Sobre o Leapp

O Leapp é a ferramenta com suporte usada para realizar upgrades locais do sistema de uma versão principal do Red Hat® Enterprise Linux® à outra. Com o Leapp, você faz upgrade com confiança e se beneficia das novas funcionalidades do Red Hat Enterprise Linux, sem precisar reinstalar seus sistemas.

Por que fazer o upgrade?

O upgrade ajuda a garantir a manutenção da continuidade de negócios. Os clientes têm acesso às melhorias, correções e patches mais recentes usando soluções com suporte, juntamente com as novas funcionalidades que acompanham a nova versão principal do Red Hat Enterprise Linux.

As melhorias no desempenho do Red Hat Enterprise Linux reduzem o seu custo total de propriedade, influencia a produtividade e maximiza seu investimento em tecnologia.

O Red Hat Enterprise Linux funciona em um ciclo previsível de lançamentos principais trianual. Sua subscrição é válida para qualquer versão com suporte no momento do Red Hat Enterprise Linux. Você terá acesso à tecnologia emergente mais recente à medida que novas versões são disponibilizadas. Cada versão principal do Red Hat Enterprise Linux vem com suporte de 10 anos, dividido em duas fases.

A primeira fase é a de suporte total, que dura cinco anos após uma disponibilidade geral. São oferecidas novas funcionalidades, novo hardware com suporte, correção de problemas e bugs. Durante a segunda fase, o lançamento entra no suporte de manutenção, que continua com a publicação de erratas de segurança classificadas como "Crítica" e "Importante" e outras funcionalidades selecionadas ou melhorias com a correção de bugs. Após a conclusão do ciclo de vida normal de 10 anos, os clientes podem adquirir um complemento de extensão ao Suporte do Ciclo de Vida da Red Hat, que proporciona dois anos adicionais de suporte, incluindo erratas de segurança "Críticas" e "Importantes". Visite a página Ciclo de vida do Red Hat Enterprise Linux para mais informações.

Os clientes têm acesso a várias funcionalidades novas, fazendo o upgrade para o Red Hat Enterprise Linux, que incluem:

- O software atualizado, através de fluxos de aplicações, oferece ambientes de execução de linguagem mais novos, bancos de dados e outras aplicações em toda a fase de suporte completo de uma versão principal do Red Hat Enterprise Linux.
- As ferramentas de containers do Red Hat Enterprise Linux, como Podman, Buildah, e Skopeo que oferecem suporte a criação, implantação e gerenciamento de containers.
- A aplicação de patches em tempo real do Kernel (kpatch) que permite a você realizar correções para selecionar vulnerabilidades e exposições comuns (CVEs) importantes e críticas, sem precisar reiniciá-lo.

Leia o checklist "Principais motivos para usar o Red Hat Enterprise Linux"

- As ferramentas de observabilidade do desempenho que usam ferramentas baseadas em eBPF para obter rapidamente uma visão dos aspectos de desempenho do sistema.
- Suporte Flatpak que permite a execução de aplicações, tipicamente utilizadas para aplicações de desktop.
- Cgroup2 que oferece capacidades simplificadas para regular os recursos utilizados pelos processos.

Há uma série de melhorias de automação e gerenciamento, incluindo uma interface melhorada do console web para uma administração mais tranquila.

As melhorias de automação incluem:

- Novas funções do sistema para o Red Hat Enterprise Linux, com tecnologia do Red Hat Ansible® Automation Platform, para automatizar o gerenciamento em escala.
- Red Hat Insights, incluído em cada subscrição do Red Hat Enterprise Linux, que procura vulnerabilidades, omissões de funções e outros critérios pré-definidos de forma proativa.

Para aqueles focados em obter o máximo do seu hardware, convém notar que o Red Hat Enterprise Linux 9 supera as versões 7 e 8, em geral. Algumas mudanças que facilitam isso incluem:

- Novos escalonadores de disco para o kernel.
- Novos perfis de desempenho ajustados.

Para informações sobre a solução, visite Como fazer upgrade do Red Hat Enterprise Linux 6 para o Red Hat Enterprise Linux 8.

O que é o Leapp e por que usá-lo?

Fazer a atualização dos seus servidores pode ser uma tarefa complicada. Porém, o Red Hat Enterprise Linux inclui o Leapp, a ferramenta de gerenciamento de upgrade com suporte, que oferece um caminho único para o upgrade da próxima versão principal do Red Hat Enterprise Linux. O Leapp permite aos clientes manter a subscrição original (anexada ao sistema), as configurações do sistema e os repositórios personalizados e aplicações de terceiros.

O Leapp vem com o Red Hat Enterprise Linux 7 e o Red Hat Enterprise Linux 8, possibilitando o upgrade do Red Hat Enterprise Linux 7.9 para o Red Hat Enterprise Linux 8. Ele também pode ser usado para o upgrade do Red Hat Enterprise Linux 8 para o Red Hat Enterprise Linux 9.

Caso você esteja usando o Red Hat Enterprise Linux 6, será necessário fazer o upgrade para o Red Hat Enterprise Linux 7 usando outras ferramentas antes de passar ao Red Hat Enterprise Linux 8 ou 9 usando o Leapp.

A tabela abaixo lista os benefícios de fazer o upgrade do seu servidor com o Leapp.

Upgrade no local com o Leapp	Reinstalação
Preserva a configuração	Os dados de configuração precisam ser copiados para o backup e reinicializados
As máquinas retêm os dados de subscrição existentes	As máquinas têm que ser subscritas utilizando o gerenciador de subscrições
Influencia positivamente a produtividade com a automação	Tempo e custo adicionais

Como funciona?

Entender como o Leapp funciona melhorará sua capacidade de realizar um upgrade bem-sucedido. O uso do Leapp é um processo de duas fases que consiste em uma análise de upgrade e o upgrade propriamente dito. São necessárias reinicializações posteriores, e é importante que isto seja contabilizado ao planejar seu upgrade.

Para um único host usando o Leapp, a análise de upgrade se baseia em considerações sobre o upgrade, baixados como metadados do *cloud.redhat.com*.

Para hosts conectados ao Red Hat Satellite, os metadados precisam ser distribuídos pelo Satellite para os servidores usando o Leapp. A análise de upgrade pode então ser realizada em escala usando o plugin do Leapp para o Red Hat Satellite.

A análise de upgrade gera um relatório que pode conter itens para você resolver antes que o upgrade seja realizado.

O Leapp usa vários programas Python como parte do fluxo de trabalho. Esses programas Python são denominados "atores" e podem realizar alterações no seu sistema.

Leia "Use o Red Hat Satellite para realizar upgrade com o Leapp"

Um exemplo de ator é o **CheckOSRelease** que verificará se a versão de manutenção atual do Red Hat Enterprise Linux tem suporte. Caso contrário, isso inibirá o processo de upgrade.

Se você tem uma questão de upgrade não tratada pelo conjunto de atores existente, você pode escrever seu próprio ator personalizado para remediar, inibir ou receber informações sobre essas questões. Seu ator pode então ser incorporado ao fluxo de trabalho do Leapp.

O Leapp está integrado com o Red Hat Insights para verificar sua população registrada e determinar quais máquinas são elegíveis para um upgrade.

O upgrade com o Leapp pode ser executado com a linha de comando ou o Red Hat Satellite.

Limitações

Antes de proceder com o upgrade de seu servidor, você precisa entender algumas limitações importantes do uso do Leapp:

- Ele só pode ser usado para upgrade de uma versão principal do Red Hat Enterprise Linux para a versão principal seguinte.
- Se seu sistema utiliza criptografia de disco para o sistema de arquivos raiz, o Leapp não funcionará.
- Os dispositivos VDO devem ser convertidos para serem gerenciados pelo LVM.
- Multipath baseados em rede ou montagens de armazenamento em rede como o iSCSI ou o sistema de arquivos de rede (NFS) não podem ser usados para uma partição do sistema.
- As instâncias sob demanda na nuvem pública que utilizam o Red Hat Update Infrastructure (diferente do Red Hat Subscription Manager) não são elegíveis para o upgrade com o Leapp.

Estou pronto: por onde começo o upgrade?

Vamos ver como seria um upgrade do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8. Um upgrade do Red Hat Enterprise Linux 8 para o Red Hat Enterprise Linux 9 seguiria um fluxo de trabalho semelhante. Certifique-se de ter feito o update do seu sistema para o Red Hat Enterprise Linux 7.9 usando **yum update:**

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

O pacote do **Leapp** precisa ser instalado. Confira se sua máquina está subscrita no Red Hat CDN ou em seu servidor Satellite, com o canal do Red Hat Enterprise Linux 7 Extras ativado. Isso pode ser verificado usando o 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
```

Se o repositório rhel-7-server-extras-rpms não estiver ativado, você poderá ativá-lo usando:

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

O Leapp pode ser instalado agora no Red Hat Enterprise Linux 7 usando:

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

Se você estiver fazendo o upgrade do Red Hat Enterprise Linux 8 para o Red Hat Enterprise Linux 9, revise os seguintes passos para instalar o utilitário de upgrade do Leapp no local. Os servidores do Red Hat Enterprise Linux 8 podem precisar ser atualizados antes do upgrade para o Red Hat Enterprise Linux 9. Consulte os Caminhos de upgrade no local com suporte para o Red Hat Enterprise Linux para obter informações adicionais.

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

Os pacotes **leapp** e **leapp-upgrade-el8toel9** precisam ser instalados e ambos estão disponíveis no repositório **rhel-8-for-x86_64-appstream-rpms**. Instale-os, usando:

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

Se você executou antes um upgrade no local do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8, remova o diretório **/root/tmp_leapp_py3** se estiver presente no seu sistema:

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

Quando você tiver instalado o(s) pacote(s) de upgrade no local do Leapp para sua versão do Red Hat Enterprise Linux, seu servidor precisará ser analisado com o **pré-upgrade do Leapp** antes de realizar o upgrade, para identificar possíveis problemas. Seu sistema permanece inalterado e cria arquivos importantes que vão traçar seu caminho de atualização.

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

Após executar o comando de pré-upgrade, é provável que você veja resultados semelhantes a estes:

```
…
 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
```

Arquivos importantes:

/var/log/leapp/leapp-report.txt	Informações acessíveis e compreensíveis sobre o relatório de upgrade do Leapp
/var/log/leapp/leapp-report.json	O arquivo formatado JSON equivalente
/var/log/leapp/leapp-preupgrade.log	A saída da depuração do comando de pré-upgrade do Leapp
/var/log/leapp/answerfile	Respostas às perguntas do comando de pré-upgrade do Leapp

O relatório de análise do upgrade é armazenado em **/var/log/leapp/leapp-report.txt** e há importantes pontos para você levar em consideração antes de realizar o upgrade. Essas considerações podem exigir um input de sua parte que pode ser tratado seguindo as instruções contidas no relatório.

Como abordar as considerações de pré-upgrade do Leapp

Pode haver vários itens de ação para você abordar no relatório de pré-atualização do Leapp em /var/log/leapp/leapp-report.txt. Um ***inibidor*** é um item de bloqueio que você precisará verificar a fim de prosseguir com o upgrade. Se os inibidores não forem resolvidos, o upgrade não será realizado no sistema pelo Leapp.

O ***fator de risco*** descreve o efeito de uma consideração de atualização usando as seguintes chaves:

Alto	Muito provável que resulte em um estado deteriorado
Médio	Pode afetar tanto o sistema quanto as aplicações
Baixo	Não deve afetar o sistema, mas pode ter um efeito sobre as aplicações
Informações	Informação sem efeito esperado, nem para o sistema, nem para as aplicações

O ***título*** identifica um elemento do relatório de pré-upgrade do Leapp e o resumo oferece mais informações.

O ***resumo*** oferece uma breve descrição do problema detectado a ser tratado.

Uma ***correção*** é uma solução acionável para um problema relatado. Tipos de correções comuns incluem:

- editar um arquivo de configuração.
- executar um comando que muda a forma como seu sistema se comporta.
- correção através do arquivo de resposta do Leapp.
- correção que afeta o software de modulação da Biblioteca de Coleções de Software do Red Hat Enterprise Linux 7, como Python, PHP, Node.js, PostgreSQL etc.
- desmontar temporariamente as exportações do NFS.

Exemplos de considerações de upgrade para fatores de alto e médio risco são mostrados nesta seção e estruturados para incluir:

- A mensagem relatada no relatório do Leapp, no fragmento de exemplo.
- O subsistema do software afetado.
- Uma explicação do que significa o item assinalado.
- Ação que você deve tomar.
- As consequências de não tratar o item acionável assinalado.

Seus sistemas podem apresentar considerações diferentes dependendo da versão do Red Hat Enterprise Linux para a qual será feito o upgrade e de sua configuração.

Exemplo 1: um inibidor de alto risco que requer mudanças temporárias em seu sistema

Este é um exemplo de um problema com um inibidor, de alta classificação, assinalado pelo relatório de pré-avaliação. Se este problema não for corrigido, um upgrade com o Leapp neste sistema apresentará um erro e o upgrade será malsucedido. Além da mensagem em si, vamos analisar como resolver essa questão no 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
```

O que acontece se ignorar essa nota?

É um inibidor e impedirá que o upgrade prossiga até que a ação apropriada seja tomada. O fator de risco é alto porque se espera que sejam feitas mudanças somente no servidor local e não nas unidades NFS.

Qual subsistema é afetado?

Montagens do NFS.

O que isso significa?

As montagens do NFS não podem ser usadas durante o processo de upgrade e devem ser desativadas até que o upgrade tenha terminado.

O que devo fazer?

Edite /etc/fstab para converter em comentário as ações do NFS temporariamente e desmontar as ações do NFS montadas atualmente. Parar e desativar temporariamente o autofs.service. As entradas do NFS e o autofs.service podem ser reativadas assim que o upgrade for concluído.

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

Exemplo 2: um inibidor de alto risco que requer alterações em um arquivo de configuração existente

Isso se aplica principalmente ao upgrade do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 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
```

O que acontece se ignorar essa nota?

É um inibidor e impedirá que o upgrade prossiga, mas vale a pena notar que o fator de risco é alto, e o tratamento incorreto desse item pode impedir que você faça login remoto em seu servidor usando o shell seguro (SSH).

Qual subsistema é afetado?

O servidor ssh (sshd.service).

O que isso significa?

Esse fragmento indica uma mudança de alto impacto entre a maneira como o servidor SSH funciona entre o Red Hat Enterprise Linux 7 e o Red Hat Enterprise Linux 8. A autenticação da senha é proibida para o usuário raiz no Red Hat Enterprise Linux 8 por padrão. No Red Hat Enterprise Linux 7, o valor padrão implícito para PermitRootLogin é sim, mas no Red Hat Enterprise Linux 8, o valor padrão implícito é "prohibit-password".

Uma diretiva de configuração implícita aparece como um comentário em /etc/ssh/sshd_config, mas não é um comentário. Ele aparece para informar os valores padrão da diretiva.

O que devo fazer?

Certifique-se de conseguir fazer o login como outro usuário, com ou sem senha.

Você deve configurar explicitamente um valor para o PermitRootLogin em /etc/ssh/sshd_config. O valor pode ser sim, para permitir que o usuário raiz faça o login via ssh, ou não, para evitar isso. O que importa é que a diretiva seja explicitamente definida.

As páginas do manual do Linux são excelente fontes para obter informações adicionais. Use o comando **man sshd_config** e busque pela string *PermitRootLogin* para saber mais sobre esta diretiva de configuração.

Exemplo 3: um inibidor de alto risco que requer o uso do arquivo de resposta do Leapp

Essa questão específica é aplicável principalmente ao upgrade do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8. O elemento único deste exemplo é que ele requer a correção usando o arquivo de respostas do Leapp, um arquivo no qual os dados podem ser automaticamente passados para o seu utilitário.

```
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
```

O que acontece se ignorar essa nota?

É um inibidor e impedirá que o upgrade continue até que você autorize a remoção do módulo pam_pkcs11. O fator de risco é alto porque você pode ter os valores de controle *necessários ou requeridos* associados ao módulo pam_pkcs11 em sua configuração PAM, e a remoção desse módulo no Red Hat Enterprise Linux 8 poderia bloquear você fora de seu sistema.

Esse item do upgrade **só** pode ser resolvido com o uso do arquivo de resposta do Leapp.

Qual subsistema é afetado?

Autenticação (pam).

O que isso significa?

Esse fragmento diz que o módulo pam_pkcs11 foi removido do Red Hat Enterprise Linux 8 e sua funcionalidade é agora fornecida pela sssd.

O que devo fazer?

Edite o /var/log/leapp/answerfile como a seguir:

```
[remove_pam_pkcs11_module_check]

confirm = True
```

Ou execute o seguinte comando para editar o arquivo de respostas /var/log/leapp/answerfile:

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

Você também deve verificar se existem outras formas de autenticação que não dependem do módulo pam_pkcs11.

Isso pode ser verificado executando **grep pam_pkcs11 /etc/pam.d/***

Visite Gerenciar software a partir de um fluxo de aplicação para o laboratório hands-on

Exemplo 4: uma consideração de alto risco, não inibidora, que afeta os programas Python pós-upgrade

Este exemplo se aplica principalmente ao upgrade de máquinas do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8. Ao contrário dos exemplos anteriores, não é um inibidor, o que significa que a ferramenta de upgrade do Leapp realizará um upgrade mesmo se esse problema detectado não for resolvido. A decisão sobre a resolução dessa questão será tomada pelo administrador de sistema. Saber se esta máquina usa ou não aplicações baseadas em Python2 e se essas aplicações são compatíveis com Python3 fornecidas pelo sistema operacional atualizado também deve ser determinado pelo administrador de sistema.

```
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
```

O que acontece se ignorar essa nota?

Esse não é um inibidor, e ignorar a solução não impedirá que o comando de upgrade do Leapp prossiga. O fator de risco é alto porque o comando python não versionado (/usr/bin/python) não está disponível por padrão no Red Hat Enterprise Linux 8. A execução do intérprete do python diretamente (por exemplo, de um terminal) ou indiretamente (outro processo executa o comando para você) vai falhar.

Qual subsistema é afetado?

Python e aplicações que dependem do comando não versionado /usr/bin/python.

O que isso significa?

Apesar de Python 2 ter se tornado obsoleto em comparação ao Python 3, ele ainda pode ser instalado utilizando fluxos de aplicação. O repositório de fluxos de aplicações oferece vários módulos Python que você pode instalar em paralelo no seu servidor. Você deve sempre especificar a versão do Python instalando-a, invocando-a ou interagindo com ela. O comando Python não versionado não está disponível por padrão, mas ainda pode ser configurado se você desejar.

O que devo fazer?

Você pode executar o seguinte comando para garantir que o /usr/bin/python3 seja usado como a versão padrão do python:

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

Quaisquer aplicações que explicitamente requerem Python 2 precisam fazer referência a /usr/bin/python2 ou você poderia definir a versão padrão de Python para Python 2, usando o seguinte comando:

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

Exemplo 5: uma consideração de risco médio, não inibidora

Esse exemplo é aplicável principalmente ao upgrade do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 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
```

O que acontece se ignorar essa nota?

Esse não é um inibidor e não impedirá que o upgrade do Leapp prossiga. O fator de risco é classificado como médio, pois os clientes do protocolo NTP (Network Time Protocol) que estão configurados para obter o tempo de múltiplos servidores, obterão tempos diferentes de servidores diferentes com o "leap smear". Esses servidores não implementam o mesmo "leap smear", ou nem todos implementam o "leap smear". Isso pode fazer com que os clientes NTP parem de atualizar seus relógios ou saltem aleatoriamente entre os servidores.

Qual subsistema é afetado?

Sincronização de tempo usando o Chrony.

O que isso significa?

O Chrony implementa a sincronização de tempo usando o NTP. No Red Hat Enterprise Linux 8, a diretiva de pool é usada por padrão para referenciar um pool de servidores NTP com as mesmas capacidades. A utilização de várias diretivas de servidores que fazem referência a servidores NTP com diferentes capacidades poderia causar uma sincronização de tempo degradada.

O que devo fazer?

A partir de /etc/chrony.conf, remova quaisquer diretivas *leapsectz* e *leapfile* e use a diretiva de pool, em vez da diretiva do servidor, em /etc/chrony.conf. Isso garantirá que servidores NTP com as mesmas capacidades sejam utilizados.

Se você desejar sincronizar o tempo de seu sistema com servidores explicitamente definidos, certifique-se de que todos os servidores tenham as mesmas capacidades.

Leia o checklist "Principais motivos para usar o Red Hat Enterprise Linux"

Estou pronto para o upgrade!

Após tratar os problemas identificados no relatório de pré-upgrade, é recomendável executar novamente o comando de **pré-upgrade do leapp** e revisitar o arquivo do relatório para garantir que não haja omissões, o que impediria um upgrade bem-sucedido.

Quando seu sistema estiver pronto para o upgrade, execute o comando: **leapp upgrade** ou **leapp upgrade --reboot**

Visite O que é o BOOM e como instalá-lo?

O comando **leapp upgrade** enfileira o processo de atualização, e são necessárias várias reinicializações para a conclusão. É importante que isso esteja planejado. Antes da primeira inicialização, você poderá continuar usando sua versão do Red Hat Enterprise Linux atual.

Para mais informações sobre o gerenciamento de upgrades do sistema com snapshots

O comando do **leapp upgrade reboot** reinicializará o servidor automaticamente.

Primeira inicialização: o carregador de inicialização vai inicializar automaticamente um ambiente de upgrade especial usando a entrada de menu **Red Hat Enterprise Linux-Upgrade-Initramfs**. É dentro desse ambiente de upgrade que seu servidor será atualizado. É necessário um backup caso você queira reverter o upgrade e continuar usando a versão principal anterior do Red Hat Enterprise Linux.

Segunda inicialização: etiquetas SELinux serão restauradas, e o seu servidor será reinicializado mais uma vez.

Terceira inicialização: você poderá validar seu upgrade e iniciar sua experiência com o novo Red Hat Enterprise Linux.

Valide a versão do Red Hat Enterprise Linux atualmente em uso:

```
[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
```

Se você estiver fazendo o upgrade do Red Hat Enterprise Linux 7 para o Red Hat Enterprise Linux 8, você poderá ver um repositório denominado *rhel-8-server-rpms*, mas o Red Hat Enterprise Linux 8 apresenta dois repositórios: *rhel-8-for-x86_64-baseos-rpms* que oferece a configuração principal da funcionalidade subjacente do sistema operacional e *rhel-8-for-x86_64-appstream-rpms* que inclui aplicações adicionais de espaço do usuário, linguagens de ambiente de execução e banco de dados para o suporte de várias cargas de trabalho e casos de uso. Isso pode ser verificado como a seguir:

```
[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
```

```
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
```

Quando seu sistema tiver terminado o upgrade e reinicializado, você deve rever o **/var/log/leapp/leapp-report.txt** que agora tem seu relatório pós-upgrade com itens de ação adicionais para você concluir.

Tem alguma dica para mim?

Antes de começar, pense nas seguintes considerações.

sosreport

Considere a possibilidade de gerar um relatório sosreport para que possamos oferecer a você suporte caso precise.

1. Use o **yum install sos** para garantir que o pacote de sos esteja instalado.
2. Gere um relatório usando o comando **sosreport**.
3. Copie o arquivo tar gerado de **/var/tmp/** para um local seguro caso você precise do Red Hat Support.

Verifique se você tem um backup

No caso de circunstâncias imprevistas que façam com que seu sistema fique inoperante ou que seus dados fiquem inacessíveis, a capacidade de recuperar a tempo e retomar as operações é de suma importância. Os backups de dados facilitam o processo de recuperação, e talvez você já tenha realizado isso. Mas deve ser enfatizado: você deve fazer backup de seus dados antes de usar o Leapp para atualizar seus servidores.

Use suas ferramentas atuais para implementar uma estratégia de backup.

- Identifique os dados que são pertinentes à operação de seu servidor.
- Faça o backup de seus dados para um local seguro, fora do servidor que está sendo atualizado.
- Teste seu backup para garantir que os dados foram copiados com sucesso.
- Verifique se você poder restaurar os dados a partir de seu backup.
- Valide seu plano de recuperação de desastres para garantir que você esteja suficientemente preparado para a possível perda de seu servidor.

Use o Red Hat Insights

O Red Hat Insights pode ser usado para determinar sua capacidade de upgrade.

Aproveite o Red Hat Satellite Server ao máximo

O Red Hat Satellite Server pode aproveitar o plugin do Leapp para escanear e atualizar sistemas elegíveis em escala.

Use o console web

Considere o uso do console web para facilitar o processo de upgrade. Ele apresenta o relatório de pré-upgrade em um formato fácil de ler.

Você deve assegurar se tem o cockpit e os pacotes cockpit-leapp instalados usando **yum install cockpit cockpit-leapp**.

Use o **systemctl enable --now cockpit.socket** para ativar o soquete do cockpit.

Adicione a porta do console web ao seu firewall usando **firewall-cmd --add-port 9090/tcp** e certifique-se de que a regra seja adicionada à configuração permanente do firewall usando **firewall-cmd --add-port 9090/tcp --permanent**.

Agora, acesse o console web em *https://your_server_name:9090*

Requisitos para o repositório do Satellite

Se você estiver usando o Satellite Server para gerenciar pacotes, certifique-se de ter os seguintes repositórios disponíveis:

- 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

Se você tiver usado o comando yum versionlock para bloquear pacotes para uma versão específica, apague-os com **yum versionlock clear**.

Sobre a Red Hat

A Red Hat é a líder mundial em soluções de software open source empresariais e utiliza uma abordagem impulsionada pela comunidade para oferecer tecnologias confiáveis e de alto desempenho em Linux, nuvem híbrida, containers e Kubernetes. A Red Hat ajuda os clientes a desenvolver aplicações nativas em nuvem, a integrar aplicações de TI existentes e novas e a automatizar e gerenciar ambientes complexos. Parceira de confiança das empresas da Fortune 500, a Red Hat fornece serviços de consultoria, treinamento e suporte premiados, compartilhando os benefícios da inovação open source com todos os setores. Como um hub de conectividade em uma rede global de empresas, parceiros e comunidades, a Red Hat ajuda organizações a crescer, se transformar e se preparar para o futuro digital.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

br.redhat.com
#F31715_0822