum atualização
      ```

   b. Atualizar o sistema para RHEL 8.2 EUS:
      i. Habilitar os repositórios RHEL 8 EUS:

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

      Substitua *repository_id** por IDs de repositórios EUS disponíveis com sua assinatura. Habilite pelo menos os repositórios BaseOS e AppStream. Por exemplo, na arquitetura Intel 64:

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

      ii. Atualize seu sistema para a última versão do RHEL 8.2.EUS

      ```
      # yum atualização
      ```

2. Se você atualizou usando o RHUI na AWS ou Microsoft Azure e sua certificação de software não estiver disponível em uma versão de versão menor, bloqueie seu sistema para uma versão de versão menor suportada por sua certificação.

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

3. Reavaliar e reaplicar suas políticas de segurança. Especialmente, mude o modo SELinux para o reforço da aplicação. Para detalhes, consulte Aplicando políticas de segurança .

CAPÍTULO 7. APLICAÇÃO DE POLÍTICAS DE SEGURANÇA

Durante o processo de atualização no local, certas políticas de segurança devem permanecer desabilitadas. Além disso, a RHEL 8 introduz um novo conceito de políticas criptográficas em todo o sistema e também os perfis de segurança podem conter mudanças entre as principais versões. Esta seção o orienta ao proteger seus sistemas RHEL atualizados.

7.1. ALTERANDO O MODO SELINUX PARA REFORÇAR

Durante o processo de atualização no local, o utilitário **Leapp** define o modo SELinux como permissivo. Quando o sistema é atualizado com sucesso, você tem que mudar manualmente o modo SELinux para o modo de execução.

Pré-requisitos

- O sistema foi atualizado e você executou as etapas de verificação descritas em Verificação do estado pós-atualização do sistema RHEL 8.

Procedimento

1. Certifique-se de que não haja negações de SELinux, por exemplo, utilizando o utilitário **ausearch**:

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

   Observe que a etapa anterior abrange apenas o cenário mais comum. Para verificar todas as negações de SELinux possíveis, consulte a seção Identificando negações de SELinux na seção Utilizando o título SELinux, que fornece um procedimento completo.

2. Abra o arquivo **/etc/selinux/config** em um editor de texto de sua escolha, por exemplo:

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

3. Configure a opção **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. Salve a mudança, e reinicie o sistema:

```
# reboot
```

Etapas de verificação

1. Após o reinício do sistema, confirme que o comando **getenforce** retorna **Enforcing**:

```
$ getenforce
Enforcing
```

Recursos adicionais

- Solução de problemas relacionados à SELinux
- Mudança de estados e modos SELinux

7.2. DEFINIÇÃO DE POLÍTICAS CRIPTOGRÁFICAS PARA TODO O SISTEMA

Políticas criptográficas é um componente do sistema que configura os subsistemas criptográficos centrais, cobrindo os protocolos TLS, IPSec, SSH, DNSSec, e Kerberos.

Após uma instalação bem sucedida ou um processo de atualização no local, a política de criptografia de todo o sistema é automaticamente definida para **DEFAULT**. O nível de política criptográfica de todo o sistema **DEFAULT** oferece configurações seguras para os modelos de ameaça atuais.

Para visualizar ou alterar a atual política criptográfica do sistema, use a ferramenta update-crypto-policies:

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

Por exemplo, o seguinte comando muda o nível da política de criptografia de todo o sistema para **FUTURE**, que deve resistir a qualquer ataque futuro a curto prazo:

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

A RHEL 8.2 também introduz a personalização das políticas criptográficas de todo o sistema. Para detalhes, consulte a personalização de políticas criptográficas em todo o sistema com modificadores de políticas e Criação e configuração de seções de políticas criptográficas personalizadas em todo o sistema.

Recursos adicionais

- Usando políticas criptográficas de todo o sistema
- **update-crypto-policies(8)** página do homem.

7.3. REMEDIANDO O SISTEMA A UMA LINHA DE BASE DE SEGURANÇA

A suíte OpenSCAP fornece remediações para tornar seu sistema compatível com linhas de base de segurança, tais como PCI-DSS, OSPP ou ACSC E8. Use as etapas do procedimento a seguir para alterar as configurações de seu sistema de acordo com o perfil do PCI-DSS.

IMPORTANTE

A Red Hat não fornece nenhum método automatizado para reverter as mudanças feitas por remediações de segurança. As remediações são suportadas nos sistemas RHEL na configuração padrão. Se seu sistema foi alterado após a instalação, a execução de remediações pode não o tornar compatível com o perfil de segurança exigido.

Pré-requisitos

- O pacote **scap-security-guide** está instalado em seu sistema RHEL 8.

Procedimento

1. Use o comando **oscap** com a opção **--remediate**:

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

   Você pode substituir *pci-dss* no exemplo anterior por um perfil exigido pelo seu cenário.

2. Reinicie seu sistema:

```
# reboot
```

Etapas de verificação

1. Avalie o sistema de conformidade com o perfil PCI-DSS, e salve os resultados no arquivo *pcidss_report.html*:

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

Recursos adicionais

- Verificação do sistema para conformidade e vulnerabilidades de segurança
- **scap-security-guide(8)** página do homem
- **oscap(8)** páginas do homem

CAPÍTULO 8. SOLUÇÃO DE PROBLEMAS

Você pode consultar as seguintes dicas para solucionar problemas na atualização da RHEL 7 para a RHEL 8.

8.1. RECURSOS PARA A SOLUÇÃO DE PROBLEMAS

Você pode consultar os seguintes recursos para a solução de problemas.

Console output

Por padrão, apenas mensagens de erro e de nível crítico de log são impressas para a saída do console pelo utilitário **Leapp**. Para alterar o nível de log, use as opções **--verbose** ou **--debug** com o comando **leapp upgrade**.

- No modo *verbose*, **Leapp** imprime informações, avisos, erros e mensagens críticas.
- No modo *debug*, **Leapp** imprime debug, info, warning, error, and critical messages.

Logs

- O arquivo **/var/log/leapp/leapp-upgrade.log** lista questões encontradas durante a fase initramfs.
- O diretório **/var/log/leapp/dnf-debugdata/** contém dados de depuração de transações. Este diretório só está presente se o comando **leapp upgrade** for executado com a opção **--debug**.
- O site **/var/log/leapp/answerfile** contém perguntas que devem ser respondidas por **Leapp**.
- O utilitário **journalctl** fornece logs completos.

Reports

- O arquivo **/var/log/leapp/leapp-report.txt** lista as questões encontradas durante a fase de pré-atualização. O relatório também está disponível no console web, veja Avaliando a possibilidade de atualização e aplicando remediações automatizadas através do console web.

8.2. DICAS DE SOLUÇÃO DE PROBLEMAS

Você pode consultar as seguintes dicas de solução de problemas.

Pre-upgrade phase

- Verifique se seu sistema atende a todas as condições listadas em Planejamento de uma atualização.
- Certifique-se de ter seguido todos os passos descritos em Preparando um sistema RHEL 7 para a atualização, por exemplo, seu sistema não usa mais de uma Placa de Interface de Rede (NIC) com um nome baseado no prefixo usado pelo kernel (**eth**).
- Certifique-se de ter respondido a todas as perguntas exigidas por **Leapp** no arquivo **/var/log/leapp/answerfile**. Se alguma resposta estiver faltando, **Leapp** inibe a atualização. Exemplos de perguntas:
  - Desativar o módulo pam_pkcs11 na configuração PAM?

- Desativar o módulo pam_krb5 na configuração PAM?
- Configurar PAM e nsswitch.conf com a seguinte chamada authselect?

- Certifique-se de ter resolvido todos os problemas identificados no relatório de pré-atualização, localizado em **/var/log/leapp/leapp-report.txt**. Para conseguir isso, você também pode usar o console web, conforme descrito em Avaliação da possibilidade de atualização e aplicação de remediações automatizadas através do console web.

Exemplo 8.1. Arquivo de respostas

A seguir, um exemplo de um arquivo **/var/log/leapp/answerfile** não editado que tem uma pergunta não respondida:

```
[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 =
```

O campo **Label** especifica a pergunta que requer uma resposta. Neste exemplo, a pergunta é **Disable pam_pkcs11 module in PAM configuration?**

Para responder à pergunta, descomente a linha **confirm** e digite uma resposta de **True** ou **False**. Neste exemplo, a resposta selecionada é **True**:

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

Download phase

- Se ocorrer um problema durante o download de pacotes RPM, examine os dados de depuração de transações localizados no diretório **/var/log/leapp/dnf-debugdata/**.

initramfs phase

- Durante esta fase, possíveis falhas o redirecionam para a casca de Dracut. Verifique o Diário de bordo:

  ```
  # journalctl
  ```

  Alternativamente, reinicie o sistema a partir da casca do Dracut usando o comando **reboot** e verifique o arquivo **/var/log/leapp/leapp-upgrade.log**.

Post-upgrade phase

- Se seu sistema parece ter sido atualizado com sucesso, mas inicializado com o antigo kernel RHEL 7, reinicie o sistema e verifique a versão do kernel da entrada padrão no GRUB.
- Certifique-se de ter seguido os passos recomendados na Verificação do estado pós-atualização do sistema RHEL 8.
- Se sua aplicação ou um serviço parar de funcionar ou se comportar incorretamente depois de ter trocado o SELinux pelo modo de aplicação, procure por negações usando o **ausearch**, **journalctl**ou **dmesg** utilidades:

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

Os problemas mais comuns são causados pela etiquetagem incorreta. Consulte Solução de problemas relacionados à SELinux para obter mais detalhes.

8.3. PROBLEMAS CONHECIDOS

A seguir estão os problemas conhecidos que você pode encontrar ao atualizar da RHEL 7 para a RHEL 8.

- A equipe de rede atualmente não funciona quando a atualização no local é realizada enquanto o Network Manager está desativado ou não instalado.
- Se você usar um proxy HTTP, o Gerenciador de Assinaturas da Red Hat deve ser configurado para usar tal proxy, ou o comando **subscription-manager** deve ser executado com a opção **--proxy <hostname>**. Caso contrário, uma execução do comando **subscription-manager** falha. Se você usar a opção **--proxy** ao invés da mudança de configuração, o processo de atualização falha porque **Leapp** é incapaz de detectar o proxy. Para evitar que este problema ocorra, edite manualmente o arquivo **rhsm.conf** como descrito em Como configurar o Proxy HTTP para o Gerenciamento de Assinaturas da Red Hat. (BZ#1689294)
- Se seu sistema RHEL 7 estiver instalado em um número de unidade lógica FCoE (LUN) e conectado a uma placa de rede que utiliza o driver **bnx2fc**, o LUN não é detectado no RHEL 8 após a atualização. Conseqüentemente, o sistema atualizado não inicia. (BZ#1718147)
- Se seu sistema RHEL 7 usa um driver de dispositivo que é fornecido pela Red Hat mas não está disponível no RHEL 8, **Leapp** inibe a atualização. Entretanto, se o sistema RHEL 7 usa um driver de dispositivo de terceiros que não está incluído na lista de drivers removidos (localizado em **/etc/leapp/repos.d/system_upgrade/el7toel8/actors/kernel/checkkerneldrivers/files/removed_drivers.txt**), **Leapp** não detecta tal driver e prossegue com a atualização. Conseqüentemente, o sistema pode falhar em inicializar após a atualização.
- Você não pode realizar uma atualização no local quando os módulos **winbind** e **wins** Samba são usados no arquivo **/etc/nsswitch.conf** no momento. A transação de atualização falha com as seguintes mensagens de erro e **Leapp** inibe a atualização:

```
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 contornar este problema, configure o sistema para que ele utilize apenas fornecedores locais para o banco de dados **user**, **groups**, e **hosts** durante a atualização:

1. Abra o arquivo de configuração do sistema **/etc/nsswitch.conf** e procure por entradas que contenham as cadeias de caracteres **winbind** ou **wins**.
2. Se você encontrar tais entradas, crie um backup de **/etc/nsswitch.conf**.
3. Editar **/etc/nsswitch.conf** e remover **winbind** ou **wins** das entradas que as contêm.
4. Realizar uma atualização no local.
5. Após a atualização, adicione as cordas **winbind** e **wins** às respectivas entradas em **/etc/nsswitch.conf**, com base nos requisitos de configuração de seu sistema. (BZ#1410154)

- O utilitário **Leapp** não altera a configuração de autenticação personalizada durante o processo de atualização. Se você usou o utilitário obsoleto **authconfig** para configurar a autenticação em seu sistema RHEL 7, a autenticação no RHEL 8 pode não funcionar corretamente. Para garantir que sua configuração personalizada funcione corretamente no sistema RHEL 8, reconfigure seu sistema RHEL 8 com o utilitário **authselect**.

IMPORTANTE

Durante a atualização no local, os módulos de autenticação (PAM) obsoletos **pam_krb5** ou **pam_pkcs11** plugáveis são removidos. Consequentemente, se a configuração do PAM em seu sistema RHEL 7 contiver os módulos **pam_krb5** ou **pam_pkcs11** e se esses módulos tiverem os valores de controle **required** ou **requisite**, a realização da atualização no local poderá resultar no bloqueio do sistema. Para resolver este problema, reconfigure seu sistema RHEL 7 para não usar **pam_krb5** ou **pam_pkcs11** antes de iniciar o processo de atualização.

- Nos sistemas IBM Z, **Leapp** espera sempre um disco DASD anexado. Conseqüentemente, se o arquivo **/etc/dasd.conf** não existir, a atualização no local falha. Para contornar este problema, crie um arquivo **dasd.conf** vazio, usando o comando **touch > /etc/dasd.conf**. (BZ#1783248)

- Se o nome de um pacote de terceiros (não assinado pela Red Hat) instalado em seu sistema for o mesmo que o de um pacote fornecido pela Red Hat, a atualização no local falha. Para contornar este problema, escolha uma das seguintes opções antes do upgrade:

  a. Remover o pacote de terceiros

  b. Substituir o pacote de terceiros pelo pacote fornecido pela Red Hat

- Durante uma atualização no local, o pacote **docker** é removido sem um aviso prévio. Se você usar containers no RHEL, migre para Podman antes de atualizar para o RHEL 8. Para instruções, veja Como migrar meus containers Docker para o Podman antes de mudar do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8?(BZ#1858711)

- Devido a razões de segurança, o suporte para os tipos de criptografia de um-DES (DES) e três-DES (3DES) foi removido do RHEL 8.3.0. A RHEL 7 Identity Management (IdM), entretanto, ainda suporta a criptografia 3DES.
  A atualização de um ambiente IdM de RHEL 7 para RHEL 8 é possível porque ambas as versões de RHEL preferem tipos de criptografia AES mais fortes por padrão:

Versão do IdM	Tipos de criptografia padrão	Tipos adicionais de criptografia suportados
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] A criptografia RC4 foi depreciada e desativada por padrão no RHEL 8, pois é considerada menos segura que os novos tipos de criptografia AES-128 e AES-256. Para mais informações sobre como ativar o suporte RC4 para compatibilidade com ambientes herdados do Active Directory, consulte Garantia de suporte para tipos comuns de criptografia em AD e RHEL.

Se você configurou manualmente um Centro de Distribuição Kerberos (KDC) não IdM, qualquer serviço, ou qualquer usuário para **only** usar criptografia DES ou 3DES, você poderá sofrer interrupções de serviço após atualização para os últimos pacotes Kerberos no RHEL 8, como por exemplo:

- Erros de autenticação Kerberos
- **unknown enctype** erros de criptografia
- Os KDCs com chaves mestras criptografadas em DES (**K/M**) não conseguem iniciar

A Red Hat recomenda que você não use a criptografia DES ou 3DES em seu ambiente. Para mais informações sobre a re-keying Kerberos principais para usar tipos de criptografia mais fortes, veja Retirando DES da Documentação do MIT Kerberos.

8.4. OBTENÇÃO DE APOIO

Você pode abrir um caso de suporte, selecionar *RHEL 8* como o produto, e fornecer um **sosreport** de seu sistema.

- Para gerar um **sosreport** em seu sistema, execute:

```
# sosreport
```

Observe que você pode deixar a identificação do caso vazia.

Para detalhes sobre como gerar um sosreport, veja a solução O que é um sosreport e como criar um no Red Hat Enterprise Linux?

Para mais informações sobre como abrir e gerenciar um caso de suporte no Portal do Cliente, veja o artigo Como abrir e gerenciar um caso de suporte no Portal do Cliente?

CAPÍTULO 9. INFORMAÇÕES RELACIONADAS

Você pode consultar os seguintes materiais instrucionais:

- Capacidades e limites da tecnologia Red Hat Enterprise Linux
- Considerações ao adotar a RHEL 8
- Personalizando seu Red Hat Enterprise Linux no local
- Como faço o upgrade do Red Hat Enterprise Linux 6 para o Red Hat Enterprise Linux 7?
- Atualização de RHEL 6 para RHEL 8
- Como converter de CentOS ou Oracle Linux para RHEL
- Atualização de Hosts de RHEL 7 para RHEL 8 no Red Hat Satellite
- Documentação da Red Hat Insights

APÊNDICE A. REPOSITÓRIOS RHEL 7

Antes da atualização, certifique-se de ter os repositórios apropriados habilitados conforme descrito no passo 3 do procedimento em Preparação de um sistema RHEL 7 para a atualização .

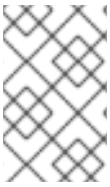
Se você planeja usar o Red Hat Subscription Manager durante o upgrade, você **must enable** os seguintes repositórios antes do upgrade, usando o **subscription-manager repos --enable *repository_id*** comando:

Arquitetura	Repositório	Identificação do Repositório
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 (pequeno endian)	Base	**rhel-7-for-power-le-rpms**
	Extras	**rhel-7-for-power-le-extras-rpms**
IBM POWER9 (pequeno 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 (Estrutura A)	Base	**rhel-7-for-system-z-a-rpms**
	Extras	**rhel-7-for-system-z-a-extras-rpms**

Você **can enable** os seguintes repositórios antes da atualização, usando o **subscription-manager repos --enable *repository_id*** comando:

Arquitetura	Repositório	Identificação do Repositório
Intel de 64 bits	Opcional	**rhel-7-server-optional-rpms**

Arquitetura	Repositório	Identificação do Repositório
	Suplemento	**rhel-7-server-supplementary-rpms**
ARM de 64 bits	Opcional	**rhel-7-for-arm-64-optional-rpms**
	Suplemento	N/A
IBM POWER8 (pequeno endian)	Opcional	**rhel-7-for-power-le-optional-rpms**
	Suplemento	**rhel-7-for-power-le-supplementary-rpms**
IBM POWER9 (pequeno endian)	Opcional	**rhel-7-for-power-9-optional-rpms**
	Suplemento	**rhel-7-for-power-9-supplementary-rpms**
IBM Z	Opcional	**rhel-7-for-system-z-optional-rpms**
	Suplemento	**rhel-7-for-system-z-supplementary-rpms**
IBM Z (Estrutura A)	Opcional	**rhel-7-for-system-z-a-optional-rpms**
	Suplemento	N/A



NOTA

Se você ativou um repositório RHEL 7 Opcional ou um repositório RHEL 7 Suplementar antes de uma atualização no local, **Leapp** habilita o Construtor Linux RHEL 8 CodeReady ou os repositórios RHEL 8 Suplementares, respectivamente.

Se você decidir usar repositórios personalizados, habilite-os de acordo com as instruções em Configuração de repositórios personalizados.