



Red Hat Enterprise Linux 8

8.2 Notas de Lançamento

Notas de Lançamento do Red Hat Enterprise Linux 8.2

Red Hat Enterprise Linux 8 8.2 Notas de Lançamento

Notas de Lançamento do Red Hat Enterprise Linux 8.2

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

Copyright © This material may only be distributed subject to the terms and conditions set forth in the GNU Free Documentation License (GFDL), V1.2 or later (the latest version is presently available at <http://www.gnu.org/licenses/fdl.txt>).

Resumo

As Notas de Lançamento fornecem uma cobertura de alto nível das melhorias e adições que foram implementadas no Red Hat Enterprise Linux 8.2 e documentam problemas conhecidos neste lançamento, bem como correções de bugs notáveis, Technology Previews, funcionalidade depreciada e outros detalhes.

Índice

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT	5
CAPÍTULO 1. VISÃO GERAL	6
Instalador e criação de imagem	6
Serviços de infra-estrutura	6
Segurança	6
Linguagens de programação dinâmica, servidores web e de banco de dados	6
Conjuntos de ferramentas de compilação	6
Gestão da Identidade	6
O console web	7
Desktop	7
Atualização in loco	7
Recursos adicionais	8
Laboratórios do Portal do Cliente Red Hat	8
CAPÍTULO 2. ARQUITETURAS	9
CAPÍTULO 3. DISTRIBUIÇÃO DO CONTEÚDO NO RHEL 8	10
3.1. INSTALAÇÃO	10
3.2. REPOSITÓRIOS	10
3.3. FLUXOS DE APLICAÇÃO	11
CAPÍTULO 4. LANÇAMENTO RHEL 8.2.1	12
4.1. NOVAS CARACTERÍSTICAS	12
CAPÍTULO 5. NOVAS CARACTERÍSTICAS	14
5.1. INSTALADOR E CRIAÇÃO DE IMAGEM	14
5.2. GESTÃO DE SOFTWARE	14
5.3. CONCHAS E FERRAMENTAS DE LINHA DE COMANDO	15
5.4. SERVIÇOS DE INFRA-ESTRUTURA	16
5.5. SEGURANÇA	17
5.6. TRABALHO EM REDE	24
5.7. KERNEL	26
5.8. SISTEMAS DE ARQUIVO E ARMAZENAMENTO	30
5.9. ALTA DISPONIBILIDADE E CLUSTERS	32
5.10. LINGUAGENS DE PROGRAMAÇÃO DINÂMICA, SERVIDORES WEB E DE BANCO DE DADOS	33
5.11. COMPILADORES E FERRAMENTAS DE DESENVOLVIMENTO	36
5.12. GESTÃO DA IDENTIDADE	45
5.13. DESKTOP	49
5.14. INFRA-ESTRUTURAS GRÁFICAS	49
5.15. O CONSOLE WEB	50
5.16. VIRTUALIZAÇÃO	52
5.17. CONTÊINERES	52
CAPÍTULO 6. MUDANÇAS IMPORTANTES NOS PARÂMETROS DO KERNEL EXTERNO	54
6.1. NOVOS PARÂMETROS DO KERNEL	54
6.2. PARÂMETROS DE KERNEL ATUALIZADOS	56
6.3. NOVOS PARÂMETROS /PROC/SYS/KERNEL	58
6.4. PARÂMETROS ATUALIZADOS /PROC/SYS/KERNEL	59
6.5. PARÂMETROS ATUALIZADOS /PROC/SYS/NET	59
CAPÍTULO 7. DRIVERS DE DISPOSITIVOS	61
7.1. NOVOS MOTORISTAS	61

Drivers de rede	61
Drivers gráficos e drivers diversos	61
Drivers de armazenamento	62
7.2. DRIVERS ATUALIZADOS	62
Atualizações de driver de rede	62
Atualizações gráficas e de drivers diversos	62
Atualizações do driver de armazenamento	62
CAPÍTULO 8. CORREÇÃO DE ERROS	64
8.1. INSTALADOR E CRIAÇÃO DE IMAGEM	64
8.2. GESTÃO DE SOFTWARE	65
8.3. CONCHAS E FERRAMENTAS DE LINHA DE COMANDO	66
8.4. SERVIÇOS DE INFRA-ESTRUTURA	67
8.5. SEGURANÇA	68
8.6. TRABALHO EM REDE	70
8.7. KERNEL	71
8.8. SISTEMAS DE ARQUIVO E ARMAZENAMENTO	72
8.9. LINGUAGENS DE PROGRAMAÇÃO DINÂMICA, SERVIDORES WEB E DE BANCO DE DADOS	73
8.10. COMPILADORES E FERRAMENTAS DE DESENVOLVIMENTO	73
8.11. GESTÃO DA IDENTIDADE	76
8.12. DESKTOP	77
8.13. VIRTUALIZAÇÃO	77
8.14. CONTÊINERES	78
CAPÍTULO 9. ANTEVISÕES TECNOLÓGICAS	79
9.1. TRABALHO EM REDE	79
9.2. KERNEL	80
9.3. SISTEMAS DE ARQUIVO E ARMAZENAMENTO	81
9.4. ALTA DISPONIBILIDADE E CLUSTERS	84
9.5. GESTÃO DA IDENTIDADE	85
9.6. DESKTOP	86
9.7. INFRA-ESTRUTURAS GRÁFICAS	86
9.8. FUNÇÕES DO SISTEMA RED HAT ENTERPRISE LINUX	86
9.9. VIRTUALIZAÇÃO	87
9.10. CONTÊINERES	89
CAPÍTULO 10. FUNCIONALIDADE DEPRECIADA	90
10.1. INSTALADOR E CRIAÇÃO DE IMAGEM	90
10.2. GESTÃO DE SOFTWARE	91
10.3. SEGURANÇA	91
10.4. TRABALHO EM REDE	92
10.5. KERNEL	92
10.6. SISTEMAS DE ARQUIVO E ARMAZENAMENTO	93
10.7. DESKTOP	94
10.8. INFRA-ESTRUTURAS GRÁFICAS	94
10.9. O CONSOLE WEB	94
10.10. VIRTUALIZAÇÃO	94
10.11. PACOTES DEPRECIADOS	95
CAPÍTULO 11. PROBLEMAS CONHECIDOS	96
11.1. INSTALADOR E CRIAÇÃO DE IMAGEM	96
11.2. GESTÃO DE ASSINATURAS	99
11.3. CONCHAS E FERRAMENTAS DE LINHA DE COMANDO	99
11.4. SEGURANÇA	99

11.5. TRABALHO EM REDE	107
11.6. KERNEL	107
11.7. SISTEMAS DE ARQUIVO E ARMAZENAMENTO	111
11.8. LINGUAGENS DE PROGRAMAÇÃO DINÂMICA, SERVIDORES WEB E DE BANCO DE DADOS	114
11.9. COMPILADORES E FERRAMENTAS DE DESENVOLVIMENTO	115
11.10. GESTÃO DA IDENTIDADE	115
11.11. DESKTOP	118
11.12. INFRA-ESTRUTURAS GRÁFICAS	120
11.13. O CONSOLE WEB	120
11.14. VIRTUALIZAÇÃO	121
11.15. APOIO	123
11.16. CONTÊINERES	123
CAPÍTULO 12. INTERNACIONALIZAÇÃO	124
12.1. RED HAT ENTERPRISE LINUX 8 IDIOMAS INTERNACIONAIS	124
12.2. MUDANÇAS NOTÁVEIS NA INTERNACIONALIZAÇÃO DA RHEL 8	124
APÊNDICE A. LISTA DE BILHETES POR COMPONENTE	126
APÊNDICE B. HISTÓRICO DE REVISÃO	133

2021-02-22Red Hat

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, certifique-se de estar visualizando a documentação no formato Multi-página HTML. Destaque a parte do texto que você deseja comentar. Em seguida, clique no pop-up **Add Feedback** que aparece abaixo do texto destacado, e siga as instruções exibidas.
- 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. VISÃO GERAL

Instalador e criação de imagem

No RHEL 8.2, você pode registrar seu sistema, anexar assinaturas RHEL e instalar a partir da Red Hat Content Delivery Network (CDN) antes da instalação do pacote. Você também pode registrar seu sistema na Red Hat Insights durante a instalação. Instalações interativas GUI, bem como instalações Kickstart automatizadas, suportam estes novos recursos.

Para mais informações, veja [Seção 5.1, "Instalador e criação de imagem"](#).

Serviços de infra-estrutura

O **Tuned** a ferramenta de ajuste do sistema foi rebaseada para a versão 2.13, que adiciona suporte para o ajuste dependente da arquitetura e múltiplas diretrizes de inclusão.

Para mais informações, veja [Seção 5.4, "Serviços de infra-estrutura"](#).

Segurança

System-wide cryptographic policies agora apoia **customization**. O administrador pode agora definir uma política completa ou modificar apenas certos valores.

O RHEL 8.2 inclui os pacotes de **análise de setools-gui** e **setools-console** que fornecem ferramentas para análise da política SELinux e inspeções de fluxo de dados.

O Guia de Segurança SCAP agora fornece um perfil em conformidade com o Centro Australiano de Segurança Cibernética (ACSC) **Essential Eight** Modelo de Maturidade.

Veja [Seção 5.5, "Segurança"](#) para mais informações.

Linguagens de programação dinâmica, servidores web e de banco de dados

Versões posteriores dos seguintes componentes estão agora disponíveis como novos fluxos de módulos:

- **Python 3.8**
- **Maven 3.6**

Veja [Seção 5.10, "Linguagens de programação dinâmica, servidores web e de banco de dados"](#) para detalhes.

Conjuntos de ferramentas de compilação

Os seguintes conjuntos de ferramentas de compilação foram atualizados no RHEL 8.2:

- **GCC Toolset 9**
- **Clang and LLVM Toolset 9.0.1**
- **Rust Toolset 1.41**
- **Go Toolset 1.13**

Veja [Seção 5.11, "Compiladores e ferramentas de desenvolvimento"](#) para mais informações.

Gestão da Identidade

O Gerenciamento da Identidade introduz uma nova ferramenta de linha de comando **Healthcheck**. **Healthcheck** ajuda os usuários a encontrar problemas que possam impactar a adequação de seus ambientes IdM.

O Gerenciamento de Identidade agora suporta funções e módulos possíveis para instalação e gerenciamento. Esta atualização facilita a instalação e configuração de soluções baseadas em IdM.

Veja [Seção 5.12, “Gestão da Identidade”](#) para mais informações.

O console web

O console web foi redesenhado para usar o projeto do sistema de interface com o usuário PatternFly 4.

Um timeout de sessão foi adicionado ao console web para melhorar a segurança.

Veja [Seção 5.15, “O console web”](#) para mais informações.

Desktop

O computador de espaço de trabalho no ambiente GNOME Classic foi modificado. O switcher agora está localizado na parte direita da barra inferior, e foi projetado como uma faixa horizontal de miniaturas. A comutação entre espaços de trabalho é possível clicando na miniatura necessária.

O subsistema gráfico do kernel **Direct Rendering Manager** (DRM) foi rebaseado para a versão 5.3 do kernel Linux upstream. Esta versão oferece uma série de melhorias em relação à versão anterior, incluindo suporte para novas GPUs e APUs, e várias atualizações de drivers.

Atualização in loco

In-place upgrade from RHEL 7 to RHEL 8

O caminho de atualização suportado no local é:

- Da RHEL 7.9 à RHEL 8.2 sobre as arquiteturas 64-bit Intel, IBM POWER 8 (little endian), e IBM Z
- De RHEL 7.6 a RHEL 8.2 em arquiteturas que requerem kernel versão 4.14: 64-bit ARM, IBM POWER 9 (little endian), e IBM Z (Estrutura A). Note que estas arquiteturas permanecem totalmente suportadas no RHEL 7, mas não recebem mais pequenas atualizações de versão desde o RHEL 7.7.

Para mais informações, consulte [Caminhos de atualização suportados no local para o Red Hat Enterprise Linux](#). Para instruções sobre como realizar um upgrade no local, consulte [Atualização de RHEL 7 para RHEL 8](#).

As melhorias notáveis incluem:

- Agora você pode usar repositórios personalizados adicionais para um upgrade no local de RHEL 7 para RHEL 8. Também é possível fazer o upgrade sem o Red Hat Subscription Manager.
- Você pode criar seus próprios atores para migrar suas aplicações personalizadas ou de terceiros usando o utilitário Leapp.

Para maiores detalhes, veja [Customizing de seu Red Hat Enterprise Linux inplace upgrade](#) .

Se você estiver usando CentOS 7 ou Oracle Linux 7, você pode converter seu sistema operacional para o RHEL 7 usando o utilitário **convert2rhel** antes de atualizar para o RHEL 8. Para instruções, veja [Como converter do CentOS ou Oracle Linux para RHEL](#).

In-place upgrade from RHEL 6 to RHEL 8

Para atualizar da RHEL 6.10 para a RHEL 8.2, siga as instruções em [Upgrading from RHEL 6 to RHEL 8](#) .

Se você estiver usando CentOS 6 ou Oracle Linux 6, você pode converter seu sistema operacional para o RHEL 6 usando o utilitário **convert2rhel** antes de atualizar para o RHEL 8. Para instruções, veja [Como converter do CentOS ou Oracle Linux para o RHEL](#).

Recursos adicionais

- **Capabilities and limits** do Red Hat Enterprise Linux 8 em comparação com outras versões do sistema estão disponíveis no artigo da Base de Conhecimento [Capacidades e limites da tecnologia Red Hat Enterprise Linux](#).
- Informações sobre o Red Hat Enterprise Linux **life cycle** são fornecidas no documento [Red Hat Enterprise Linux Life Cycle \(Ciclo de Vida do Red Hat Enterprise Linux\)](#).
- O documento de [manifesto do Pacote](#) fornece um **package listing** para a RHEL 8.
- A maior parte **differences between RHEL 7 and RHEL 8** está documentada em [Considerações sobre a adoção do RHEL 8](#).
- As instruções sobre como realizar um **in-place upgrade from RHEL 7 to RHEL 8** são fornecidas pelo documento [Upgrading to RHEL 8](#).
- O serviço **Red Hat Insights**, que lhe permite identificar, examinar e resolver proativamente questões técnicas conhecidas, está agora disponível com todas as assinaturas RHEL. Para instruções sobre como instalar o cliente Red Hat Insights e registrar seu sistema no serviço, consulte a página [Red Hat Insights Get Started](#).

Laboratórios do Portal do Cliente Red Hat

Red Hat Customer Portal Labs é um conjunto de ferramentas em uma seção do Portal do Cliente disponível em <https://access.redhat.com/labs/>. As aplicações nos laboratórios do Portal do Cliente da Red Hat podem ajudar a melhorar o desempenho, solucionar rapidamente problemas, identificar problemas de segurança e implementar e configurar rapidamente aplicações complexas. Algumas das aplicações mais populares são:

- [Assistente de Registro](#)
- [Verificador do ciclo de vida do produto](#)
- [Gerador de pontapé de saída](#)
- [Conversor Kickstart](#)
- [Red Hat Satellite Upgrade Helper](#)
- [Navegador de Código Red Hat](#)
- [Ferramenta de configuração das opções JVM](#)
- [Checador de CVE Red Hat](#)
- [Certificados de Produto Red Hat](#)
- [Ferramenta de Configuração do Balanceador de Carga](#)
- [Ajudante de configuração do Yum Repository](#)

CAPÍTULO 2. ARQUITETURAS

O Red Hat Enterprise Linux 8.2 é distribuído com o kernel versão 4.18.0-193, que fornece suporte para as seguintes arquiteturas:

- Arquiteturas AMD e Intel de 64 bits
- A arquitetura ARM de 64 bits
- IBM Power Systems, Little Endian
- IBM Z

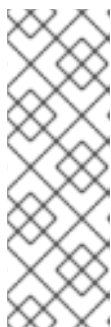
Certifique-se de adquirir a assinatura apropriada para cada arquitetura. Para mais informações, veja [Get Started with Red Hat Enterprise Linux - arquiteturas adicionais](#). Para uma lista de assinaturas disponíveis, consulte [Utilização de Assinaturas](#) no Portal do Cliente.

CAPÍTULO 3. DISTRIBUIÇÃO DO CONTEÚDO NO RHEL 8

3.1. INSTALAÇÃO

O Red Hat Enterprise Linux 8 é instalado usando imagens ISO. Dois tipos de imagem ISO estão disponíveis para as arquiteturas AMD64, Intel 64-bit, 64-bit ARM, IBM Power Systems e IBM Z:

- DVD binário ISO: Uma imagem de instalação completa que contém os repositórios BaseOS e AppStream e permite que você complete a instalação sem repositórios adicionais.



NOTA

A imagem ISO do DVD Binário é maior que 4,7 GB, e como resultado, pode não caber em um DVD de uma única camada. Um DVD de camada dupla ou uma chave USB é recomendado quando se usa a imagem ISO do DVD Binário para criar uma mídia de instalação inicializável. Você também pode usar a ferramenta Image Builder para criar imagens RHEL personalizadas. Para mais informações sobre o Image Builder, consulte a [Composing a customized RHEL system image](#) documento.

- ISO de inicialização: Uma imagem ISO mínima de inicialização que é usada para iniciar no programa de instalação. Esta opção requer acesso aos repositórios BaseOS e AppStream para instalar os pacotes de software. Os repositórios são parte da imagem ISO do DVD Binário.

Consulte o documento [Executando uma instalação padrão da RHEL](#) para obter instruções sobre como baixar imagens ISO, criar mídia de instalação e concluir uma instalação RHEL. Para instalações Kickstart automatizadas e outros tópicos avançados, veja o documento [Executando uma instalação RHEL avançada](#).

3.2. REPOSITÓRIOS

O Red Hat Enterprise Linux 8 é distribuído através de dois repositórios principais:

- BaseOS
- AppStream

Ambos os repositórios são necessários para uma instalação básica da RHEL, e estão disponíveis com todas as assinaturas RHEL.

O conteúdo no repositório BaseOS destina-se a fornecer o conjunto central da funcionalidade do SO subjacente que fornece a base para todas as instalações. Este conteúdo está disponível no formato RPM e está sujeito a termos de suporte semelhantes aos de versões anteriores da RHEL. Para uma lista de pacotes distribuídos através do BaseOS, veja o [manifesto de pacotes](#).

O conteúdo no repositório Application Stream inclui aplicações adicionais de espaço do usuário, linguagens de tempo de execução e bancos de dados em apoio às diversas cargas de trabalho e casos de uso. Os fluxos de aplicações estão disponíveis no familiar formato RPM, como uma extensão do formato RPM chamado *modules*, ou como Coleções de Software. Para uma lista de pacotes disponíveis no AppStream, veja o [manifesto de pacotes](#).

Além disso, o repositório CodeReady Linux Builder está disponível com todas as assinaturas RHEL. Ele fornece pacotes adicionais para uso dos desenvolvedores. Os pacotes incluídos no repositório do CodeReady Linux Builder não são suportados.

Para mais informações sobre os repositórios RHEL 8, consulte o [manifesto do pacote](#).

3.3. FLUXOS DE APLICAÇÃO

O Red Hat Enterprise Linux 8 introduz o conceito de Fluxos de Aplicação. Múltiplas versões de componentes de espaço do usuário são agora entregues e atualizadas com mais frequência do que os pacotes do sistema operacional principal. Isto proporciona maior flexibilidade para personalizar o Red Hat Enterprise Linux sem impactar a estabilidade subjacente da plataforma ou implementações específicas.

Os componentes disponibilizados como Application Streams podem ser empacotados como módulos ou pacotes RPM e são entregues através do repositório AppStream no RHEL 8. Cada componente do Application Stream tem um determinado ciclo de vida, seja o mesmo que o RHEL 8 ou menor. Para detalhes, veja o [Ciclo de Vida do Red Hat Enterprise Linux](#) .

Os módulos são coleções de pacotes que representam uma unidade lógica: uma aplicação, uma pilha de idiomas, um banco de dados ou um conjunto de ferramentas. Estes pacotes são construídos, testados e lançados juntos.

Os fluxos de módulos representam versões dos componentes do Application Stream. Por exemplo, dois fluxos (versões) do servidor de banco de dados PostgreSQL estão disponíveis no módulo postgresql: PostgreSQL 10 (o fluxo padrão) e PostgreSQL 9.6. Apenas um fluxo de módulo pode ser instalado no sistema. Versões diferentes podem ser utilizadas em containers separados.

Os comandos detalhados do módulo são descritos no documento [Instalar, gerenciar e remover componentes de espaço do usuário](#). Para uma lista de módulos disponíveis no AppStream, veja o [manifesto de pacotes](#).

CAPÍTULO 4. LANÇAMENTO RHEL 8.2.1

A Red Hat torna o conteúdo do Red Hat Enterprise Linux 8 disponível trimestralmente, entre versões menores (8.Y). As versões trimestrais são numeradas usando o terceiro dígito (8.Y.1). Os novos recursos no lançamento RHEL 8.2.1 são descritos abaixo.

4.1. NOVAS CARACTERÍSTICAS

JDK Mission Control rebaseado para a versão 7.1.1

O JDK Mission Control (JMC) para JVMs HotSpot, fornecido pelo fluxo de módulos **jmc:rhel8**, foi atualizado para a versão 7.1.1 com o lançamento RHEL 8.2.1.

Esta atualização inclui numerosas correções e melhorias de bugs, inclusive:

- Otimizações de múltiplas regras
- Uma nova visualização JOverflow baseada no Standard Widget Toolkit (SWT)
- Uma nova visualização gráfica da chama
- Uma nova forma de visualização da latência usando o Histograma de Alta Gama Dinâmica (HDR)

O módulo **jmc:rhel8** tem dois perfis:

- O perfil **comum**, que instala toda a aplicação JMC
- O perfil **central**, que instala apenas as bibliotecas centrais Java (**jmc-core**)

Para instalar o perfil **comum** do fluxo do módulo **jmc:rhel8**, use:

```
#mc:rhel8/módulo yum instalar jmc:rhel8/comum
```

Mude o nome do perfil para **core** para instalar apenas o pacote **jmc-core**.

(BZ#1792519)

Rust Toolset rebaseado para a versão 1.43

O Rust Toolset foi atualizado para a versão 1.43. As mudanças notáveis incluem:

- Os números de linhas úteis estão agora incluídos nas mensagens de pânico de **Opção** e **Resultado** onde foram invocados.
- Suporte ampliado para a correspondência de padrões de subslice.
- A macro **fósforos!** fornece uma combinação de padrões que retorna um valor booleano.
- os fragmentos **do item** podem ser interpolados em traços, impls e blocos externos.
- Inferência de tipo melhorada em torno dos primitivos.
- Constantes associadas para flutuadores e inteiros.

Para instalar o módulo Rust Toolset, execute o seguinte comando como **raiz**:

■

módulo yum instalar ferrugem

Para informações sobre o uso, consulte a documentação [Using Rust Toolset](#).

(BZ#1811997)

Os registros de contêineres agora suportam o comando **skopeo sync**

Com este aperfeiçoamento, os usuários podem usar o comando **skopeo sync** para sincronizar os registros de contêineres e os registros locais. O comando de **sincronização skopeo** é útil para sincronizar um espelho de registro de contêineres local, e para preencher registros em execução dentro de ambientes com ar comprimido.

O comando **skopeo sync** requer que os transportes de origem (**--src**) e de destino (**--dst**) sejam especificados separadamente. Os transportes de origem e destino disponíveis são **docker** (repositório hospedado em um registro de containers) e **dir** (diretório em um caminho de diretório local). Os transportes de origem também incluem o **yaml** (caminho de arquivo local YAML). Para informações sobre o uso do **skopeo sync**, consulte a página de manual **skopeo-sync**.

(BZ#1811779)

O arquivo de configuração **container.conf** já está disponível

Com este aperfeiçoamento, usuários e administradores podem especificar opções de configuração padrão e bandeiras de linha de comando para motores de contêineres. Os motores de contêineres lêem os arquivos **/usr/share/containers/containers.conf** e **/etc/containers/containers.conf**, se eles existirem. No modo sem raiz, os motores de contêineres lêem os arquivos **\$HOME/.config/containers/containers.conf**.

Os campos especificados no arquivo **containers.conf** substituem as opções padrão, assim como as opções em arquivos **containers.conf** lidos anteriormente. O arquivo **container.conf** é compartilhado entre Podman e Buildah e substitui o arquivo **libpod.conf**.

(BZ#11826486)

Agora você pode entrar e sair de um servidor de registro

Com este aperfeiçoamento, você pode entrar e sair de um servidor de registro especificado usando os comandos de **login** e **logout** do **skopeo**. O comando de **login do skopeo** lê no nome de usuário e na senha a partir da entrada padrão. O nome de usuário e a senha também podem ser definidos usando as opções **--username** (ou **-u**) e **--password** (ou **-p**).

Você pode especificar o caminho do arquivo de autenticação, definindo a bandeira **--authfile**. O caminho padrão é **\${XDG_RUNTIME_DIR}/containers/auth.json**. Para informações sobre o uso do **login** e **logout** do **skopeo**, veja as páginas man **skopeo-login** e **skopeo-logout**, respectivamente.

(JIRA:RHELPLAN-47311)

Agora você pode reiniciar o armazenamento do podman

Com este aprimoramento, os usuários podem usar o comando de **reset do sistema podman** para repor o armazenamento do **podman** de volta ao estado inicial. O comando de **reinicialização do sistema podman** remove todos os pods, containers, imagens e volumes. Para mais informações, consulte a página de manual de **reinicialização do sistema podman**.

(JIRA:RHELPLAN-48941)

CAPÍTULO 5. NOVAS CARACTERÍSTICAS

Esta parte descreve as novas características e principais melhorias introduzidas no Red Hat Enterprise Linux 8.2.

5.1. INSTALADOR E CRIAÇÃO DE IMAGEM

Capacidade de registrar seu sistema, anexar assinaturas RHEL, e instalar a partir do Red Hat CDN

No RHEL 8.2, você pode registrar seu sistema, anexar assinaturas RHEL e instalar a partir da Red Hat Content Delivery Network (CDN) antes da instalação do pacote. Instalações interativas GUI, bem como instalações Kickstart automatizadas, suportam este recurso. Os benefícios incluem:

- O uso do arquivo de imagem ISO de Boot menor elimina a necessidade de baixar o arquivo de imagem ISO de DVD binário maior.
- O CDN utiliza os últimos pacotes que resultam em um sistema totalmente subscrito e atualizado imediatamente após a instalação. Não há necessidade de instalar atualizações de pacotes após a instalação.
- O registro é realizado antes da instalação da embalagem, resultando em um processo de instalação mais curto e mais ágil.
- Está disponível suporte integrado para o Red Hat Insights.

(BZ#1748281)

Capacidade de registrar seu sistema na Red Hat Insights durante a instalação

No RHEL 8.2, você pode registrar seu sistema no Red Hat Insights durante a instalação. Instalações interativas GUI, bem como instalações Kickstart automatizadas, suportam este recurso.

Os benefícios incluem:

- Mais fácil de identificar, priorizar e resolver problemas antes que as operações comerciais sejam afetadas.
- Identificar e remediar proativamente as ameaças à segurança, desempenho, disponibilidade e estabilidade com uma análise preditiva.
- Evite problemas e tempos de inatividade não planejados em seu ambiente.

(BZ#1746391)

O Image Builder oferece agora suporte de nuvens para a criação de imagens Azure

Com este aprimoramento, o suporte de nuvens está disponível para as imagens Azure criadas pelo Image Builder. Como resultado, a criação de imagens on-premise com rápido fornecimento e a capacidade de adicionar dados personalizados está disponível aos clientes.

(BZ#1754711)

5.2. GESTÃO DE SOFTWARE

A seqüência de cabeçalho do **Agente-usuário** agora inclui informações lidas do arquivo **/etc/os-release**

Com este aperfeiçoamento, a cadeia de cabeçalho **User-Agent**, que normalmente é incluída nas solicitações HTTP feitas pelo DNF, foi ampliada com informações lidas no arquivo **/etc/os-release**.

Para obter mais informações, veja **user_agent** na página man do **dnf.conf(5)**.

(BZ#1676891)

Todas as unidades **dnf-automatic.timer** agora usam o relógio em tempo real por padrão

Anteriormente, as unidades temporizadas **dnf-automatic.timer** utilizavam o relógio monotônico, o que resultava em um tempo de ativação imprevisível após a inicialização do sistema. Com esta atualização, as unidades temporizadas funcionam entre 6h e 7h. Se o sistema estiver desligado durante este tempo, as unidades temporizadas são ativadas dentro de uma hora após a inicialização do sistema.

(BZ#1754609)

O utilitário **createrepo_c** agora salta pacotes cujos metadados contêm os caracteres de controle não permitidos

Para garantir um XML válido, os metadados do pacote não devem conter nenhum caractere de controle, com exceção de:

- a aba horizontal
- o novo personagem da linha
- o caráter de retorno do carro

Com esta atualização, o utilitário **createrepo_c** não inclui pacotes com metadados contendo caracteres de controle não permitidos em um repositório recém-criado, e retorna a seguinte mensagem de erro:

```
C_CREATEREPOLIB: Crítico: Não é possível despejar XML para PACKAGE_NAME
(PACKAGE_SUM): Cartas de controle proibidas encontradas (valores ASCII
```

(BZ#1743186)

5.3. CONCHAS E FERRAMENTAS DE LINHA DE COMANDO

opencv rebaseado para a versão 3.4.6

Os pacotes **opencv** foram atualizados para a versão upstream 3.4.6. Mudanças notáveis incluem:

- Suporte para novos parâmetros Open CL, tais como **OPENCV_OPENCL_BUILD_EXTRA_OPTIONS** e **OPENCV_OPENCL_DEVICE_MAX_WORK_GROUP_SIZE**.
- O módulo **objdetect** agora suporta o algoritmo de detecção de código QR.
- Vários métodos novos, tais como **MatSize::dims** ou **VideoCapture::getBackendName**.
- Múltiplas novas funções, tais como **drawFrameAxes** ou **getVersionMajor**.
- Várias melhorias de desempenho, incluindo melhorias da função **GaussianBlur**, **v_load_deinterleave** e **v_store_interleave** intrínsecas ao usar as instruções SSE3.

[\(BZ#1694647\)](#)

5.4. SERVIÇOS DE INFRA-ESTRUTURA

graphviz-python3 é agora distribuído no repositório CRB

Esta atualização adiciona o pacote **graphviz-python3** ao RHEL 8. O pacote fornece os bindings necessários para o uso do software de visualização gráfica Graphviz da Python.

Note que o pacote **graphviz-python3** é distribuído no [repositório](#) não suportado [CodeReady Linux Builder \(CRB\)](#).

[\(BZ#1704875\)](#)

sintonizado rebaseado para a versão 2.13.0

Os pacotes **ajustados** foram atualizados para a versão upstream 2.13.0. Melhorias notáveis incluem:

- Foi adicionada uma estrutura de ajuste dependente da arquitetura.
- Foi adicionado suporte para múltiplas diretrizes de inclusão.
- O ajuste dos perfis de **seiva**, de **latência** e de **desempenho em tempo real** foi atualizado.

[\(BZ#1738250\)](#)

powertop rebaseado para a versão 2.11

O pacote **powertop** foi atualizado para a versão 2.11, o que proporciona uma mudança notável a seguir:

- Suporte para as plataformas EHL, TGL, ICL/ICX

[\(BZ#1716721\)](#)

BIND agora suporta **.GeoIP2** ao invés de **GeoLite Legacy GeoIP**

A biblioteca do GeoLite Legacy GeoIP não é mais suportada no BIND. Com esta atualização, o GeoLite Legacy GeoP foi substituído pelo GeoIP2, que é fornecido no formato de dados **libmaxminddb**.

Note que o novo formato pode exigir algumas mudanças de configuração, e o formato também não suporta as configurações da lista de controle de acesso GeoIP (ACL) herdada:

- velocidade das redes geoip
- geoip org
- Códigos de países ISO 3166 Alpha-3

[\(BZ#1564443\)](#)

stale-answer agora fornece antigos registros em cache em caso de ataque DDoS

Anteriormente, o ataque de Negação de Serviço Distribuído (DDoS) causou a falha dos servidores autorizados com o erro SERVFAIL. Com esta atualização, a funcionalidade de **stale-answer** fornece os registros expirados até que uma nova resposta seja obtida.

Para habilitar ou desabilitar a função **servir-estação**, use qualquer uma destas:

- Arquivo de configuração
- Canal de controle remoto (rndc)

(BZ#1664863)

BIND rebaseado para a versão 9.11.13

Os pacotes **de encadernação** foram atualizados para a versão 9.11.13. Mudanças notáveis incluem:

- A variável estatística **tcp-highwater** statistics foi adicionada. Esta variável mostra o máximo de clientes TCP simultâneos registrados durante uma execução.
- Foi adicionado o algoritmo **SipHash-2-4 baseado em Cookies DNS** (RFC 7873).
- Endereços de cola para consultas de enraizamento são devolvidos independentemente de como a opção de configuração de **mínimo de respostas** é definida.
- O comando **checkconf nomeado** garante agora a validade dos prefixos da rede **DNS64**.
- A rolagem automática por RFC 5011 não falha mais quando as declarações de **chaves fiduciárias** e **chaves administradas** estão ambas configuradas para o mesmo nome. Ao invés disso, uma mensagem de aviso é registrada.
- O processamento de nomes de domínio internacionalizados (IDN) nos utilitários de **escavação** e **nslookup** está agora desabilitado por padrão quando não são executados em terminal (por exemplo, em um script). O processamento de IDN na **escavação** pode ser ligado usando as opções **idnin** e **idnout**.

(BZ#1704328)

5.5. SEGURANÇA

RHEL 8 contém agora o perfil DISA STIG

Os Guias de Implementação Técnica de Segurança (STIG) são um conjunto de recomendações de base publicadas pela Agência de Sistemas de Informação de Defesa (DISA) para reforçar a segurança dos sistemas de informação e software que, de outra forma, poderiam ser vulneráveis. Esta versão inclui o perfil e o arquivo Kickstart para esta política de segurança. Com esta melhoria, os usuários podem verificar a conformidade dos sistemas, corrigir os sistemas para que estejam em conformidade e instalar sistemas em conformidade com o DISA STIG para o Red Hat Enterprise Linux 8.

(BZ#1755447)

as políticas criptográficas podem agora ser personalizadas

Com esta atualização, você pode ajustar certos algoritmos ou protocolos de qualquer nível de política ou definir um novo arquivo de política completo como a política criptográfica atual de todo o sistema. Isto permite aos administradores personalizar a política criptográfica de todo o sistema, conforme exigido por diferentes cenários.

Os pacotes RPM devem armazenar as políticas fornecidas por eles no diretório **/usr/share/crypto-policies/policies**. O diretório **/etc/crypto-policies/policies** contém políticas personalizadas locais.

Para mais informações, consulte a seção **Políticas Personalizadas** na página de manual **update-crypto-policies(8)** e a seção **Formato de Definição de Políticas Crypto** na página de manual **update-crypto-policies(8)**.

(BZ#1690565)

Guia de Segurança SCAP agora suporta ACSC Essential Eight

Os pacotes **scap-security-guide** fornecem agora o perfil de conformidade Essential Cyber Security Centre (ACSC) da Austrália e um arquivo Kickstart correspondente. Com esta melhoria, os usuários podem instalar um sistema que esteja em conformidade com esta linha de base de segurança. Além disso, é possível usar a suíte **OpenSCAP** para verificar a conformidade e correção de segurança usando esta especificação de controles mínimos de segurança definidos pelo ACSC.

(BZ#1755194)

oscap-podman para segurança e verificação de conformidade de containers está agora disponível

Esta atualização dos pacotes **openscap** introduz uma nova utilidade para segurança e verificação de conformidade de contêineres. A ferramenta **oscap-podman** fornece um equivalente do utilitário **oscap-docker** que serve para escanear imagens de contêineres e contêineres no RHEL 7.

(BZ#1642373)

asolução de problemas pode agora analisar e reagir às negações de acesso de execmem

Esta atualização introduz um novo **setroubleshoot** plugin. O plugin pode analisar as negações de acesso **execmem** (AVCs) e fornecer conselhos relevantes. Como resultado, o **setroubleshoot** pode agora sugerir a possibilidade de trocar um booleano se ele permitir o acesso, ou relatar o problema quando nenhum booleano puder permitir o acesso.

(BZ#1649842)

Novos pacotes: setools-gui e setools-console-análises

O pacote **setools-gui**, que fez parte do RHEL 7, está agora sendo apresentado ao RHEL 8. Ferramentas gráficas ajudam a inspecionar relações e fluxos de dados, especialmente em sistemas multiníveis com políticas SELinux altamente especializadas. Com a ferramenta gráfica **apol** do pacote **setools-gui**, você pode inspecionar e analisar aspectos de uma política SELinux. As ferramentas do pacote **setools-console-analyses** permitem analisar as transições de domínio e os fluxos de informações sobre políticas SELinux.

(BZ#1731519)

Usuários confinados no SELinux podem agora gerenciar os serviços de sessão do usuário

Anteriormente, os usuários confinados não eram capazes de gerenciar os serviços de sessão do usuário. Como resultado, eles não podiam executar comandos de **usuário do systemctl --usuário** ou **busctl --** ou trabalhar no console web RHEL. Com esta atualização, os usuários confinados podem gerenciar as sessões de usuários.

(BZ#1727887)

O serviço lvmdbusd está agora confinado pela SELinux

O serviço **lvmdbusd** fornece um D-Bus API para o gerenciador de volume lógico (LVM). Anteriormente, o daemon **lvmdbusd** não podia fazer a transição para o contexto **lvm_t**, embora a política SELinux para o **lvm_t** estivesse definida. Como consequência, o daemon **lvmdbusd** era executado no domínio **lvmdbusd não-confinado_t** e o SELinux rotulado **lvmdbusd** como não-confinado. Com esta atualização, o arquivo executável **do lvmdbusd** tem o contexto **lvm_exec_t** definido e o **lvmdbusd** pode agora ser usado corretamente com o SELinux no modo de execução.

(BZ#1726166)

semanage agora suporta a listagem e modificação de portas SCTP e DCCP.

Anteriormente, as **portas semanais** permitiam a listagem e modificação apenas das portas TCP e UDP. Esta atualização adiciona suporte ao protocolo SCTP e DCCP à **porta semmanage**. Como resultado, os administradores podem agora verificar se duas máquinas podem se comunicar via SCTP e habilitar totalmente os recursos do SCTP para implementar com sucesso aplicações baseadas no SCTP.

(BZ#1563742)

aexportação semanal mostra agora customizações relacionadas a domínios permissivos

Com esta atualização, o utilitário **semanário**, que faz parte do pacote de **policoreutils** para SELinux, é capaz de exibir personalizações relacionadas a domínios permissivos. Os administradores do sistema podem agora transferir modificações locais permissivas entre máquinas usando o comando de **exportação semmanage**.

(BZ#1417455)

udica pode adicionar novas regras de permissão geradas a partir de recusas da SELinux à política de contêineres existente

Quando um contêiner que está funcionando sob uma política gerada pelo utilitário **udica** aciona uma negação da SELinux, **a udica** agora é capaz de atualizar a política. O novo parâmetro **-a** ou **--as regras abertas-** pode ser usado para anexar regras de um arquivo AVC.

(BZ#1732704)

Os novos tipos de SELinux permitem que os serviços funcionem confinados

Esta atualização introduz novos tipos de SELinux que permitem que os seguintes serviços sejam executados como serviços confinados no modo de aplicação do SELinux, em vez de serem executados no domínio **não-confinado_service_t**:

- **lldpd** agora funciona como **lldpad_t**
- **rrdcached** agora funciona como **rrdcached_t**
- **stratisd** agora funciona como **stratisd_t**
- **timedatex** agora funciona como **timedatex_t**

(BZ#1726246, BZ#1726255, BZ#1726259, BZ#1730204)

Clevis é capaz de listar as políticas em vigor para um determinado dispositivo LUKS

Com esta atualização, o comando **clevis luks luks** lista as políticas PBD em vigor para um determinado dispositivo LUKS. Isto facilita encontrar informações sobre os pinos Clevis em uso e a configuração dos pinos, por exemplo, endereços de servidores Tang, detalhes sobre políticas **tpm2** e limites SSS.

(BZ#1766526)

Clevis fornece novos comandos para informar o status da chave e rebobinar chaves vencidas

O comando **clevis luks report** agora fornece uma maneira simples de informar se as chaves para uma determinada ligação requerem rotação. Rotações regulares de chaves em um servidor Tang melhoram a segurança das implementações de Criptografia de Disco Ligado à Rede (NBDE) e, portanto, o cliente

deve fornecer a detecção de chaves expiradas. Se a chave estiver expirada, Clevis sugere o uso do comando **clevis luks regen** que religa o slot da chave expirada com uma chave atual. Isto simplifica significativamente o processo de rotação da chave.

(BZ#1564559, BZ#1564566)

Clevis pode agora extrair a frase-senha utilizada para encadernar um determinado slot em um dispositivo LUKS

Com esta atualização da estrutura de decriptação baseada na política Clevis, você pode agora extrair a senha usada para encadernar um determinado slot em um dispositivo LUKS. Anteriormente, se a senha de instalação do LUKS fosse apagada, Clevis não poderia realizar tarefas administrativas do LUKS, tais como recriptação, permitindo um novo slot chave com uma senha de usuário, e religando Clevis quando o administrador precisar alterar o limiar **sss**. Esta atualização introduz o comando **clevis luks pass** que mostra a frase-chave usada para encadernar um determinado slot.

(BZ#1436780)

Clevis agora fornece melhor suporte para decodificação de múltiplos dispositivos LUKS na inicialização

Os pacotes **clevis** foram atualizados para fornecer melhor suporte à decriptação de múltiplos dispositivos criptografados LUKS na inicialização. Antes desta melhoria, o administrador teve que realizar alterações complicadas na configuração do sistema para permitir a decriptação adequada de múltiplos dispositivos pela Clevis no momento da inicialização. Com este lançamento, você pode configurar a decriptação usando o comando **clevis luks bind** e atualizando o initramfs através do comando **dracut -fv --regenerate-all**.

Para mais detalhes, consulte a seção [Configurando o desbloqueio automatizado de volumes criptografados utilizando a decodificação baseada em políticas](#).

(BZ#1784524)

openssl-pkcs11 rebaseado para 0,4,10

O pacote **openssl-pkcs11** foi atualizado para a versão 0.4.10, que fornece muitas correções de bugs e melhorias em relação à versão anterior. O pacote **openssl-pkcs11** fornece acesso aos módulos PKCS #11 através da interface do motor. As principais mudanças introduzidas pela nova versão são:

- Se um objeto de chave pública correspondente à chave privada não estiver disponível ao carregar uma chave privada ECDSA, o motor carrega a chave pública a partir de um certificado correspondente, se presente.
- Você pode usar URI genérico PKCS #11 (por exemplo **pkcs11:type=public**) porque o motor **openssl-pkcs11** procura todos os tokens que correspondem a um determinado URI PKCS #11.
- O sistema tenta entrar com um PIN somente se um único dispositivo corresponder à busca URI. Isto evita falhas de autenticação devido ao fornecimento do PIN a todos os tokens correspondentes.
- Ao acessar um dispositivo, o motor **openssl-pkcs11** agora marca a estrutura dos métodos RSA com a bandeira **RSA_FLAG_FIPS_METHOD**. No modo FIPS, OpenSSL exige que a bandeira seja definida na estrutura dos métodos RSA. Observe que o motor não pode detectar se um dispositivo é certificado por FIPS.

(BZ#1745082)

rsyslog rebaseado para 8.1911.0

O utilitário **rsyslog** foi atualizado para a versão upstream 8.1911.0, que fornece uma série de correções de bugs e melhorias em relação à versão anterior. A lista a seguir inclui melhorias notáveis:

- O novo módulo **omhttp** permite que você envie mensagens através da interface HTTP REST.
- O módulo de entrada de arquivo é aprimorado para melhorar a estabilidade, relatório de erros e detecção de truncagem.
- Novo parâmetro **Action.resumelIntervalMax** que pode ser usado com qualquer ação permite limitar o crescimento do intervalo de reentrada a um valor especificado.
- Nova opção **StreamDriver.PermitExpiredCerts** para TLS permite conexões mesmo que um certificado tenha expirado.
- Agora você pode suspender e retomar a saída com base no conteúdo do arquivo externo configurado. Isto é útil nos casos em que a outra extremidade sempre aceita mensagens e as deixa cair silenciosamente quando não é capaz de processá-las todas.
- O relatório de erros para o módulo de saída do arquivo foi melhorado e agora contém nomes de arquivos reais e mais informações sobre as causas dos erros.
- As filas de discos agora rodam com várias filas, o que melhora o desempenho.
- Você pode definir modos de operação TLS mais rígidos: verificação do campo de certificado **estendido doKeyUsage** e verificação mais rígida dos campos de certificado **CN/SAN**.

(BZ#1740683)

rsyslog agora fornece o plugin **omhttp** para comunicação através de uma interface HTTP REST

Com esta atualização dos pacotes **rsyslog**, você pode usar o novo plugin **omhttp** para produzir uma saída compatível com serviços usando uma API Representational State Transfer (REST), como a plataforma de armazenamento Ceph, Amazon Simple Storage Service (Amazon S3), e Grafana Loki. Este novo módulo de saída HTTP fornece um caminho REST configurável e formato de mensagem, suporte a vários formatos de lotes, compressão e criptografia TLS.

Para mais detalhes, consulte o arquivo

/usr/share/doc/rsyslog/html/configuration/modules/omhttp.html instalado em seu sistema com o pacote **rsyslog-doc**.

(BZ#1676559)

omelasticsearch no **rsyslog** agora suporta **rebindinterval**

Esta atualização dos pacotes **rsyslog** introduz suporte para definir o tempo de reconexão periódica no módulo de **pesquisa omelástica**. Você pode melhorar o desempenho ao enviar registros para um cluster de nós de Elasticsearch definindo este parâmetro de acordo com seu cenário. O valor do parâmetro **rebindinterval** indica o número de operações submetidas a um nó após o qual **o rsyslog** fecha a conexão e estabelece uma nova. O valor padrão **-1** significa que **o rsyslog** não restabelece a conexão.

(BZ#1692073)

rsyslog mmkubernetes agora fornece o prazo de validade do cache de metadados

Com esta atualização dos pacotes **rsyslog**, você pode usar dois novos parâmetros para o módulo **mmkubernetes** para definir a expiração do cache de metadados. Isto assegura que objetos Kubernetes

apagados sejam removidos do cache estático **mmkubernetes**. O valor do parâmetro **cacheentryttl** indica a idade máxima das entradas de cache em segundos. O parâmetro **cacheexpireintervalo** tem os seguintes valores:

- **-1** para desativar as verificações de validade do cache
- **0** para permitir verificações de validade de cache
- maior que 0 para verificações regulares de validade de cache em segundos

[\(BZ#1692072\)](#)

auditoria rebaseada para a versão 3.0-0.14

Os pacotes de **auditoria** foram atualizados para a versão upstream 3.0-0.14, que fornece muitas correções e melhorias em relação à versão anterior, mais notadamente:

- Adicionada uma opção para interpretar os campos no plugin syslog
- Dividiu o arquivo **30-ospp-v42.rules** em arquivos mais granulares
- Mudou as regras de exemplo para o diretório **/usr/share/audit/sample-rules/**
- Auditoria fixa Modo de transporte KRB5 para registro remoto

[\(BZ#1757986\)](#)

A auditoria agora contém muitas melhorias do kernel v5.5-rc1

Esta adição ao kernel Linux contém a maioria das melhorias, correções de bugs e limpezas relacionadas ao subsistema de Auditoria e introduzidas entre a versão 4.18 e 5.5-rc1. A lista a seguir destaca mudanças importantes:

- Uso mais amplo do campo **exe** para filtragem
- Apoio às capacidades de nomes v3
- Melhorias para filtragem em sistemas de arquivos remotos
- Fixação da regra do filtro **gid**
- Consertos de um uso - após a corrupção e vazamentos de memória livres
- Melhorias na associação de registros de eventos
- Limpeza da interface **fanoticia**, opções de configuração de Auditoria e interface syscall
- Fixação do valor de retorno do Módulo de Verificação Estendida (EVM)
- Consertos e limpezas de vários formatos de registros
- Simplificações e correções da auditoria do Sistema de Arquivo Virtual (VFS)

[\(BZ#1716002\)](#)

fapolicyd rebaseado para 0,9,1-2

Os pacotes **fapolicyd** que fornecem a lista branca de aplicações RHEL foram atualizados para a versão 0.9.1-2. Correções de erros notáveis e melhorias incluem:

- A identificação do processo é fixa.
- A parte sujeita e a parte objeto estão agora posicionadas estritamente na regra. Ambas as partes são separadas por dois pontos e contêm a permissão necessária (executar, abrir, qualquer).
- O assunto e os atributos do objeto são consolidados.
- O novo formato de regras é o seguinte:

```
ASSUNTO DA PERMISSÃO DE DECISÃO : OBJETO
```

Por exemplo:

```
permitir perm=exe=/usr/bin/rpm : todos
```

(BZ#1759895)

sudo rebaseado para 1.8.29-3.el8

os pacotes **sudo** foram atualizados para a versão upstream 1.8.29-3, que fornece uma série de correções de bugs e melhorias em relação à versão anterior. As principais mudanças introduzidas pela nova versão são:

- **sudo** agora escreve mensagens do Módulo de Autenticação Plugável (PAM) no terminal do usuário, se disponível, ao invés da saída padrão ou saída de erro padrão. Isto evita possível confusão da saída do PAM e da saída do comando enviado para arquivos e pipes.
- As opções **notBefore** e **notAfter** do LDAP e SSSD agora funcionam e exibem corretamente com o comando **sudo -l**.
- O comando **cvtsudoers** agora rejeita a entrada de dados não-LDAP Data Interchange Format (LDIF) ao converter de LDIF para **sudoers** e formatos JSON.
- Com as novas configurações **log_allowed** e **log_denied** para **os processadores**, você pode desativar o registro e a auditoria dos comandos permitidos e negados.
- Agora você pode usar **sudo** com a opção **-g** para especificar um grupo que corresponda a qualquer grupo do usuário alvo, mesmo que nenhum grupo esteja presente na especificação **runas_spec**. Anteriormente, você só poderia fazê-lo se o grupo correspondesse ao grupo primário do usuário alvo.
- Corrigido um bug que impedia o **sudo** de combinar o nome do host com o valor do **ipa_hostname** do **sssd.conf**, se especificado.
- Uma vulnerabilidade que permitiu que um usuário **sudo** executasse um comando como root quando a especificação **Runas** proibia o acesso **root** com a palavra-chave **ALL** é agora corrigida (CVE-2019-14287).
- O uso de IDs de usuários e grupos desconhecidos para entradas de **substitutos** permissivos, por exemplo, usando a palavra-chave **ALL**, está agora desativado. Você pode habilitá-lo com a configuração **runas_allow_unknown_id** (CVE-2019-19232).

(BZ#1733961)

O módulo **pam_namespace** agora permite especificar opções adicionais de montagem para **tmpfs**

As opções de montagem **nosuid**, **noexec** e **noddev** podem agora ser usadas no arquivo de configuração **/etc/security/namespace.conf** para respectivamente desativar o efeito **setuid** bit, desativar os executáveis em execução e impedir que os arquivos sejam interpretados como caracteres ou dispositivos de bloqueio no sistema de arquivos **tmpfs** montados.

Opções adicionais de montagem são especificadas na página de manual **tmpfs(5)**.

(BZ#1252859)

pam_faillock agora pode ler os ajustes do arquivo de configuração **faillock.conf**

O módulo **pam_faillock**, parte dos módulos de autenticação plugáveis (PAM), agora pode ler as configurações do arquivo de configuração localizado em **/etc/security/faillock.conf**. Isto facilita a configuração de um bloqueio de conta nas falhas de autenticação, fornece perfis de usuário para esta funcionalidade e lida com diferentes configurações PAM simplesmente editando o arquivo **faillock.conf**.

(BZ#1537242)

5.6. TRABALHO EM REDE

As aplicações de espaço do usuário podem agora recuperar a identificação da rede selecionada pelo kernel

Aplicações de espaço do usuário podem solicitar ao kernel para selecionar um novo ID de **rede** e atribuí-lo a um espaço de nome de rede. Com este aperfeiçoamento, os usuários podem especificar a bandeira **NLM_F_ECHO** ao enviar uma mensagem **RTM_NETNSID netlink** para o kernel. O kernel então envia a mensagem **netlink** de volta para o usuário. Esta mensagem inclui o ID **netns** definido para o valor do kernel selecionado. Como resultado, as aplicações de espaço do usuário agora têm uma opção confiável para identificar o ID **netlink** do kernel selecionado.

(BZ#1763661)

firewalld rebaseado para a versão 0.8

Os pacotes **firewalld** foram atualizados para a versão 0.8. Mudanças notáveis incluem:

- Esta versão do **firewalld** inclui todas as correções de bugs desde a versão 0.7.0.
- **firewalld** agora usa a interface JSON **libnftables** para o subsistema **nftables**. Isto melhora o desempenho e a confiabilidade da aplicação de regras.
- Nas definições de serviço, o novo elemento de **ajuda** substitui o **módulo**.
- Esta versão permite que os helpers personalizados utilizem módulos de helper padrão.

(BZ#1740670)

a **ndptool** pode agora especificar um endereço de destino no cabeçalho IPv6

Com esta atualização, o utilitário **ndptool** pode enviar uma mensagem de Solicitação de Vizinhança (NS) ou um Anúncio de Vizinhança (NA) para um destino específico, especificando o endereço no cabeçalho IPv6. Como resultado, uma mensagem pode ser enviada para outros endereços que não apenas para o endereço local do link.

(BZ#1697595)

nftables agora suporta tipos de conjuntos IP multidimensionais

Com este aperfeiçoamento, a estrutura de filtragem de pacotes **nftables** suporta tipos definidos com concatenações e intervalos. Como resultado, os administradores não precisam mais de soluções para criar tipos de conjuntos IP multidimensionais.

(BZ#1593711)

nftables rebaseado para a versão 0.9.3

Os pacotes **nftables** foram atualizados para a versão 0.9.3, que fornece uma série de correções de bugs e melhorias em relação à versão anterior:

- Um JSON API foi adicionado à biblioteca de **libnftables**. Esta biblioteca fornece uma interface de alto nível para gerenciar conjuntos de regras de **nftables** a partir de aplicações de terceiros. Para usar a nova API em Python, instale o pacote **python3-nftables**.
- As declarações suportam prefixos e faixas IP, tais como **192.0.2.0/24** e **192.0.2.0-192.0.2.30**.
- O suporte para impressões digitais do sistema operacional foi adicionado para marcar os pacotes com base no sistema operacional adivinhado. Para mais detalhes, veja a seção de **expressão osf** na página **nft(8)** man.
- Foi adicionado suporte de proxy transparente para redirecionar os pacotes para um soquete local sem alterar de forma alguma o cabeçalho do pacote. Para detalhes, veja a seção de **declaração tproxy** na página **nft(8)** man.
- Por padrão, **nft** exibe os nomes textuais da prioridade definida durante a criação das cadeias nft. Para visualizar os valores numéricos de prioridade padrão, use a opção **-y**. Para detalhes, consulte a seção [Valores de prioridade padrão e nomes textuais](#).
- O suporte da marca de segurança foi adicionado.
- O suporte para atualizações de conjuntos dinâmicos foi melhorado para definir atualizações a partir do caminho do pacote.
- Foi adicionado o suporte para a correspondência da porta de cabeçalho de transporte.

Para maiores informações sobre mudanças notáveis, leia as notas de lançamento a montante antes de atualizar:

- <https://lore.kernel.org/netfilter-devel/20190624164910.defehs5giqziqnir@salvia/>
- <https://lore.kernel.org/netfilter-devel/20190819115807.myv6owxzblj2bthd@salvia/>
- <https://lore.kernel.org/netfilter-devel/20191202211737.xvmd6e6xxj4xvvl@salvia/>

(BZ#1643192)

As regras para o serviço firewalld podem agora usar ajudantes de rastreamento de conexão para serviços executados em um porto não-padrão

Os ajudantes definidos pelo usuário no serviço **firewalld** podem agora usar módulos de ajuda padrão do kernel. Isto permite que os administradores criem regras **firewalld** para usar helpers de rastreamento de conexão para serviços executados em uma porta não-standard.

([BZ#1733066](#))

O pacote **whois** já está disponível

Com este aperfeiçoamento, o pacote **whois** está agora disponível em RHEL 8.2.0. Como resultado, a recuperação de informações sobre um nome de domínio ou endereço IP específico é agora possível.

([BZ#1734183](#))

o **eBPF** para **tc** é agora totalmente suportado

O subsistema de Controle de Tráfego (**tc**) e a ferramenta **tc** podem anexar programas ampliados de Filtragem de Pacotes Berkeley (**eBPF**) como classificadores de pacotes e ações para ambas as disciplinas de entrada e saída em fila. Isto permite o processamento programável de pacotes dentro do caminho de dados da rede do kernel. O **eBPF** para **tc**, anteriormente disponível como uma previsão tecnológica, é agora totalmente suportado no RHEL 8.2.

([BZ#1755347](#))

5.7. KERNEL

Versão do Kernel em RHEL 8.2

O Red Hat Enterprise Linux 8.2 é distribuído com o kernel versão 4.18.0-193.

Veja também [Mudanças Importantes nos Parâmetros de Kernel Externos](#) e [Drivers de Dispositivos](#).

([BZ#1797671](#))

Filtro de Pacote Estendido Berkeley para RHEL 8.2

A **Extended Berkeley Packet Filter (eBPF)** é uma máquina virtual in-kernel que permite a execução do código no espaço do kernel, no ambiente restrito do sandbox com acesso a um conjunto limitado de funções. A máquina virtual executa um código especial tipo montagem. O bytecode **eBPF** primeiro carrega para o kernel, seguido por sua verificação, tradução do código para o código da máquina nativa com compilação just-in-time, e então a máquina virtual executa o código.

A Red Hat envia inúmeros componentes que utilizam a máquina virtual **eBPF**. Cada componente está em uma fase de desenvolvimento diferente e, portanto, nem todos os componentes são atualmente totalmente suportados. Na RHEL 8.2, os seguintes componentes **eBPF** são suportados:

- O pacote de ferramentas **BPF Compiler Collection (BCC)**, que é uma coleção de utilitários de rastreamento dinâmico de kernel que utilizam a máquina virtual **eBPF** para criar programas eficientes de rastreamento e manipulação de kernel. O **BCC** fornece ferramentas para análise de E/S, rede e monitoramento de sistemas operacionais Linux usando **eBPF**.
- A biblioteca **BCC** que permite o desenvolvimento de ferramentas similares àquelas fornecidas no pacote de ferramentas **BCC**.
- O recurso **eBPF for Traffic Control (tc)** que permite o processamento de pacotes programáveis dentro do caminho de dados do kernel da rede.

Todos os outros componentes **eBPF** estão disponíveis como Technology Preview, a menos que um componente específico seja indicado como suportado.

Os seguintes componentes notáveis **eBPF** estão atualmente disponíveis como Technology Preview:

- A linguagem **bpftool** tracing

- A característica **eXpress Data Path (XDP)**

Para mais informações sobre os componentes da Technology Previews, consulte [Technology Previews](#).

(BZ#1780124)

Software hospedeiro Intel® Omni-Path Architecture (OPA)

O software hospedeiro Intel Omni-Path Architecture (OPA) é totalmente suportado no Red Hat Enterprise Linux 8.2. A Intel OPA fornece hardware Host Fabric Interface (HFI) com inicialização e configuração para transferências de dados de alto desempenho (alta largura de banda, alta taxa de mensagens, baixa latência) entre nós de computação e de E/S em um ambiente cluster.

Para instruções sobre a instalação da documentação da arquitetura Intel Omni-Path, veja: <https://cdrdv2.intel.com/v1/dl/getContent/616368>

(BZ#1833541)

Control Group v2 é agora totalmente suportado na RHEL 8

o mecanismo **Control Group v2** é um grupo de controle unificado de hierarquia. **Control Group v2** organiza os processos hierarquicamente e distribui os recursos do sistema ao longo da hierarquia de forma controlada e configurável.

Ao contrário da versão anterior, **Control Group v2** tem apenas uma única hierarquia. Esta hierarquia única permite que o kernel Linux o faça:

- Categorizar os processos com base no papel de seu proprietário.
- Eliminar problemas com políticas conflitantes de múltiplas hierarquias.

Control Group v2 suporta numerosos controladores. Alguns dos exemplos são:

- O controlador de CPU regula a distribuição dos ciclos da CPU. Este controlador implementa:
 - Modelos de limite de peso e largura de banda absoluta para a política normal de programação.
 - Modelo absoluto de alocação de largura de banda para política de programação em tempo real.
- O controlador Cpuset limita a colocação do processador e/ou memória dos processos apenas àqueles dos recursos mencionados que estão especificados nos arquivos de interface **do cpuset**.
- O controlador de memória regula a distribuição da memória. Atualmente, os seguintes tipos de utilização de memória são rastreados:
 - Memória do espaço do usuário - cache de páginas e memória anônima.
 - Estruturas de dados do núcleo, tais como amolgadelas e inodes.
 - Tampões de soquete TCP.
- O controlador de E/S regula a distribuição dos recursos de E/S.
- O controlador Writeback interage tanto com os controladores de Memória como de E/S e é específico para **Control Group v2**

As informações acima foram baseadas na documentação do [Grupo de Controle v2](#) a montante. Você pode consultar o mesmo link para obter mais informações sobre determinados controladores **Control Group v2**.

Esteja avisado de que nem todas as características mencionadas no documento a montante estão ainda implementadas no RHEL 8.

(BZ#1401552)

Randomização de listas livres: Melhor desempenho e utilização da cache lateral de memória com mapeamento direto

Com este aprimoramento, você pode habilitar o alocador de páginas para randomizar listas livres e melhorar a utilização média de uma cache lateral de memória com mapeamento direto. A opção de linha de comando do kernel **page_alloc.shuffle**, permite que o alocador de páginas aleatorize as listas livres e coloca a bandeira booleana em **True**. O arquivo **sysfs**, que está localizado em **/sys/module/page_alloc/parameters/shuffle** lê o status da bandeira, embaralha as listas livres, de modo que a Memória Dinâmica de Acesso Aleatório (DRAM) é armazenada em cache, e a banda de latência entre a DRAM e a memória persistente é reduzida. Como resultado, a memória persistente com maior capacidade e menor largura de banda está disponível em plataformas de servidores de uso geral.

(BZ#1620349)

A ferramenta TPM userspace foi atualizada para a última versão

A ferramenta **tpm2-tools** userspace foi atualizada para a versão 3.2.1. Esta atualização fornece várias correções de erros, em particular relacionados à configuração da plataforma Código de registro e limpeza manual da página.

(BZ#1725714)

O chipset PCH série C620 suporta agora o recurso Intel Trace Hub

Esta atualização adiciona suporte de hardware para o Intel Trace Hub (TH) na série C620 Platform Controller Hub (PCH), também conhecido como Lewisburg PCH. Os usuários com a série C620 PCH podem agora usar o Intel TH.

(BZ#1714486)

A ferramenta perf agora suporta a agregação de eventos por matriz para processadores CLX-AP e CPX

Com esta atualização, a ferramenta **perf** agora fornece suporte para a agregação de contagens por evento para algumas CPUs Intel com múltiplas matrizes. Para ativar este modo, adicione a opção **--per-die** além da opção **-a** para os processadores do sistema Xeon Cascade Lake-AP (CLX-AP) e Cooper Lake (CPX). Como resultado, esta atualização detecta qualquer desequilíbrio entre os estampos. O comando **perf stat** captura a contagem do evento e exibe a saída como:

```
# perf stat -e cycles --per-die -a -- sleep 1
Performance counter stats for 'system wide':
S0-D0      8      21,029,877   cycles
S0-D1      8      19,192,372   cycles
```

(BZ#1660368)

O limiar de **crashkernel=auto** é reduzido na IBM Z

O limite inferior do parâmetro de linha de comando **crashkernel=auto** kernel é agora reduzido de 4G

para 1G nos sistemas IBM Z. Esta implementação permite que o IBM Z se alinhe com o limiar dos sistemas AMD64 e Intel 64 para compartilhar a mesma política de reserva no limiar inferior do **crashkernel=auto**. Como resultado, o crash kernel é capaz de reservar automaticamente memória para **kdump** em sistemas com menos de 4GB de RAM.

(BZ#1780432)

A entrada manual **numctl** esclarece a saída de uso de memória

Com este lançamento do RHEL 8, a página do manual de **numctl** menciona explicitamente que as informações de uso da memória refletem apenas as páginas residentes no sistema. A razão para este acréscimo é eliminar possíveis confusões para os usuários, quer as informações de uso de memória estejam relacionadas às páginas residentes ou à memória virtual.

(BZ#1730738)

O documento **kexec-tools** é agora atualizado para incluir o suporte ao alvo **Kdump FCoE**

Neste lançamento, o arquivo **/usr/share/doc/kexec-tools/supported-kdump-targets.txt** foi atualizado para incluir o suporte ao alvo **Kdump Fibre Channel over Ethernet (FCoE)**. Como resultado, os usuários agora podem ter um melhor entendimento do status e detalhes do mecanismo de despejo do **kdump** em um suporte de alvo **FCoE**.

(BZ#1690729)

O depósito de lixo assistido agora suporta o **PowerNV**

O mecanismo de despejo assistido por firmware (**fadump**) é agora suportado na plataforma **PowerNV**. O recurso é suportado com a versão do firmware **IBM POWER9 FW941** e mais tarde. No momento da falha do sistema, o **fadump**, junto com o arquivo **vmcore**, também exporta o arquivo **opalcore**. O arquivo **opalcore** contém informações sobre o estado da memória **OpenPOWER Abstraction Layer (OPAL)** no momento da falha. O arquivo **opalcore** é útil na depuração de falhas dos sistemas baseados em **OPAL**.

(BZ#1524687)

kernel-rt agora combina com a última árvore **RHEL 8**

As fontes de **kernel-rt** foram atualizadas para utilizar a última árvore de fontes do kernel **RHEL**. O conjunto de correções em tempo real também foi atualizado para a última versão upstream **v5.2.21-rt13**. Ambas as atualizações fornecem uma série de correções e melhorias de bugs.

(BZ#1680161)

rngd agora é capaz de funcionar com privilégios não-root

O daemon gerador de números aleatórios (**rngd**) verifica se os dados fornecidos pela fonte de aleatoriedade são suficientemente aleatórios e então armazena os dados no pool de entropia de números aleatórios do kernel. Com esta atualização, o **rngd** é capaz de rodar com privilégios de usuário não-root para aumentar a segurança do sistema.

(BZ#1692435)

Memória Virtual Persistente agora suportada para **RHEL 8.2** e posteriormente **POWER 9**

Ao executar um host **RHEL 8.2** ou posterior com um **PowerVM** hypervisor em hardware **IBM POWER9**, o host pode agora usar o recurso de Memória Virtual Persistente (**vPMEM**). Com o **vPMEM**, os dados persistem em toda a aplicação e a partição é reiniciada até que o servidor físico seja desligado. Como resultado, reiniciar as cargas de trabalho que utilizam o **vPMEM** é significativamente mais rápido.

Os seguintes requisitos devem ser atendidos para que seu sistema possa utilizar o vPMEM:

- Console de Gerenciamento de Hardware (HMC) V9R1 M940 ou posterior
- Firmware nível FW940 ou posterior
- Firmware do sistema E980 FW940 ou posterior
- Firmware do sistema L922 FW940 ou posterior
- PowerVM nível V3.1.1

Observe que vários problemas conhecidos ocorrem atualmente no RHEL 8 com o vPMEM. Para detalhes, veja os seguintes artigos da Base de Conhecimento:

- [O plug/desplug quente da memória pmem pode causar pânico no kernel em POWER9](#)
- [A inicialização do núcleo de captura leva muito tempo usando os espaços de nomes vPMEM como alvo de despejo para kdump/fadump](#)

(BZ#1859262)

5.8. SISTEMAS DE ARQUIVO E ARMAZENAMENTO

LVM agora suporta o método **dm-writecache** caching

Os volumes de cache LVM agora fornecem o método de cache **dm-writecache**, além do método **de cache dm** existente.

dm-cache

Este método acelera o acesso aos dados freqüentemente utilizados, armazenando-os em cache no volume mais rápido. O método armazena as operações de leitura e escrita.

dm-writecache

Este método só permite escrever operações de escrita. O volume mais rápido, geralmente um disco SSD ou uma memória persistente (PMEM), armazena primeiro as operações de gravação e depois as migra para o disco mais lento em segundo plano.

Para configurar o método de cache, use a opção **--type cache** ou **--type writecache** com o utilitário **lvconvert**.

Para mais informações, consulte [Permitindo o cache para melhorar o desempenho do volume lógico](#) .

(BZ#1600174)

A política de **assimetria** da VDO agora está em conformidade com o ACID

Com este lançamento, o modo de escrita **assimétrica** VDO está agora em conformidade com Atomicidade, Consistência, Isolamento, Durabilidade (ACID). Se o sistema parar inesperadamente enquanto o VDO estiver escrevendo dados em modo **assíncrono**, os dados recuperados agora são sempre consistentes.

Devido à conformidade com o ACID, o desempenho da **async** é agora menor em comparação com a versão anterior. Para restaurar o desempenho original, você pode mudar o modo de gravação em seu volume VDO para o modo **async-unsafe**, que não é compatível com o ACID.

Para mais informações, consulte [Seleção de um modo de escrita VDO](#) .

(BZ#1657301)

Agora você pode importar volumes VDO

O utilitário **vdo** agora permite importar volumes VDO existentes que atualmente não estão registrados em seu sistema. Para importar um volume VDO, use o comando de **importação vdo**.

Além disso, você pode modificar o Identificador Universalmente Único (UUID) de um volume VDO usando o comando de **importação vdo**.

(BZ#1713749)

Novo contador de erros per-op agora está disponível na saída dos mountstats e nfsiostat

Um pequeno recurso de suporte está disponível para os sistemas clientes NFS: a saída dos comandos **mountstats** e **nfsiostat** em **nfs-utils** tem uma contagem de erros **por operação**. Este aprimoramento permite que estas ferramentas exibam contagens de erros **por operação** e porcentagens que podem ajudar a reduzir os problemas em pontos de montagem específicos do NFS em uma máquina cliente NFS. Note que estas novas estatísticas dependem de mudanças no kernel que estão dentro do kernel do Red Hat Enterprise Linux 8.2.

(BZ#1719983)

As IOs de retorno com cgroup awareness estão agora disponíveis em XFS

Com este lançamento, a XFS suporta IOs de retorno com consciência de **cgroup**. De modo geral, a reversão de dados de **cgroup** requer apoio explícito do sistema de arquivos subjacente. Até agora, as IOs de writeback no XFS eram o atributo apenas para o **cgroup** raiz.

(BZ#1274406)

Os sistemas de arquivo FUSE agora implementam copy_file_range()

A chamada de sistema **copy_file_range()** fornece uma maneira para os sistemas de arquivos implementarem um mecanismo eficiente de cópia de dados. Com esta atualização, o GlusterFS, que está usando a estrutura do sistema de arquivos no espaço do usuário (FUSE), aproveita este mecanismo. Como a funcionalidade de leitura/gravação dos sistemas de arquivos FUSE envolve múltiplas cópias de dados, o uso do **copy_file_range()** pode melhorar significativamente o desempenho.

(BZ#1650518)

Suporte para estatísticas per-op agora está disponível para os comandos mountstats e nfsiostat

Um recurso de suporte está agora disponível para os sistemas clientes NFS: o arquivo **/proc/self/mountstats** tem o contador de erros **per-op**. Com esta atualização, sob cada linha de estatísticas **per-op**, o nono número indica o número das operações que foram concluídas com um valor de status inferior a zero. Este valor de status indica um erro. Para maiores informações, veja as atualizações dos programas **mountstats** e **nfsiostat** nos **nfs-utils** que exibem estas novas contagens de erros.

(BZ#1636572)

Novas estatísticas de montarias lease_time e lease_expired estão disponíveis no arquivo /proc/self/mountstats

Um recurso de suporte está disponível para sistemas clientes NFSv4.x. O arquivo **/proc/self/mountstats**

tem os campos **lease_time** e **lease_expired** no final da linha, começando com **nfsv4:**. O campo **lease_time** indica o número de segundos no tempo de locação do NFSv4. O campo **lease_expired** indica o número de segundos desde que a locação expirou, ou 0 se a locação não tiver expirado.

(BZ#1727369)

5.9. ALTA DISPONIBILIDADE E CLUSTERS

Novas opções de comando para desativar um recurso somente se isso não afetar outros recursos

S vezes é necessário desativar recursos somente se isso não tiver efeito sobre outros recursos. Assegurar que este seria o caso pode ser impossível de fazer à mão quando relações complexas de recursos são estabelecidas. Para resolver esta necessidade, o comando de **desativação de recursos** **pcs** agora suporta as seguintes opções:

- **pcs resource disable --simulate**: mostrar os efeitos de desativar o(s) recurso(s) especificado(s), sem alterar a configuração do cluster
- **pcs resource disable --safe**: desabilitar recursos especificados somente se nenhum outro recurso for afetado de alguma forma, tal como ser migrado de um nó para outro
- **pcs resource disable --safe --no-strict**: desabilitar recurso(s) especificado(s) somente se nenhum outro recurso for interrompido ou despromovido

Além disso, o comando **pcs resource safe-disable** foi introduzido como um alias para **pcs resource disable --safe**.

(BZ#1631519)

Novo comando para mostrar as relações entre os recursos

O novo comando **pcs resource relations** permite exibir as relações entre os recursos de cluster em uma estrutura em árvore.

(BZ#1631514)

Novo comando para exibir o status de um site primário e de um cluster de sites de recuperação

Se você configurou um cluster para usar como um local de recuperação, agora você pode configurar esse cluster como um cluster de local de recuperação com o comando **pcs dr**. Você pode então usar o comando **pcs dr** para exibir o status tanto de seu cluster de site principal quanto de seu cluster de site de recuperação de um único nó.

(BZ#1676431)

Restrições expiradas de recursos são agora escondidas por padrão ao listar restrições

A listagem de restrições de recursos não mais por padrão exibe restrições expiradas. Para incluir os consumos expirados, use a opção **--all** do comando **pcs constraint**. Isto listará as restrições expiradas, anotando as restrições e suas regras associadas como **(expiradas)** no display.

(BZ#1442116)

Suporte de marcapasso para configuração de recursos para permanecer parado no desligamento do nó limpo

Quando um nó de cluster se desliga, a resposta padrão do Pacemaker é interromper todos os recursos que correm naquele nó e recuperá-los em outro lugar. Alguns usuários preferem ter alta disponibilidade apenas para falhas, e tratar as paradas limpas como interrupções programadas. Para resolver isso, o Pacemaker agora suporta as propriedades de cluster de **bloqueio** e **limite de bloqueio** para especificar que os recursos ativos em um nó quando ele se desliga devem permanecer parados até que o próximo nó se junte novamente. Os usuários podem agora usar desligamentos limpos como interrupções programadas sem qualquer intervenção manual. Para informações sobre como configurar recursos para permanecerem parados em um desligamento de nó limpo, consulte o link: [Configurando os recursos para permanecerem parados no desligamento do nó limpo](#).

(BZ#1712584)

Suporte para o funcionamento do ambiente de cluster em um único nó

Um cluster com apenas um membro configurado é agora capaz de iniciar e executar recursos em um ambiente de cluster. Isto permite que um usuário configure um site separado de recuperação de desastres para um cluster com vários nós que usa um único nó para backup. Note que um cluster com apenas um nó não é, por si só, tolerante a falhas.

(BZ#1700104)

5.10. LINGUAGENS DE PROGRAMAÇÃO DINÂMICA, SERVIDORES WEB E DE BANCO DE DADOS

Um novo módulo: **python38**

RHEL 8.2 apresenta o Python 3.8, fornecido pelo novo módulo **python38** e a imagem do recipiente **ubi8/python-38**.

As melhorias notáveis em comparação com o Python 3.6 incluem:

- Novos módulos Python, por exemplo, **contextvars**, **dataclasses**, ou **importlib.resources**
- Novas características de linguagem, tais como expressões de atribuição (o chamado operador de morsa, **:=**) ou parâmetros apenas posicionais
- Melhor experiência do desenvolvedor com a função integrada de **breakpoint()**, a especificação da string de formato **=** e a compatibilidade entre os módulos de depuração e não depuração do Python e módulos de extensão
- Melhorias de desempenho
- Suporte melhorado para dicas de tipo estático opcional
- Uma adição do **=** especificador para formatar literalmente as cordas (f-strings) para facilitar a depuração
- Versões atualizadas de pacotes, tais como **pip**, **pedidos** ou **Cython**

Python 3.8 e pacotes construídos para ele podem ser instalados em paralelo com o Python 3.6 no mesmo sistema.

Observe que o módulo **python38** não inclui as mesmas ligações binárias para ferramentas do sistema (RPM, DNF, SELinux e outras) que são fornecidas para o módulo **python36**.

Para instalar pacotes a partir do módulo **python38**, use, por exemplo:

■

```
# yum install python38
# yum install python38-Cython
```

O fluxo do módulo **python38:3.8** será ativado automaticamente.

Para dirigir o intérprete, utilizar, por exemplo:

```
$ python3.8
$ python3.8 -m cython --help
```

Veja [Usando Python](#) para mais informações.

Note que a Red Hat continuará fornecendo suporte ao Python 3.6 até o final da vida útil do RHEL 8. Python 3.8 terá um ciclo de vida mais curto, ver [RHEL 8 Application Streams Life Cycle](#).

(BZ#1747329)

Mudanças na instalação do `mod_wsgi`

Anteriormente, quando o usuário tentava instalar o módulo **mod_wsgi** usando o comando **yum install mod_wsgi**, o pacote **python3-mod_wsgi** era sempre instalado. O RHEL 8.2 introduz o Python 3.8 como uma adição ao Python 3.6. Com esta atualização, você precisa especificar qual versão do **mod_wsgi** você deseja instalar, caso contrário, uma mensagem de erro é retornada.

Para instalar a versão Python 3.6 do **mod_wsgi**:

```
# yum instalar python3-mod_wsgi
```

Para instalar a versão Python 3.8 do **mod_wsgi**:

```
# yum instalar python38-mod_wsgi
```

Observe que os pacotes **python3-mod_wsgi** e **python38-mod_wsgi** entram em conflito entre si, e apenas um módulo **mod_wsgi** pode ser instalado em um sistema devido a uma limitação do Servidor HTTP Apache.

Esta mudança introduziu um problema conhecido de dependência descrito no [BZ#1829692](#).

(BZ#1779705)

Suporte para deflacionar em `zlib` com aceleração de hardware no IBM Z

Esta atualização adiciona suporte para um algoritmo de deflacionamento acelerado por hardware à biblioteca **zlib** nos mainframes IBM Z. Como resultado, o desempenho de compressão e descompressão nas máquinas vetoriais IBM Z foi melhorado.

(BZ#1659433)

Desempenho melhorado na descompressão de `gzip` em IBM Power Systems, little endian

Esta atualização adiciona otimização para a verificação da redundância cíclica de 32 bits (CRC32) à biblioteca **zlib** em IBM Power Systems, little endian. Como resultado, o desempenho dos arquivos **gzip** descompactadores foi melhorado.

(BZ#1666798)

Um novo fluxo de módulos: **maven:3.6**

RHEL 8.2 apresenta um novo fluxo de módulos, **maven:3.6**. Esta versão da ferramenta de gerenciamento e compreensão do projeto de software Maven fornece numerosas correções de bugs e várias melhorias sobre o fluxo **maven:3.5** distribuído com o RHEL 8.0.

Para instalar o fluxo **maven:3.6**, use:

```
#módulo yum instalar maven:3.6
```

Se você quiser atualizar do fluxo **maven:3.5**, veja [Mudando para um fluxo posterior](#).

(BZ#1783926)

mod_md agora suporta o protocolo ACMEv2

O módulo **mod_md** foi atualizado para a versão 2.0.8. Esta atualização acrescenta uma série de características, notadamente o suporte à versão 2 do protocolo de emissão e gerenciamento de certificados do Ambiente de Gerenciamento de Certificados Automáticos (ACME), que é o padrão da Internet Engineering Task Force (IETF) (RFC 8555). O protocolo ACMEv1 original continua a ter suporte, mas é depreciado pelos provedores de serviços populares.

(BZ#1747923)

Novas extensões para PHP 7.3

O fluxo do módulo **php:7.3** foi atualizado para fornecer duas novas extensões PHP: **rrd** e **Xdebug**.

A extensão **do rrd** fornece ligações para a biblioteca do **RRDtool C**. O **RRDtool** é um sistema de registro de dados e gráficos de alto desempenho para dados de séries temporais.

A extensão **Xdebug** está incluída para ajudá-lo com a depuração e desenvolvimento. Note que a extensão é fornecida somente para fins de desenvolvimento e não deve ser usada em ambientes de produção.

Para informações sobre a instalação e uso do PHP no RHEL 8, veja [Utilizando a linguagem PHP scripting](#).

(BZ#1769857, BZ#1764738)

Novos pacotes: **perl-LDAP** e **perl-Convert-ASN1**

Esta atualização adiciona os pacotes **perl-LDAP** e **Perl-Convert-ASN1** à RHEL 8. O pacote **perl-LDAP** fornece um cliente LDAP para a linguagem Perl. **perl-LDAP** requer o pacote **perl-Convert-ASN1**, que codifica e decodifica a Notação de Sintaxe Abstrata Um (ASN.1) estruturas de dados usando Regras Básicas de Codificação (BER) e Regras de Codificação Distinta (DER).

(BZ#1663063, BZ#1746898)

sscg agora suporta gerar arquivos chave privados protegidos por uma senha

O utilitário **sscg** é agora capaz de gerar arquivos chave privados protegidos por uma senha. Isto acrescenta outro nível de proteção para chaves privadas, e é exigido por alguns serviços, como o FreeRADIUS.

(BZ#1717880)

5.11. COMPILADORES E FERRAMENTAS DE DESENVOLVIMENTO

grafana rebaseada para a versão 6.3.6

O pacote **grafana** foi atualizado para a versão 6.3.6, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Base de dados: Reescreve a consulta de estatísticas do sistema para um melhor desempenho.
- Explorar:
 - Conserta o layout do campo de consulta em vista dividida para os navegadores Safari.
 - Adiciona a opção Live para as fontes de dados suportadas, adiciona a **orgId** à URL para fins de compartilhamento.
 - Adiciona suporte para os novos parâmetros **iniciais** e **finais** do **loki** para o ponto final das etiquetas.
 - Adiciona suporte para alternar o modo de consulta bruta no Explorar, permite alternar entre métricas e logs.
 - Exibe o contexto das linhas de registro, não analisa os níveis de registro se fornecidos por campo ou etiqueta.
 - Suporta a nova sintaxe de filtragem **LogQL**.
 - Utiliza o novo **TimePicker** da Grafana/UI.
 - Lida com novas linhas no **LogRow** Highlighter.
 - Fixa a navegação de volta ao painel do painel.
 - Fixa o filtro por nível de série no gráfico de logs.
 - Corrigir problemas quando o carregamento e o gráfico/tabela são colapsados.
 - Fixa a seleção/cópia das linhas de troncos.
- Painel de controle: Corrige o erro de carregamento de painéis de controle **com** links de painel que tinham propriedades ausentes, e corrige a configuração do painel de controle de fuso horário ao exportar para os valores separados por vírgula (CSV) Links de dados.
- Editor: Corrige um número onde apenas linhas inteiras estavam sendo copiadas.
- LDAP: Integração dos componentes de autenticação **multi ldap** e **ldap**.
- Perfil/UserAdmin: Corrige o agente parser do usuário que trava o **grafana-server** em builds de 32 bits.
- Prometheus:
 - Evita que o editor do painel trave enquanto muda para a fonte de dados **Prometheus**, muda o comportamento de **inserção de braçadeiras** para ser menos irritante.
 - Fixa as consultas com o **label_replace** e remove a correspondência de \$1 ao carregar o editor de consultas.

- Consistentemente permite consultas de várias linhas no editor, levando em conta o fuso horário para o alinhamento dos passos.
- Utiliza a faixa de painéis sobrepostos por **\$__range** em vez da faixa do painel de instrumentos.
- Adiciona filtro de intervalo de tempo à consulta de rótulos em série, escapa | literalmente nas variáveis interpoladas **da PromQL**.
- Fixa enquanto adiciona etiquetas para métricas que contêm colons no Explore.
- Auth: Permite expirar as chaves API, devolver dispositivo, os e navegador enquanto lista os tokens auth do usuário em HTTP API, suporta lista e revogação de tokens auth do usuário em UI.
- DataLinks: Aplica corretamente as variáveis escapadas aos links de dados, segue o fuso horário enquanto exibe o carimbo de data no menu de contexto gráfico, utiliza corretamente o carimbo de data quando interpola as variáveis, corrige a interpolação incorreta do **nome_série** **\$_series_name**.
- Gráfico: Corrige o problema da legenda clicando no ícone de linha em série e o problema com a barra de rolagem horizontal visível nas janelas, adiciona nova opção de gradiente de preenchimento.
- Grafite: Evita o globo de variáveis de array de valor único, corrige problemas com a função de alias sendo movida por último, corrige problemas com a **sérieByTag**
- Série TimeSeries: Supõe que os valores são todos os números.
- Bitola/BarGauge: Corrige o problema com os limites perdidos e um gabarito de carga de problemas com o **avg** stat.
- PanelLinks: Corrige problema de colisão com o Gauge
- OAuth: Corrige a falha de login do OAuth em **falta** devido à política de cookies do SameSite, corrige o token de usuário errado atualizado na atualização do **OAuth** no proxy DS.
- Auth Proxy: Inclui cabeçalhos adicionais como uma parte da chave do cache.
- **cli**: Correção para reconhecer quando em modo dev, corrige a questão da falha de **criptografia de senhas-fonte de dados** com o erro sql.
- Permissões: Mostrar plugins na navegação para usuários não administradores, mas esconde a configuração de plugins.
- TimePicker: Aumenta a altura máxima de queda rápida de alcance e corrige o problema de estilo para o popover de alcance personalizado.
- Loki: Exibe os logs com cauda ao vivo na ordem correta no Explore.
- Timerange: Corrige um bug onde os intervalos de tempo personalizados não estavam seguindo o Tempo Universal Coordenado (UTC).
- **remote_cache**: Conserta o **redis connstring** parsing.

- Alerta: Adicionar tags às regras de alerta, tentativas de enviar notificações por e-mail para todos os endereços de e-mail fornecidos, melhora o teste das regras de alerta, suporte para configurar o campo de conteúdo do notificador de alerta **Discord**.
- Alertmanager: Substitui caracteres ilegais por sublinhados nos nomes dos rótulos.
- AzureMonitor: Mudanças que colidem com variáveis Grafana embutidas ou nomes de macros para os Logs Azure.
- CloudWatch: Tornou a região visível para o Amazon Web Services (AWS) Cloudwatch Expressions, acrescenta a métrica AWS **DocDB**.
- GraphPanel: Não ordenar séries quando a tabela de legendas e a coluna de ordenação não estiverem visíveis.
- InfluxDB: Suporta a visualização de logs no Explore.
- MySQL/Postgres/MSSQL: Adiciona análise para intervalos de dias, semanas e anos em macros, adiciona suporte para recarga periódica de certificados do cliente.
- Plugins: Substitui a lista **DataFormats** pela bandeira **SkipDataQuery** no arquivo **plugin.json**.
- Refresh picker: Manipula intervalos vazios.
- Singlestat: Adicione **a** configuração min/max aos sparklines do singlestat.
- Modelagem: Exibe corretamente o **__texto** na variável multi-valor após recarregar a página, suporta a seleção de todos os valores filtrados de uma variável multi-valor.
- Frontend: Conserta componente de árvore Json não funcionando problema.
- InfluxDB: Corrige problemas com aspas simples que não escaparam nos filtros de valor do rótulo.
- Config: Fixa a opção **connectionstring** para a **cache_controle remota** no arquivo **default.ini**.
- Elasticsearch: Corrige a consulta vazia (via variável modelo) deve ser enviada como curinga, corrige os pedidos de fragmentos simultâneos máximos padrão, suporta a visualização de logs no Explore.
- QuadroPainel: Fixa a exibição das anotações.
- Grafana-CLI: Fixa bandeiras de recepção via linha de comando, invólucro para o **grafana-cli** dentro dos pacotes **RPM/DEB** e **config/homepath** são agora bandeiras globais.
- HTTPServer: Conserta a formatação do cabeçalho **X-XSS-Protection**, opções para retornar novos cabeçalhos **X-Content-Type-Options**, **X-XSS-Protection** e **Strict-Transport-Security**, conserta o cabeçalho **Strict-Transport-Security**, serve a Grafana com um prefixo de caminho de URL personalizado.

([BZ#1725278](#))

pcp rebaseado para a versão 5.0.2

O pacote **pcp** foi atualizado para a versão 5.0.2, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Os pacotes **pcp-webapp-*** são agora substituídos pelo pacote **grafana-pcp** e **pmproxy**.

- A ferramenta **pcp-collectl** é agora substituída pelas configurações **pmrep**.
- Novos e melhores agentes de domínio métrico de desempenho (PMDAs):
 - **pmdamssql**: Novo PMDA para implementação do Microsoft SQL Server.
 - **pmdanetcheck**: Novo PMDA para realizar verificações de rede.
 - **pmdaopenmetrics**: Renomeia agente **prometheus** para **openmetrics**.
 - **pmdanfsclient**: Adiciona as métricas de erro **por operação** e **por montagem rpc**.
 - **pmdalmsensors**: Melhorias na análise do nome e tratamento de erros.
 - **pmdaperfevent**: Suporta eventos **hv_24x7** ninho no sistema multi-nó.
 - **pmdalinux**:
 - Manipula corretamente os nós esparsos ou descontínuos em nós.
 - Usa o **instname** cpu e não o **instid** para **per-cpu** numa estatística.
 - Adiciona uma placa ativa e total de lajes à análise da **placa** v2
 - Fixa vários soquetes unix, sistema métrico **icmp6**, valor métrico da página de abraço. cálculos, **segmentação** em código de interrupção com grandes contagens de CPU
 - Obtém mais métricas de rede no espaço de nomes **--container**.
 - **pmdabcc**: Fixa o módulo tracepoints para o **bcc** 0.10.0 e versões superiores
 - **pmdabpfttrace**: Novo PMDA para métricas dos roteiros **bpfttrace**
 - **pmdaproc**:
 - Corrige o vazamento de memória na atualização da **lista de pendências**.
 - Evita chamadas excessivas em **cgroups_scan**.
 - Retém caminhos de **grupos** e apenas nomes de instâncias não escapadas.
 - **pmdaroot**: Melhora o manuseio do comportamento em cache ou inativo do **cgroup** e refresca o conteúdo **do cgroup** fs também.
- Fixa as ferramentas de coleta (servidor):
 - **pmproxy**: Suporte Openmetrics através do endpoint **/metrics**, consolida o **pmseries/grafana** REST API, e adiciona a nova implementação do **PMWEBAPI(3)** REST API assíncrono.
 - **selinux**: Numerosas atualizações da política de pcp.
 - python **pmdas**: Permite o suporte de autenticação, novo método **set_comm_flags** para definir as bandeiras de comunicação.
 - **python api**: Exporta o **pmdaGetContext()** e adiciona o invólucro de depuração.
 - **perl api**: Assegura o contexto criado para a loja PMDA como com a embalagem de python.

- **sistemad**: Adiciona um timeout de 120s em todos os serviços e conserta a falha para iniciar o serviço de **pmlogger**.
- Fixa as ferramentas de análise (cliente):
 - **pmchart**: Corrige a autoescala do gráfico sob condições de erro de fetch.
 - **pmrep**: Fixa a **fórmula wait.formula** para **collectl-dm-sD** e **collectl-sD**.
 - **pmseries**: Fornece suporte para a palavra-chave delta e melhores timestamps.
 - **pcp-atop**: Conserta o modo de escrita (**-w**) para lidar com a métrica **proc** vs **hotproc**.
 - **pcp-atopsar**: Corrige o maltrato de alguns argumentos de linha de comando.
 - **pcp-dstat**: Fixa cabeçalhos desalinhados na saída CSV e manuseio da opção **--bits** da linha de comando.
 - **libpcp**: Conserta o **segv do cockpit-pcp** com contexto local e tratamento de erros de replay multi-arquivos para o(s) arquivo(s) corrompido(s).

(BZ#1723598)

grafana-pcp está agora disponível em RHEL 8.2

O pacote **grafana-pcp** fornece novas fontes de dados de **grafana** e plugins de aplicação conectando o **PCP** com a **grafana**. Com o pacote **grafana-pcp**, você pode analisar métricas históricas de **PCP** e métricas de **PCP** em tempo real usando a linguagem de consulta **pmseries** e serviços ao vivo **pmwebapi**, respectivamente. Para mais informações, veja [Performance Co-Pilot Grafana Plugin](#).

(BZ#1685315)

Conjunto de Ferramentas GCC Atualizadas 9

O GCC Toolset 9 é um conjunto de ferramentas de compilação que fornece versões recentes de ferramentas de desenvolvimento. Ele está disponível como um Application Stream na forma de uma Coleção de Software no repositório **AppStream**.

As mudanças notáveis introduzidas com o RHEL 8.2 incluem:

- O compilador GCC foi atualizado para a versão 9.2.1, que fornece muitas correções e melhorias de bugs que estão disponíveis no GCC upstream.
 - Os componentes do GCC Toolset 9 estão agora disponíveis nas duas imagens do contêiner:
 - **rhel8/gcc-toolset-9-toolchain**, que inclui o compilador GCC, o depurador GDB, e a ferramenta de automação **make**.
 - **rhel8/gcc-toolset-9-perftools**, que inclui as ferramentas de monitoramento de desempenho, tais como SystemTap e Valgrind.
- Para puxar uma imagem de recipiente, execute o seguinte comando como raiz:

```
# podman pull registry.redhat.io/<image_name>
```

As seguintes ferramentas e versões são fornecidas pelo GCC Toolset 9:

Ferramenta	Versão
GCC	9.2.1
GDB	8.3
Valgrind	3.15.0
SystemTap	4.1
Dyninst	10.1.0
binutils	2.32
elfutils	0.176
dwz	0.12
fazer	4.2.1
strace	5.1
ltrace	0.7.91
annobin	9.08

Para instalar o GCC Toolset 9, execute o seguinte comando como raiz:

```
# yum instalar gcc-toolset-9
```

Para executar uma ferramenta do GCC Toolset 9:

```
$ scl habilita gcc-toolset-9 tool
```

Para executar uma sessão de shell onde as versões de ferramentas do GCC Toolset 9 têm precedência sobre as versões de sistema dessas ferramentas:

```
$ scl habilita gcc-toolset-9 bash
```

Para mais informações, consulte [Utilizando o GCC Toolset](#).

[\(BZ#1789401\)](#)

O GCC Toolset 9 agora suporta a descarga do alvo NVIDIA PTX

O compilador GCC no GCC Toolset 9 agora suporta o OpenMP target offloading para NVIDIA PTX.

[\(BZ#1698607\)](#)

O compilador GCC atualizado está agora disponível para a RHEL 8.2

O compilador do sistema GCC, versão 8.3.1, foi atualizado para incluir numerosas correções de erros e melhorias disponíveis no GCC a montante.

A coleção GNU Compiler Collection (GCC) fornece ferramentas para desenvolver aplicações com as linguagens de programação C, C++, e Fortran.

Para informações de uso, consulte [Desenvolvendo aplicações C e C++ no RHEL 8](#).

(BZ#1747157)

Um novo sintonizador para mudar o tamanho máximo do fastbin em **glibc**

A função **malloc** utiliza uma série de caixotes rápidos que retêm pedaços de memória reutilizáveis até um tamanho específico. O tamanho máximo padrão do pedaço é 80 bytes em sistemas de 32 bits e 160 bytes em sistemas de 64 bits. Este aperfeiçoamento introduz uma nova **glibc.malloc.mxfast** tunable para a **glibc** que permite mudar o tamanho máximo da fastbin.

(BZ#1764218)

Biblioteca matemática vetorizada está agora habilitada para o GNU Fortran no GCC Toolset 9

Com esta melhoria, o GNU Fortran do GCC Toolset pode agora usar rotinas da biblioteca matemática vetorizada **libmvec**. Anteriormente, o compilador Fortran do GCC Toolset precisava de um arquivo de cabeçalho Fortran antes de poder usar as rotinas da **libmvec** fornecidas pela **glibc** da GNU C Library.

(BZ#1764238)

O **glibc.malloc.tcache** sintonizável foi melhorado

A **glibc.malloc.tcache_count** tunable permite definir o número máximo de pedaços de memória de cada tamanho que podem ser armazenados no cache por fio (tcache). Com esta atualização, o limite superior do **glibc.malloc.tcache_count** tunable foi aumentado de 127 para 65535.

(BZ#1746933)

O carregador dinâmico **glibc** é aperfeiçoado para fornecer um mecanismo de pré-carga não hermético da biblioteca

Com este aperfeiçoamento, o carregador pode agora ser invocado para carregar um programa de usuário com uma opção **--preload** seguido por uma lista de bibliotecas separadas por dois pontos para pré-carregar. Este recurso permite que os usuários invoquem seus programas diretamente através do carregador com uma lista de pré-carga de biblioteca não-interferida.

Anteriormente, os usuários tinham que usar a variável de ambiente LD_PRELOAD que era herdada por todos os processos infantis através de seu ambiente.

(BZ#1747453)

GDB agora suporta a extensão ARCH(13) sobre a arquitetura IBM Z

Com este aperfeiçoamento, o GNU Debugger (GDB) agora suporta as novas instruções implementadas pela extensão ARCH(13) sobre a arquitetura IBM Z.

(BZ#1768593)

elfutils rebaseado para a versão 0.178

O pacote **elfutils** foi atualizado para a versão 0.178, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- **elfclassificar**: uma nova ferramenta para analisar objetos ELF.
- **debuginfod**: um novo servidor, ferramenta cliente e biblioteca para indexar e buscar automaticamente ELF, DWARF, e fonte de arquivos e arquivos RPM através de HTTP.
- **libeb1** é agora diretamente compilada em **libdw.so**.
- **eu-readelf** tem múltiplas bandeiras novas para notas, numeração de seções e tabelas de símbolos.
- **a libdw** melhorou o suporte multithreading.
- **a libdw** suporta extensões adicionais do GNU DWARF.

(BZ#1744992)

SystemTap rebaseado para a versão 4.2

A ferramenta de instrumentação SystemTap foi atualizada para a versão 4.2. As melhorias notáveis incluem:

- Os backtraces podem agora incluir nomes de arquivos fonte e números de linha.
- Numerosas extensões back-end do Berkeley Packet Filter (BPF) estão agora disponíveis, por exemplo, para looping, timing, e outros processos.
- Um novo serviço de gerenciamento de scripts SystemTap está disponível. Este serviço envia métricas para um sistema de monitoramento compatível com o Prometheus.
- O SystemTap herdou a funcionalidade de um novo servidor de arquivos HTTP para **elfutils** chamado **de debuginfod**. Este servidor envia automaticamente recursos de debugging para SystemTap.

(BZ#1744989)

Melhorias nos contadores de desempenho da série IBM Z

As máquinas IBM série Z tipo 0x8561, 0x8562, e 0x3907 (z14 ZR1) são agora reconhecidas pela **libpfm**. Eventos de desempenho para monitoramento de operações de criptografia de curvas elípticas (ECC) na série IBM Z estão agora disponíveis. Isto permite o monitoramento de subsistemas adicionais em máquinas da série IBM Z.

(BZ#1731019)

Rust Toolset rebaseado para a versão 1.41

O Rust Toolset foi atualizado para a versão 1.41. As mudanças notáveis incluem:

- A implementação de novas características é agora mais fácil porque a regra dos órfãos é menos rígida.
- Agora você pode anexar o atributo **#[non_exhaustive]** a uma **estrutura**, um **enum**, ou variantes de **enum**.
- Usando **Box<T>** na Interface de Função Estrangeira (FFI) tem mais garantias agora. **Box<T>** terá a mesma Interface Binária de Aplicação (ABI) que um ponteiro **T*** na FFI.

- O Rust é suposto detectar bugs de segurança da memória em tempo de compilação, mas o verificador de empréstimos anteriores tinha limitações e permitia um comportamento indefinido e a falta de segurança da memória. O novo verificador de vida não-lexical (NLL) pode relatar problemas de falta de segurança de memória como erros graves. Ele agora se aplica às edições Rust 2015 e Rust 2018. Anteriormente, em Rust 2015, o verificador de empréstimos NLL apenas levantava avisos sobre tais problemas.

Para instalar o módulo **ferrugem**, execute o seguinte comando como raiz:

```
# módulo yum instalar ferrugem
```

Para obter informações sobre o uso, consulte [Utilização do conjunto de ferramentas ferrugem](#) .

(BZ#1776847)

LLVM Toolset rebaseado para a versão 9.0.1

O conjunto de ferramentas LLVM foi atualizado para a versão 9.0.1. Com esta atualização, as declarações **asm goto** agora são suportadas. Esta mudança permite compilar o kernel Linux nas arquiteturas AMD64 e Intel 64.

Para instalar o módulo **llvm-toolset**, execute o seguinte comando como raiz:

```
#módulo yum instalar llvm-toolset
```

Para mais informações, consulte [Utilizando o conjunto de ferramentas LLVM](#) .

(BZ#1747139)

Go Toolset rebaseado para a versão 1.13

O Go Toolset foi atualizado para a versão 1.13. Melhorias notáveis incluem:

- Go pode agora usar um módulo criptográfico certificado FIPS quando o sistema RHEL é inicializado no modo FIPS. Os usuários podem ativar este modo manualmente usando a variável de ambiente **GOLANG_FIPS=1**.
- O depurador Delve, versão 1.3.2, está agora disponível para Go. É um depurador de nível de fonte para a linguagem de programação Go(**golang**).

Para instalar o módulo **go-toolset**, execute o seguinte comando como raiz:

```
#módulo yum instalar go-toolset
```

Para instalar o depurador Delve, execute o seguinte comando como raiz:

```
# yum install delve
```

Para depurar um programa **helloworld.go** usando Delve, execute o seguinte comando:

```
$ dlv debug helloworld.go
```

Para obter mais informações sobre o Go Toolset, consulte [Utilizando o Go Toolset](#).

Para mais informações sobre a Delve, veja a [documentação da Delve](#) a montante.

(BZ#1747150)

OpenJDK agora também suporta secp256k1

Anteriormente, o Open Java Development Kit (OpenJDK) podia usar apenas curvas da biblioteca NSS. Conseqüentemente, o OpenJDK forneceu apenas as curvas secp256r1, secp384r1, e secp521r1 para criptografia de curvas elípticas (ECC). Com esta atualização, o OpenJDK utiliza a implementação interna do ECC e suporta também a curva secp256k1.

(BZ#1746875, BZ#1746879)

5.12. GESTÃO DA IDENTIDADE

IdM agora suporta novos módulos de gerenciamento Ansible management

Esta atualização introduz vários módulos **ansible-freeipa** para automatizar tarefas comuns de Gerenciamento de Identidade (IdM) usando Livros de Jogadas Ansíveis:

- O módulo **ipauser** automatiza a adição e remoção de usuários.
- O módulo **ipagroup** automatiza a adição e remoção de usuários e grupos de usuários de e para grupos de usuários.
- O módulo **ipahost** automatiza a adição e remoção de hospedeiros.
- O módulo **ipahostgroup** automatiza a adição e remoção de hosts e grupos anfitriões de e para grupos anfitriões.
- O módulo **ipasudorule** automatiza o gerenciamento do comando **sudo** e da regra **sudo**.
- O módulo **ipapwpolicy** automatiza a configuração das políticas de senhas na IdM.
- O módulo **ipahbacrule** automatiza o gerenciamento do controle de acesso baseado em host na IdM.

Note que você pode combinar duas ou mais chamadas **ipauser** em uma com a variável **usuários** ou, alternativamente, usar um arquivo JSON contendo os usuários. Da mesma forma, você pode combinar duas ou mais chamadas **ipahost** em uma com a variável **hosts** ou, alternativamente, usar um arquivo JSON contendo os hosts. O módulo **ipahost** também pode garantir a presença ou ausência de vários endereços IPv4 e IPv6 para um host.

(JIRA:RHELPLAN-37713)

IdM Healthcheck agora suporta a triagem de registros DNS

Esta atualização introduz um teste manual independente dos registros DNS em um servidor de Gerenciamento de Identidade (IdM).

O teste usa a ferramenta **Healthcheck** e realiza uma consulta DNS usando o resolvidor local no arquivo **etc/resolv.conf**. O teste garante que os registros DNS esperados necessários para a auto-descoberta sejam resolvidos.

(JIRA:RHELPLAN-37777)

A integração direta da RHEL no AD usando SSSD agora suporta FIPS

Com este aperfeiçoamento, o System Services Security Daemon (SSSD) agora se integra às implantações do Active Directory (AD) cujos mecanismos de autenticação utilizam tipos de criptografia

que foram aprovados pelo Federal Information Processing Standard (FIPS). O aprimoramento permite integrar diretamente os sistemas RHEL ao AD em ambientes que devem atender aos critérios FIPS.

[\(BZ#1841170\)](#)

O protocolo SMB1 foi desativado por padrão no servidor Samba e nas utilidades do cliente

No Samba 4.11, os valores padrão do **protocolo servidor min** e os parâmetros do **protocolo cliente min** foram alterados de **NT1** para **SMB2_02** porque o protocolo de bloco de mensagens do servidor versão 1 (SMB1) foi depreciado. Se você não tiver definido estes parâmetros no arquivo **/etc/samba/smb.conf**:

- Os clientes que suportam apenas SMB1 não são mais capazes de se conectar ao servidor Samba.
- Os utilitários do cliente Samba, como o **smbclient**, e a biblioteca **libsmbclient** não conseguem se conectar a servidores que só suportam SMB1.

A Red Hat recomenda que não se utilize o protocolo SMB1. Entretanto, se seu ambiente exigir o SMB1, você pode reativar o protocolo manualmente.

Para reativar o SMB1 em um servidor Samba:

- Adicione a seguinte configuração ao arquivo **/etc/samba/smb.conf**:

```
server min protocol = NT1
```

- Reinicie o serviço **smb**:

```
# systemctl restart smb
```

Para reativar o SMB1 para as utilidades dos clientes Samba e a biblioteca **libsmbclient**:

- Adicione a seguinte configuração ao arquivo **/etc/samba/smb.conf**:

```
protocolo cliente min = NT1
```

- Reinicie o serviço **smb**:

```
# systemctl restart smb
```

Note que o protocolo SMB1 será removido em um futuro lançamento do Samba.

[\(BZ#1785248\)](#)

samba rebaseado para a versão 4.11.2

Os pacotes *samba* foram atualizados para a versão 4.11.2, que fornece uma série de correções e melhorias em relação à versão anterior. Mudanças notáveis incluem:

- Por padrão, o protocolo de bloco de mensagens do servidor versão 1 (SMB1) está agora desabilitado no servidor Samba, nos utilitários do cliente e na biblioteca **da libsmbclient**. Entretanto, ainda é possível definir manualmente os parâmetros do **protocolo server min** e **client min protocol** para **NT1** para reativar o SMB1. A Red Hat não recomenda a reativação do protocolo SMB1.

- Os parâmetros do **lanman auth** e **criptografar senhas** são depreciados. Estes parâmetros permitem autenticação insegura e só estão disponíveis no protocolo SMB1 depreciado.
- O parâmetro **-o** foi removido da utilidade do banco de dados trivial agrupado **onode** (CTDB).
- O Samba agora usa a biblioteca GnuTLS para criptografia. Como resultado, se o modo FIPS no RHEL estiver habilitado, o Samba está em conformidade com a norma FIPS.
- O serviço **ctdbd** agora registra quando utiliza mais de 90% de uma linha de CPU.
- O suporte Python 2 depreciado foi removido.

O Samba atualiza automaticamente seus arquivos de banco de dados **tdb** quando o serviço **smbd**, **nmbd**, ou **winbind** é iniciado. Faça o backup dos arquivos do banco de dados antes de iniciar o Samba. Note que a Red Hat não suporta o downgrade dos arquivos de banco de dados **tdb**.

Para mais informações sobre mudanças notáveis, leia as notas de lançamento a montante antes de atualizar: <https://www.samba.org/samba/history/samba-4.11.0.html>

(BZ#1754409)

Servidor de Diretório rebaseado para a versão 1.4.2.4

Os pacotes **389-ds-base** foram atualizados para a versão upstream 1.4.2.4, que fornece uma série de correções e melhorias de bugs em relação à versão anterior. Para uma lista completa de mudanças notáveis, leia as notas de lançamento upstream antes de atualizar:

- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-4.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-3.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-2.html>
- <https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-1.html>

(BZ#1748994)

Alguns scripts legados foram substituídos no Directory Server

Este aprimoramento fornece substitutos para os scripts legados **dbverify**, **validate-syntax.pl**, **cl-dump.pl**, **fixup-memberuid.pl** e **repl-monitor.pl** não suportados no Directory Server. Estes scripts foram substituídos com os seguintes comandos:

- **dbverify**: `dsctl instance_name dbverify`
- **validate-syntax.pl**: `dsconf schema validate-syntax`
- **cl-dump.pl**: `dsconf replicação dsconf dump-changelog`
- **fixup-memberuid.pl**: `dsconf plugin posix-winsync fixup`
- **repl-monitor.pl**: `monitor de replicação dsconf`

Para uma lista de todos os scripts legados e suas substituições, veja [utilitários de linha de comando substituídos no Red Hat Directory Server 11](#).

(BZ#1739718)

A criação do IdM como uma réplica oculta é agora totalmente suportada

O Gerenciamento de Identidade (IdM) no RHEL 8.2 suporta totalmente a configuração de servidores IdM como réplicas ocultas. Uma réplica oculta é um servidor IdM que tem todos os serviços funcionando e disponíveis. Entretanto, ela não é anunciada para outros clientes ou masters porque não existem registros **SRV** para os serviços no DNS, e as funções do servidor LDAP não estão habilitadas. Portanto, os clientes não podem usar a descoberta de serviços para detectar réplicas ocultas.

As réplicas ocultas são projetadas principalmente para serviços dedicados que de outra forma podem perturbar os clientes. Por exemplo, um backup completo da IdM requer o encerramento de todos os serviços da IdM no master ou réplica. Como nenhum cliente usa uma réplica oculta, os administradores podem fechar temporariamente os serviços neste host sem afetar nenhum cliente. Outros casos de uso incluem operações de alta carga na API do IdM ou no servidor LDAP, tais como uma importação em massa ou consultas extensivas.

Para instalar uma nova réplica oculta, use o comando **ipa-replica-install --hidden-replica**. Para alterar o estado de uma réplica existente, use o comando **ipa server-state**.

Para mais detalhes, consulte [Instalando uma réplica oculta da IdM](#).

(BZ#1719767)

A política de bilhetes Kerberos agora suporta indicadores de autenticação

Os indicadores de autenticação são anexados aos bilhetes Kerberos com base nos quais o mecanismo de pré-autenticação foi usado para adquirir o bilhete:

- **otp** para autenticação de dois fatores (senha OTP)
- **raio** para autenticação RADIUS
- **pkinit** para PKINIT, cartão inteligente ou autenticação de certificado
- **endurecido** para senhas endurecidas (SPAKE ou FAST)

O Centro de Distribuição Kerberos (KDC) pode aplicar políticas tais como controle de acesso a serviços, duração máxima do bilhete e idade máxima renovável, nos pedidos de bilhetes de serviço que se baseiam nos indicadores de autenticação.

Com este aprimoramento, os administradores podem obter um controle mais preciso sobre a emissão de tickets de serviço, exigindo indicadores específicos de autenticação dos tickets de um usuário.

(BZ#1777564)

O pacote **krb5** agora está em conformidade com o FIPS

Com este aprimoramento, a criptografia não conforme é proibida. Como resultado, os administradores podem usar Kerberos em ambientes regulados por FIPS.

(BZ#1754690)

O servidor de diretório define o parâmetro **sslVersionMin** com base na política de criptografia de todo o sistema

Por padrão, o Directory Server agora define o valor do parâmetro **sslVersionMin** com base na política de criptografia do sistema. Se você definir o perfil da política de criptografia no arquivo **/etc/crypto-policies/config** para:

- **DEFAULT, FUTURO**, ou **FIPS**, Conjuntos de Servidores de Diretório **sslVersionMin** para **TLS1.2**
- **LEGACY**, Servidor de Diretório define **sslVersionMin** para **TLS1.0**

Alternativamente, você pode definir manualmente o **sslVersionMin** para um valor mais alto do que o definido na política criptográfica:

```
# dsconf -D |"cn=Directory Manager" __ldap://server.example.com__ conjunto de segurança --tls-protocol-min TLS1.3
```

(BZ#1828727)

O SSSD agora impõe por padrão os GPO AD

A configuração padrão para a opção SSSD **ad_gpo_access_control** está agora **fazendo cumprir**. No RHEL 8, o SSSD aplica por padrão as regras de controle de acesso baseadas nos Objetos de Políticas de Grupos de Diretórios Ativos (GPOs).

A Red Hat recomenda garantir que os GPOs sejam configurados corretamente no Active Directory antes de atualizar de RHEL 7 para RHEL 8. Se você não quiser reforçar os GPOs, altere o valor da opção **ad_gpo_access_control** no arquivo **/etc/sss/sss.conf** para **permissivo**.

(JIRA:RHELPLAN-51289)

5.13. DESKTOP

A Wayland agora está habilitada em sistemas dual-GPU

Anteriormente, o ambiente do GNOME era padronizado para a sessão **X11** em laptops e outros sistemas que possuem duas unidades de processamento gráfico (GPUs). Com este lançamento, o GNOME agora tem como padrão a sessão **Wayland** nos sistemas dual-GPU, que é o mesmo comportamento que nos sistemas single-GPU.

(BZ#1749960)

5.14. INFRA-ESTRUTURAS GRÁFICAS

Suporte para novas placas gráficas

As seguintes placas gráficas são agora suportadas:

- Intel HD Graphics 610, 620, e 630, que são encontrados com os processadores Intel Comet Lake H e U
- Intel Ice Lake UHD Graphics 910 e Iris Plus Graphics 930, 940, e 950.
Você não precisa mais definir a opção **alpha_support** kernel para permitir o suporte aos gráficos da Intel Ice Lake.
- A família AMD Navi 10, que inclui os seguintes modelos:
 - Radeon RX 5600
 - Radeon RX 5600 XT
 - Radeon RX 5700

- Radeon RX 5700 XT
- Radeon Pro W5700
- A família Nvidia Turing TU116, que inclui os seguintes modelos.
Note que o **novo** driver gráfico ainda não suporta aceleração 3D com a família Nvidia Turing TU116.
 - GeForce GTX 1650 Super
 - GeForce GTX 1660
 - GeForce GTX 1660 Super
 - GeForce GTX 1660 Ti
 - GeForce GTX 1660 Ti Max-Q

Além disso, os seguintes drivers gráficos foram atualizados:

- O motorista Matrox **mgag2000**
- O motorista Aspeed **ast** driver
- O driver Intel **i915**

(JIRA:RHELPLAN-41384)

5.15. O CONSOLE WEB

Os administradores podem agora usar certificados de clientes para autenticar no console web RHEL 8

Com este aperfeiçoamento do console web, um administrador de sistema pode usar certificados de cliente para acessar um sistema RHEL 8 localmente ou remotamente, usando um navegador com autenticação de certificados embutida. Nenhum software cliente adicional é necessário. Estes certificados são normalmente fornecidos por um cartão inteligente ou Yubikey, ou podem ser importados para o navegador.

Ao fazer o login com um certificado, o usuário não pode atualmente realizar ações administrativas no console web. Mas o usuário pode realizá-las na página do Terminal com o comando **sudo** após autenticar-se com uma senha.

(JIRA:RHELPLAN-2507)

Opção de login no console web com um certificado de cliente TLS

Com esta atualização, é possível configurar o console web para fazer o login com um certificado de cliente TLS que é fornecido por um navegador ou um dispositivo como um cartão inteligente ou um YubiKey.

(BZ#1678465)

Mudanças no login do console web

O console web RHEL foi atualizado com as seguintes mudanças:

- O console web fará o logout automático de sua sessão atual após 15 minutos de inatividade. Você pode configurar o tempo limite em minutos no arquivo **/etc/cockpit/cockpit.conf**.
- Da mesma forma que o SSH, o console web pode agora opcionalmente mostrar o conteúdo dos arquivos de banner na tela de login. Os usuários precisam configurar a funcionalidade no arquivo **/etc/cockpit/cockpit.conf**.

Consulte a página do manual **cockpit.conf(5)** para mais informações.

(BZ#1754163)

O console web RHEL foi redesenhado para usar o sistema de design da interface de usuário PatternFly 4

O novo design oferece melhor acessibilidade e combina com o design do OpenShift 4. As atualizações incluem:

- A página Visão Geral foi completamente redesenhada. Por exemplo, as informações são agrupadas em painéis mais fáceis de entender, as informações de saúde são mais proeminentes, os gráficos de recursos foram movidos para sua própria página, e a página de informações de hardware agora é mais fácil de encontrar.
- Os usuários podem usar o novo campo Pesquisar no menu Navegação para encontrar facilmente páginas específicas que são baseadas em palavras-chave.

Para mais informações sobre o PatternFly, consulte a página do [projeto PatternFly](#).

(BZ#1784455)

Atualizações da página de Máquinas Virtuais

A página de **Máquinas Virtuais** do console web obteve várias melhorias em termos de armazenamento:

- A criação de volume de armazenamento agora funciona para todos os tipos suportados por libvirt.
- Os pools de armazenamento podem ser criados em LVM ou iSCSI.

Além disso, a página de **máquinas virtuais** agora suporta a criação e remoção de interfaces de rede virtuais.

(BZ#1676506, BZ#1672753)

Atualizações da página de armazenamento do console Web

Os testes de usabilidade mostraram que o conceito *default mount point* na página de **armazenamento** do console web RHEL era difícil de entender, e levou a muita confusão. Com esta atualização, o console web não oferece mais uma opção *Default* ao montar um sistema de arquivo. A criação de um novo sistema de arquivo agora requer sempre um ponto de montagem especificado.

Além disso, o console web agora esconde a distinção entre a configuração (**/etc/fstab**) e o estado de tempo de execução (**/proc/mounts**). As mudanças feitas no console web sempre se aplicam tanto à configuração quanto ao estado de tempo de execução. Quando a configuração e o estado de tempo de execução diferem um do outro, o console web mostra um aviso e permite que os usuários os tragam de volta facilmente em sincronia.

(BZ#1784456)

5.16. VIRTUALIZAÇÃO

A tentativa de criar uma máquina virtual RHEL a partir de uma árvore instalada agora retorna uma mensagem de erro mais útil.

As máquinas virtuais RHEL 7 e RHEL 8 criadas usando o utilitário **virt-install** com a opção **--location** em alguns casos não inicializam. Esta atualização adiciona uma mensagem de erro de instalação **vir-install** que fornece instruções sobre como contornar este problema.

(BZ#1677019)

Processadores Intel Xeon Platinum série 9200 suportados por convidados da KVM

O suporte para processadores Intel Xeon Platinum série 9200 (anteriormente conhecido como **Cascade Lake**) foi agora adicionado ao hipervisor KVM e ao código do kernel, e ao libvirt API. Isto permite que as máquinas virtuais KVM utilizem processadores Intel Xeon Platinum série 9200.

(JIRA:RHELPLAN-13995)

EDK2 rebaseado para a versão estável201908

O pacote **EDK2** foi atualizado para a versão **stable201908**, que oferece vários aprimoramentos. Notadamente:

- **EDK2** agora inclui suporte para OpenSSL-1.1.1.
- Para cumprir as exigências de licenciamento do projeto upstream, a licença do pacote **EDK2** foi alterada de **BSD e OpenSSL e MIT** para **BSD-2-Clause-Patent e OpenSSL e MIT**.

(BZ#1748180)

Criando máquinas virtuais aninhadas

Com esta atualização, a virtualização aninhada é totalmente suportada para máquinas virtuais KVM (VMs) rodando em um host Intel 64 com RHEL 8. Com este recurso, uma RHEL 7 ou RHEL 8 VM que roda em um host RHEL 8 físico pode atuar como um hipervisor, e hospedar suas próprias VMs.

Observe que nos sistemas AMD64, a virtualização KVM aninhada continua sendo uma Visão Tecnológica Prevista.

(JIRA:RHELPLAN-14047, JIRA:RHELPLAN-24437)

5.17. CONTÊINERES

A lista de busca padrão de registros em **/etc/containers/registries.conf** foi atualizada

A lista padrão de **registros.search** em **/etc/containers/registries.conf** foi atualizada para incluir apenas registros confiáveis que fornecem imagens de contêineres curados, corrigidos e mantidos pela Red Hat e seus parceiros.

A Red Hat recomenda sempre o uso de nomes de imagens totalmente qualificados, inclusive:

- O servidor de registro (nome DNS completo)
- Namespace
- Nome da imagem

- Tag (por exemplo **register.redhat.io/ubi8/ubu:latest**)

Ao utilizar nomes curtos, há sempre um risco inerente de falsificação. Por exemplo, um usuário quer tirar uma imagem chamada **foobar** de um registro e espera que ela venha do **myregistry.com**. Se o **myregistry.com** não for o primeiro na lista de busca, um atacante pode colocar uma imagem **foobar** diferente em um registro mais cedo na lista de busca. O usuário puxaria e executaria acidentalmente a imagem e o código do atacante, em vez do conteúdo pretendido. A Red Hat recomenda apenas adicionar registros que sejam confiáveis, ou seja, registros que não permitam que usuários desconhecidos ou anônimos criem contas com nomes arbitrários. Isto evita que uma imagem seja falsificada, agachada ou tornada insegura de outra forma.

(BZ#1810053)

Podman não depende mais do gancho do sistema ocito-gancho

Podman não precisa ou depende do pacote de **gancho do sistema Oci** que foi removido do módulo **container-tools:rhel8** e **container-tools:2.0**.

(BZ#1645280)

CAPÍTULO 6. MUDANÇAS IMPORTANTES NOS PARÂMETROS DO KERNEL EXTERNO

Este capítulo fornece aos administradores de sistemas um resumo das mudanças significativas no kernel distribuído com o Red Hat Enterprise Linux 8.2. Estas mudanças incluem entradas **proc** adicionadas ou atualizadas, valores default **sysctl** e **sysfs**, parâmetros de inicialização, opções de configuração do kernel ou quaisquer mudanças perceptíveis de comportamento.

6.1. NOVOS PARÂMETROS DO KERNEL

cpuidle.governor = [CPU_IDLE]

Nome do governador do **cpuidle** a ser usado.

deferred_probe_timeout = [KNL]

Este é um parâmetro de depuração para definir um tempo limite em segundos para que a sonda diferida desista de aguardar as dependências para sondar.

Somente as dependências específicas (subsistemas ou motoristas) que optaram por entrar serão ignoradas. Um timeout de 0 será timeout no final dos **initcalls**. Este parâmetro também descarta os dispositivos ainda na lista de sondas diferidas após nova tentativa.

kvm.nx_huge_pages = [KVM]

Este parâmetro controla o funcionamento do software para o bug **X86_BUG_ITLB_MULTIHIT**.

As opções são:

- **força** - Sempre implantar workaround.
- **desligados** - Nunca implante trabalho de volta.
- **auto** (default) - Implantar workaround baseado na presença de **X86_BUG_ITLB_MULTIHIT**.

Se o software estiver habilitado para o anfitrião, os hóspedes não precisam habilitá-lo para os hóspedes aninhados.

kvm.nx_huge_pages_recovery_ratio = [KVM]

Este parâmetro controla quantas páginas de 4KiB são periodicamente zappingadas de volta para páginas enormes. O desativa a recuperação, caso contrário, se o valor for N, a Máquina Virtual baseada no Kernel (KVM) fará zap 1/Nth das páginas de 4KiB a cada minuto. O valor padrão é 60.

page_alloc.shuffle = [KNL]

Bandeira booleana para controlar se o alocador de páginas deve randomizar suas listas livres.

A randomização pode ser ativada automaticamente se o kernel detectar que está sendo executado em uma plataforma com um cache de memória mapeado diretamente no lado da memória. Este parâmetro pode ser usado para sobrepor/desabilitar esse comportamento.

O estado da bandeira pode ser lido a partir do pseudo sistema de arquivos **sysfs** do arquivo **/sys/module/page_alloc/parameters/shuffle**.

panic_print =

Máscara de bits para informações sobre o sistema de impressão quando o pânico acontece.

O usuário pode escolher a combinação das seguintes partes:

- bit 0: imprimir todas as informações de tarefas

- bit 1: informações sobre a memória do sistema de impressão
- bit 2: informações sobre o temporizador de impressão
- bit 3: imprimir informações sobre bloqueios se a configuração do kernel **CONFIG_LOCKDEP** estiver ligada
- bit 4: imprimir o buffer **ftrace**
- bit 5: imprimir todas as mensagens **impressas** em buffer

rcutree.sysrq_rcu = [KNL]

Comandeer uma chave **sysrq** para descarregar a árvore **rcu_node** da Tree RCU com um olho para determinar porque um novo período de carência ainda não começou.

rcutorture.fwd_progress = [KNL]

Habilitar a atualização de leitura-cópia (RCU) do período de carência para teste de progresso para os tipos de RCU que suportam esta noção.

rcutorture.fwd_progress_div = [KNL]

Especifique a fração de um período de aviso de instalação de CPU para fazer testes de avanço de loop apertado.

rcutorture.fwd_progress_holdoff = [KNL]

Número de segundos para esperar entre os sucessivos testes de avanço.

rcutorture.fwd_progress_need_resched = [KNL]

Encerre as chamadas **cond_resched()** dentro das verificações de **necessidade_resched()** durante os testes de avanço de loop apertado.

tsx = [X86]

Este parâmetro controla o recurso de Extensões de Sincronização Transacional (TSX) nos processadores Intel que suportam o controle TSX.

As opções são:

- **on** - Habilitar o TSX no sistema. Embora haja atenuações para todas as vulnerabilidades de segurança conhecidas, o TSX acelerou vários CVEs anteriores relacionados à especulação. Como resultado, pode haver riscos de segurança desconhecidos associados a deixá-lo habilitado.
- **desligado** - Desabilite o TSX no sistema. Esta opção tem efeito somente em CPUs mais novas que não são vulneráveis à Amostragem de Dados Microarquitetônicos (MDS). Em outras palavras, eles têm **MSR_IA32_ARCH_CAPABILITIES.MDS_NO=1** e recebem o novo registro específico do Modelo **IA32_TSX_CTRL** (MSR) através de uma atualização do microcódigo. Este novo MSR permite uma desativação confiável da funcionalidade do TSX.
- **auto** - Desative o TSX se **X86_BUG_TAA** estiver presente, caso contrário, habilite o TSX no sistema.

A não especificação deste parâmetro é equivalente a **tsx=off**.

Para obter detalhes, consulte a [documentação do núcleo](#) a montante.

tsx_async_abort = [X86,INTEL]

Este parâmetro controla a mitigação da vulnerabilidade do TSX Async Abort (TAA).

Semelhante ao MDS (Micro-architectural Data Sampling), certas CPUs que suportam Extensões de Sincronização Transacional (TSX) são vulneráveis a uma exploração contra buffers internos de CPU. O exploit é capaz de encaminhar informações para um gadget de divulgação sob certas condições.

Em processadores vulneráveis, os dados enviados especulativamente podem ser usados em um ataque de canal lateral de cache, para acessar dados aos quais o atacante não tem acesso direto.

As opções são:

- **total** - Habilitar a mitigação do TAA em CPUs vulneráveis se o TSX estiver habilitado.
- **full,nosmt** - Habilitar a mitigação do TAA e desabilitar a Multi-Tarefa Simultânea (SMT) em CPUs vulneráveis. Se o TSX estiver desativado, o SMT não está desativado porque a CPU não é vulnerável a ataques de TAA cruzados.
- **off** - Desabilitar incondicionalmente a mitigação do TAA.
Em máquinas afetadas pelo MDS, o parâmetro **tsx_async_abort=off** pode ser evitado por uma mitigação ativa do MDS, uma vez que ambas as vulnerabilidades são mitigadas com o mesmo mecanismo. Portanto, para desativar esta mitigação, é necessário especificar também o parâmetro **mds=off**.

Não especificar esta opção é equivalente a **tsx_async_abort=full**. Nas CPUs que são MDS afetadas e implantam a mitigação MDS, a mitigação TAA não é necessária e não fornece nenhuma mitigação adicional.

Para obter detalhes, consulte a [documentação do núcleo](#) a montante.

6.2. PARÂMETROS DE KERNEL ATUALIZADOS

intel_iommu = [DMAR]

Remapping de Acesso Direto à Memória Intel IOMMU (DMAR).

As opções são:

- **sm_on** [Default Off] - Por padrão, o modo escalável será desativado mesmo se o hardware anunciar que tem suporte para a tradução do modo escalável. Com esta opção definida, o modo escalável será usado no hardware que afirma ter suporte a ele.

isolcpus = [KNL,SMP,ISOL]

Este parâmetro isola um determinado conjunto de CPUs de distúrbios.

- **managed_irq** - Um sub-parâmetro, que impede que as CPUs isoladas sejam alvo de interrupções gerenciadas, que têm uma máscara de interrupção contendo CPUs isoladas. A afinidade das interrupções gerenciadas é tratada pelo kernel e não pode ser alterada através das interfaces **/proc/irq/***.
Este isolamento é o melhor esforço e só é eficaz se a máscara de interrupção automaticamente atribuída de uma fila de dispositivos contiver CPUs isoladas e domésticas. Se as CPUs domésticas estiverem on-line, tais interrupções são direcionadas para a CPU doméstica de modo que as E/S apresentadas na CPU doméstica não possam perturbar a CPU isolada.

Se a máscara de afinidade da fila contém apenas CPUs isoladas, então este parâmetro não tem efeito sobre a decisão de roteamento de interrupção. Entretanto, as interrupções só são entregues quando as tarefas executadas nessas CPUs isoladas apresentam E/S. As E/S submetidas nas CPUs domésticas não têm influência sobre essas filas.

mds = [X86,INTEL]

As mudanças nas opções:

- **off** - Nas máquinas TSX Async Abort (TAA)-afectadas, **mds=off** pode ser prevenido por uma mitigação ativa do TAA, pois ambas as vulnerabilidades são mitigadas com o mesmo mecanismo. Portanto, para desativar esta mitigação, é necessário especificar também o parâmetro **tsx_async_abort=off** kernel.

A não especificação deste parâmetro é equivalente a **mds=full**.

Para obter detalhes, consulte a [documentação do núcleo](#) a montante.

mem_encrypt = [X86-64]

Controle de Criptografia de Memória Segura AMD (SME)

...

Para detalhes sobre quando a criptografia da memória pode ser ativada, consulte a [documentação do kernel](#) a montante.

mitigações =

As mudanças nas opções:

- **off** - Desativar todas as atenuações opcionais da CPU. Isto melhora o desempenho do sistema, mas também pode expor os usuários a várias vulnerabilidades da CPU. Equivalente a:

- **nopti [X86,PPC]**
- **kpti=0 [ARM64]**
- **nospectre_v1 [X86,PPC]**
- **nobp=0 [S390]**
- **nospectre_v2 [X86,PPC,S390,ARM64]**
- **spectre_v2_user=off [X86]**
- **spec_store_bypass_disable=off [X86,PPC]**
- **ssbd=force-off [ARM64]**
- **l1tf=off [X86]**
- **mds=off [X86]**
- **tsx_async_abort=off [X86]**
- **kvm.nx_huge_pages=off [X86]**

Exceções:

Isto não tem nenhum efeito sobre **kvm.nx_huge_pages** quando **kvm.nx_huge_pages=force**.

- **auto,nosmt** - Atenuar todas as vulnerabilidades da CPU, desativando o Multi Threading Simultâneo (SMT), se necessário. Esta opção é para usuários que sempre querem ser totalmente mitigados, mesmo que isso signifique a perda do SMT.

Equivalente a:

- **l1tf=flush,nosmt [X86]**
- **mds=full,nosmt [X86]**
- **tsx_async_abort=full,nosmt [X86]**

rcutree.jiffies_till_sched_qs = [KNL]

Este parâmetro define a idade requerida em jiffies para um determinado período de carência antes que a Read-copy update (RCU) comece a solicitar ajuda de estado quiescente das funções **rcu_note_context_switch()** e **cond_resched()**. Se não especificado, o kernel calculará um valor baseado nas configurações mais recentes do **rcutree.jiffies_till_first_fqs** e **rcutree.jiffies_till_next_fqs** parâmetros do kernel.

Este valor calculado pode ser visualizado no parâmetro **rcutree.jiffies_to_sched_qs** kernel. Qualquer tentativa de definir **rcutree.jiffies_to_sched_qs** será sobregravada.

tsc =

Este parâmetro desativa a verificação da estabilidade da fonte do relógio para o contador de carimbo de tempo (TSC).

Formato: <string>

As opções são:

- **confiável** [x86] - Marca a fonte dos relógios TSC como confiável. Esta opção desativa a verificação da fonte do relógio em tempo de execução, assim como as verificações de estabilidade feitas na inicialização. A opção também habilita o modo temporizador de alta resolução em hardware mais antigo, e em ambiente virtualizado.
- **noirqtime** [x86] - Não utilizar o TSC para fazer a contabilidade de Pedido de Interrupção (IRQ). Usado para executar a contabilização **IRQ_TIME_ACCOUNTING** em qualquer plataforma onde o Read Time-Stamp Counter (RDTSC) é lento e esta contabilização pode adicionar despesas gerais.
- **instável** [x86] - Marca a fonte dos relógios TSC como instável. Esta opção marca o TSC incondicionalmente instável na inicialização e evita qualquer oscilação adicional quando o cão de guarda do TSC notar.
- **nowatchdog** [x86] - Desativa o cão de guarda da fonte dos relógios. A opção é usada em situações com requisitos rigorosos de latência, onde as interrupções do cão de guarda-relógio não são aceitáveis.

6.3. NOVOS PARÂMETROS /PROC/SYS/KERNEL

panic_print

Bitmask para imprimir as informações do sistema quando ocorre o pânico.

O usuário pode escolher a combinação das seguintes partes:

- bit 0: imprimir todas as informações de tarefas
- bit 1: informações sobre a memória do sistema de impressão

- bit 2: informações sobre o temporizador de impressão
- bit 3: imprimir informações sobre bloqueios se o item de configuração do kernel **CONFIG_LOCKDEP** estiver ligado
- bit 4: tampão de impressão **ftrace**
Por exemplo, para imprimir tarefas e informações de memória sobre o pânico, executar:

```
# echo 3 > /proc/sys/kernel/panic_print
```

agenda_energia_consciente

Este parâmetro habilita ou desabilita a Programação Consciente de Energia (EAS).

O EAS começa automaticamente em plataformas com topologias de CPU assimétricas que têm um Modelo Energético disponível.

Se sua plataforma atende aos requisitos da EAS, mas você não quer utilizá-la, altere este valor para 0.

6.4. PARÂMETROS ATUALIZADOS /PROC/SYS/KERNEL

roscas-max

Este parâmetro controla o número máximo de roscas que a função **garfo()** pode criar.

Durante a inicialização, o núcleo define este valor de tal forma que mesmo que o número máximo de fios seja criado, as estruturas de fios ocupam apenas uma parte (1/8º) das páginas de RAM disponíveis.

O valor mínimo que pode ser escrito em **roscas-max** é 1. O valor máximo é dado pela constante **FUTEX_TID_MASK (0x3fffffff)**.

Se um valor fora deste intervalo for escrito em **roscas-máximo**, ocorre um erro **EINVAL**.

6.5. PARÂMETROS ATUALIZADOS /PROC/SYS/NET

bpf_jit_enable

Este parâmetro habilita o compilador **Berkeley Packet Filter Just-in-Time (BPF JIT)**

BPF é uma infra-estrutura flexível e eficiente que permite a execução de bytecode em vários pontos de gancho. Ela é utilizada em vários subsistemas de kernel Linux, como rede (por exemplo **XDP, tc**), rastreamento (por exemplo, **kprobes, uprobes, tracepoints**) e segurança (por exemplo, **seccomp**).

LLVM tem um back-end **BPF** que pode compilar C restrito em uma seqüência de **BPF** instruções. Depois de carregar o programa através da chamada ao sistema **bpf()** e passar um verificador no kernel, **JIT** traduzirá então estes programas **BPF** em instruções nativas da CPU.

Há dois sabores de **JIT**, o mais novo **eBPF JIT** é atualmente suportado nas seguintes arquiteturas de CPU:

- **x86_64**
- **braço64**
- **ppc64** (tanto pequenos como grandes endidos)

- **s390x**

CAPÍTULO 7. DRIVERS DE DISPOSITIVOS

Este capítulo fornece uma lista abrangente de todos os drivers de dispositivos que são novos ou que foram atualizados no Red Hat Enterprise Linux 8.2.

7.1. NOVOS MOTORISTAS

Drivers de rede

- gVNIC Motorista (gve.ko.xz)
- Broadcom UniMAC MDIO controlador de ônibus (mdio-bcm-unimac.ko.xz)
- Software iWARP Driver (siw.ko.xz)

Drivers gráficos e drivers diversos

- Auxiliares de gerenciamento de memória DRM VRAM (drm_vram_helper.ko.xz)
- condutor de cpuidle para haltpoll governor (cpuidle-haltpoll.ko.xz)
- stm_ftrace driver (stm_ftrace.ko.xz)
- stm_console driver (stm_console.ko.xz)
- Classe do dispositivo System Trace Module (stm_core.ko.xz)
- dispositivo dummy_stm (dummy_stm.ko.xz)
- stm_heartbeat driver (stm_heartbeat.ko.xz)
- Intel® Trace Hub Global Trace Hub driver (intel_th_gth.ko.xz)
- Driver de saída Intel® Trace Hub PTI/LPP (intel_th_pti.ko.xz)
- Driver do controlador Intel® Trace Hub (intel_th.ko.xz)
- Driver da unidade de armazenamento de memória Trace Hub Intel® (intel_th_msu.ko.xz)
- Software Intel® Trace Hub driver Trace Hub (intel_thh_sth.ko.xz)
- Unidade de armazenamento de memória Intel® Trace Hub (intel_th_msu_sink.ko.xz)
- Controlador Intel® Trace Hub PCI (intel_th_pci.ko.xz)
- Controlador Intel® Trace Hub ACPI (intel_th_acpi.ko.xz)
- Driver MC para processadores de servidores Intel 10nm (i10nm_edac.ko.xz)
- Dispositivo DAX: dispositivo de mapeamento de acesso direto (dax_pmem_core.ko.xz)
- PMEM DAX: acesso direto à memória persistente (dax_pmem.ko.xz)
- PMEM DAX: suporta a interface depreciada /sys/class/dax (dax_pmem_compat.ko.xz)
- Plataforma Intel PMC Core init (intel_pmc_core_pltdrv.ko.xz)

- Controle Intel RAPL (Running Average Power Limit) via interface MSR (intel_rapl_msr.ko.xz)
- Intel Runtime Average Power Limit (RAPL) código comum (intel_rapl_common.ko.xz)

Drivers de armazenamento

- Suporte de agrupamento para MD (md-cluster.ko.xz)

7.2. DRIVERS ATUALIZADOS

Atualizações de driver de rede

- O driver virtual NIC VMware vmxnet3 (vmxnet3.ko.xz) foi atualizado para a versão 1.4.17.0-k.
- O driver Intel® 10 Gigabit Virtual Function Network Driver (ixgbevf.ko.xz) foi atualizado para a versão 4.1.0-k-rh8.2.0.
- O Intel® 10 Gigabit PCI Express Network Driver (ixgbe.ko.xz) foi atualizado para a versão 5.1.0-k-rh8.2.0.
- O driver Intel® Ethernet Connection E800 Series Linux (ice.ko.xz) foi atualizado para a versão 0.8.1-k.
- O controlador Netronome Flow Processor (NFP) (nfp.ko.xz) foi atualizado para a versão 4.18.0-185.el8.x86_64.
- O Adaptador de Rede Elástica (ENA) (ena.ko.xz) foi atualizado para a versão 2.1.0K.

Atualizações gráficas e de drivers diversos

- HPE watchdog driver (hpwdt.ko.xz) foi atualizado para a versão 2.0.3.
- O driver Intel I/OAT DMA Linux (ioatdma.ko.xz) foi atualizado para a versão 5.00.

Atualizações do driver de armazenamento

- Driver for HPE Smart Array Controller (hpsa.ko.xz) foi atualizado para a versão 3.4.20-170-RH4.
- O LSI MPT Fusion SAS 3.0 Device Driver (mpt3sas.ko.xz) foi atualizado para a versão 32.100.00.00.
- O QLogic FCoE Driver (bnx2fc.ko.xz) foi atualizado para a versão 2.12.10.
- O driver SCSI Emulex LightPulse Fibre Channel (lpfc.ko.xz) foi atualizado para a versão 0:12.6.0.2.
- O módulo QLogic FastLinQ 4xxxx FCoE (qedf.ko.xz) foi atualizado para a versão 8.42.3.0.
- O QLogic Fibre Channel HBA Driver (qla2xxx.ko.xz) foi atualizado para a versão 10.01.00.21.08.2-k.
- Driver para a versão Microsemi Smart Family Controller (smartpqi.ko.xz) foi atualizado para a versão 1.2.10-025.
- QLogic FastLinQ 4xxxx iSCSI Module (qedf.ko.xz) foi atualizado para a versão 8.37.0.20.

- Broadcom MegaRAID SAS Driver (megaraid_sas.ko.xz) foi atualizado para a versão 07.710.50.00-rc1.

CAPÍTULO 8. CORREÇÃO DE ERROS

Esta parte descreve os bugs corrigidos no Red Hat Enterprise Linux 8.2 que têm um impacto significativo sobre os usuários.

8.1. INSTALADOR E CRIAÇÃO DE IMAGEM

O uso dos parâmetros de inicialização da `versão` ou `inst.version` kernel não pára mais o programa de instalação

Anteriormente, a inicialização do programa de instalação a partir da linha de comando do kernel utilizando os parâmetros de inicialização da `versão` ou `inst.version` imprimiu a versão, por exemplo, **anaconda 30.25.6**, e parou o programa de instalação.

Com esta atualização, a `versão` e os parâmetros `inst.version` são ignorados quando o programa de instalação é inicializado a partir da linha de comando do kernel, e como resultado, o programa de instalação não é interrompido.

(BZ#1637472)

Suporte de inicialização segura para s390x no instalador

Anteriormente, a RHEL 8.1 fornecia suporte para preparar discos de inicialização para uso em ambientes IBM Z que forçavam o uso de inicialização segura. As capacidades do servidor e do hipervisor utilizados durante a instalação determinavam se o formato resultante no disco continha suporte de inicialização segura. Não havia maneira de influenciar o formato on-disk durante a instalação. Conseqüentemente, se você instalou o RHEL 8.1 em um ambiente que suportava boot seguro, o sistema não foi capaz de inicializar quando movido para um ambiente que não tinha suporte de boot seguro, como é feito em alguns cenários de failover.

Com esta atualização, você pode agora configurar a opção de inicialização segura da ferramenta **zipl**. Para fazer isso, você pode usar qualquer uma das duas:

- O comando Kickstart **zipl** e uma de suas opções, por exemplo: **--botão seguro**, **--botão sem segurança**, e **--botão com força segura**.
- Da janela **Resumo da Instalação** na GUI, você pode selecionar o **Sistema > Destino da Instalação > Resumo completo do disco e link do carregador de inicialização** e configurar o dispositivo de inicialização. Como resultado, a instalação pode agora ser inicializada em ambientes que não possuem suporte de inicialização seguro.

(BZ#1659400)

O recurso de boot seguro está agora disponível

Anteriormente, o valor padrão para a opção `secure=` boot não estava definido para **auto**, e como resultado, o recurso de boot seguro não estava disponível. Com esta atualização, a menos que previamente configurado, o valor padrão é definido para **auto**, e o recurso de boot seguro está agora disponível.

(BZ#1750326)

O arquivo `/etc/sysconfig/kernel` não faz mais referência ao script `new-kernel-pkg`

Anteriormente, o arquivo `/etc/sysconfig/kernel` referenciava o script `new-kernel-pkg`. Entretanto, o script do **novo kernel-pkg** não está incluído em um sistema RHEL 8. Com esta atualização, a referência ao script `new-kernel-pkg` foi removida do arquivo `/etc/sysconfig/kernel`.

(BZ#1747382)

A instalação não define mais do que o número máximo de dispositivos permitidos na variável **NVRAM do dispositivo de inicialização**

Anteriormente, o programa de instalação RHEL 8 definia mais do que o número máximo de dispositivos permitidos na variável **NVRAM do dispositivo de inicialização**. Como resultado, a instalação falhou em sistemas que possuíam mais do que o número máximo de dispositivos. Com esta atualização, o programa de instalação RHEL 8 agora verifica a configuração máxima do dispositivo e apenas adiciona o número permitido de dispositivos.

(BZ#1748756)

As instalações funcionam para um local de imagem que usa um comando URL em um arquivo Kickstart localizado em um local não-rede

Anteriormente, a instalação falhou no início do processo quando a ativação da rede acionada pela localização remota da imagem foi especificada por um comando URL em um arquivo Kickstart localizado em um local não-rede. Esta atualização corrige o problema e as instalações que fornecem o local da imagem usando um comando URL em um arquivo Kickstart que está localizado em um local não-rede, por exemplo, um CD-ROM ou um dispositivo de bloco local, agora funcionam como esperado.

(BZ#1649359)

O programa de instalação RHEL 8 verifica apenas ECKD DASD para dispositivos não formatados

Anteriormente, na verificação de dispositivos não formatados, o programa de instalação verificava todos os dispositivos DASD. Entretanto, o programa de instalação só deveria ter verificado os dispositivos DASD do ECKD. Como consequência, a instalação falhou com um traceback quando um dispositivo FBA DASD com SWAPGEN foi usado. Com esta atualização, o programa de instalação não verifica os dispositivos FBA DASD, e a instalação é concluída com sucesso.

(BZ#1715303)

8.2. GESTÃO DE SOFTWARE

yum repolist não termina mais no primeiro repositório indisponível

Anteriormente, a opção de configuração do repositório **Skip_if_una disponível** era, por padrão, definida como segue:

```
skip_if_unavailable=false
```

Esta configuração forçou o comando **yum repolist** a terminar no primeiro repositório indisponível com um erro e status de saída 1. Conseqüentemente, o **yum repolist** não continuou listando os repositórios disponíveis.

Com esta atualização, o **yum repolist** foi corrigido para não requerer mais nenhum download. Como resultado, o **yum repolist** não fornece nenhuma saída que requeira metadados, e o comando agora continua listando os repositórios disponíveis, como esperado.

Note que o número de pacotes disponíveis só é devolvido pelo **yum repolist --verbose** ou **yum repoinfo** que ainda requerem metadados disponíveis. Portanto, estes comandos terminarão no primeiro repositório indisponível.

(BZ#1697472)

8.3. CONCHAS E FERRAMENTAS DE LINHA DE COMANDO

Atualizações do ReaR

RHEL 8.2 introduz uma série de atualizações na utilidade Relax-and-Recover(**ReaR**).

O manuseio do diretório de construção foi alterado. Anteriormente, o diretório de construção era mantido em um local temporário no caso de **o ReaR** encontrar uma falha. Com esta atualização, o diretório de compilação é apagado por padrão em execuções não interativas para evitar o consumo de espaço em disco.

A semântica da variável de configuração **KEEP_BUILD_DIR** foi melhorada para incluir um novo valor de **erros**. A variável **KEEP_BUILD_DIR** pode ser definida para os seguintes valores:

- **erros** para preservar o diretório de construção sobre erros para depuração (o comportamento anterior)
- **y(verdadeiro)** para preservar sempre o diretório de construção
- **n(falso)** para nunca preservar o diretório de construção

O valor padrão é uma cadeia vazia com o significado de **erros** quando **o ReaR** está sendo executado interativamente (em um terminal) e **falso** se **o ReaR** estiver sendo executado não-interativamente. Note que **KEEP_BUILD_DIR** é automaticamente definido como **verdadeiro** no modo de depuração (**-d**) e no modo de depuração (**-D**); este comportamento não foi alterado.

Correções notáveis de erros incluem:

- O suporte para o NetBackup 8.0 foi fixado.
- **ReaR** não aborta mais com um erro de bash semelhante ao **xrealloc: não pode alocar** em sistemas com um grande número de usuários, grupos e usuários por grupo.
- O comando **bconsole** agora mostra sua rapidez, o que lhe permite realizar uma operação de restauração ao utilizar a integração Bacula.
- **O ReaR** agora faz o backup correto dos arquivos também em situações em que o serviço de **estivador** está em execução, mas nenhum diretório raiz do **estivador** foi definido, ou quando é impossível determinar o status do serviço de **estivador**.
- A recuperação não falha mais ao usar pools finos ou ao recuperar um sistema no Modo Migração.
- A reconstrução extremamente lenta dos **initramfs** durante o processo de recuperação com LVM foi corrigida.
- **ReaR** agora cria uma imagem ISO bootável funcional nas arquiteturas AMD e Intel 64 bits ao usar o bootloader UEFI. O boot de uma imagem de recuperação nesta configuração não mais aborta no Grub com a mensagem de erro **Desconhecido comando 'configfile' (...) Entrando no modo de recuperação....** O suporte ao GRUB_RESCUE nesta configuração, que anteriormente poderia falhar devido à falta de suporte ao sistema de arquivos XFS, também foi corrigido.

([BZ#1729501](#))

mlocate-updatedb.timer agora está habilitado durante a instalação do pacote **mlocate**

Anteriormente, a reindexação do banco de dados do arquivo não era realizada automaticamente, porque o **mlocate-updatedb.timer** era desativado após a instalação do pacote **mlocate**. Com esta atualização, o temporizador **mlocate-updatedb.timer** agora faz parte do arquivo **90-default.preset** e é habilitado por padrão após a instalação do pacote **mlocate**. Como resultado, o banco de dados do arquivo é atualizado automaticamente.

(BZ#1817591)

8.4. SERVIÇOS DE INFRA-ESTRUTURA

o dnsmasq agora trata corretamente as consultas DNS não recursivas

Anteriormente, o **dnsmasq** encaminhou todas as consultas não recursivas para um servidor upstream, o que levou a respostas diferentes. Com esta atualização, as consultas não recursivas a nomes conhecidos locais, tais como nomes de DHCP para locação de host ou hosts lidos do arquivo **/etc/hosts**, são tratadas pelo **dnsmasq** e não são encaminhadas a um servidor upstream. Como resultado, a mesma resposta às consultas recursivas a nomes conhecidos é devolvida.

(BZ#1700916)

dhclient não mais falha em renovar o endereço IP após mudanças no tempo do sistema

Anteriormente, se o tempo do sistema mudasse, o sistema poderia perder o endereço IP atribuído devido à remoção pelo kernel. Com esta atualização, o **dhclient** usa o temporizador monotônico para detectar saltos no tempo para trás e emite a mensagem **DHCPREQUEST** para extensão do aluguel em caso de salto descontínuo no tempo do sistema. Como resultado, o sistema não perde mais o endereço IP no cenário descrito.

(BZ#1729211)

ipcalc agora retorna o endereço de transmissão correto para as redes /31

Esta atualização corrige o utilitário **ipcalc** para seguir corretamente a norma RFC 3021. Como resultado, o **ipcalc** retorna o endereço de transmissão correto quando o prefixo **/31** é usado em uma interface.

(BZ#1638834)

/etc/services contém agora uma definição adequada do porto NRPE

Esta atualização adiciona a definição apropriada da porta de serviço Nagios Remote Plug-in Executor (NRPE) ao arquivo **/etc/services**.

(BZ#1730396)

O código de resolução DNS postfix agora usa res_search em vez de res_query

Após sua atualização anterior no **postfix**, o código resolvidor DNS usou a função **res_query** em vez da função **res_search**. Como consequência, o resolvidor DNS não procurou nomes de host nos domínios atual e pai com a seguinte configuração **postfix**:

```
# postconf -e "smtp_host_lookup = dns"
# postconf -e "smtp_dns_resolver_options = res_defnames, res_dnsrch"
```

Por exemplo, para:

```
# Post-onf -e "relayhost = [smtp]"
```

e o nome de domínio no formato *example.com*, o resolvedor DNS não utilizou o *smtp.example.com* servidor SMTP para retransmissão.

Com esta atualização, o código resolvedor DNS foi alterado para usar **res_search** em vez de **res_query**, e agora ele procura corretamente os nomes dos hosts nos domínios atual e pai.

([BZ#1723950](#))

PCRE, CDB, e SQLite agora podem ser usados com Postfix

No RHEL 8, o pacote **postfix** foi dividido em vários subpacotes, cada subpacote fornecendo um plug-in para um banco de dados específico. Anteriormente, os pacotes RPM contendo os plug-ins **postfix-pcre**, **postfix-cdb**, e **postfix-sqlite** não eram distribuídos. Consequentemente, bancos de dados com estes plug-ins não podiam ser usados com Postfix. Esta atualização adiciona pacotes RPM contendo os plug-ins PCRE, CDB, e SQLite ao repositório AppStream. Como resultado, estes plug-ins podem ser usados depois que o pacote RPM apropriado for instalado.

([BZ#1745321](#))

8.5. SEGURANÇA

fapolicyd não impede mais as atualizações da RHEL

Quando uma atualização substitui o binário de uma aplicação em execução, o kernel modifica o caminho binário da aplicação na memória anexando o sufixo " (excluído). Anteriormente, o daemon da política de acesso a arquivos **fapolicyd** tratava tais aplicações como não confiáveis, e as impedia de abrir e executar quaisquer outros arquivos. Como consequência, o sistema às vezes era incapaz de inicializar após a aplicação de atualizações.

Com o lançamento do [RHBA-2020:5243](#) advisory, **fapolicyd** ignora o sufixo no caminho binário para que o binário possa combinar com o banco de dados de confiança. Como resultado, **fapolicyd** aplica as regras corretamente e o processo de atualização pode terminar.

([BZ#1897091](#))

openssl-pkcs11 não trava mais os dispositivos ao tentar entrar em múltiplos dispositivos

Anteriormente, o motor **openssl-pkcs11** tentou entrar no primeiro resultado de uma busca usando o PKCS #11 URI fornecido e usou o PIN fornecido mesmo que o primeiro resultado não fosse o dispositivo pretendido e o PIN correspondesse a outro dispositivo. Estas tentativas de autenticação falhadas bloquearam o dispositivo.

openssl-pkcs11 agora tenta entrar em um dispositivo somente se o PKCS #11 URI fornecido corresponder somente a um único dispositivo. O motor agora falha intencionalmente caso a busca do PKCS #11 encontre mais de um dispositivo. Por esta razão, você deve fornecer um PKCS #11 URI que corresponda apenas a um único dispositivo quando usar o **openssl-pkcs11** para fazer o login no dispositivo.

([BZ#1705505](#))

OpenSCAP varreduras offline usando rpmverifyfile agora funcionam corretamente

Antes desta atualização, o scanner **OpenSCAP** não alterou corretamente o diretório de trabalho atual no modo offline, e a função **fchdir** não foi chamada com os argumentos corretos na sonda **OpenSCAP rpmverifyfile**. O scanner **OpenSCAP** foi corrigido para mudar corretamente o diretório de trabalho atual

em modo offline, e a função **fchdir** foi corrigida para usar os argumentos corretos no **rpmverifyfile**. Como resultado, o conteúdo SCAP que contém o OVAL **rpmverifyfile** pode ser usado pelo OpenSCAP para escanear sistemas de arquivos arbitrários.

(BZ#163636431)

httpd agora começa corretamente se usar uma chave privada ECDSA sem correspondência de chave pública armazenada em um dispositivo PKCS #11

Ao contrário das chaves da RSA, as chaves privadas da ECDSA não contêm necessariamente informações de chave pública. Neste caso, você não pode obter a chave pública de uma chave privada ECDSA. Por esta razão, um dispositivo PKCS #11 armazena informações de chave pública em um objeto separado, seja ele um objeto de chave pública ou um objeto de certificado. OpenSSL esperava que a estrutura **EVP_PKEY** fornecida por um motor para uma chave privada contivesse a informação da chave pública. Ao preencher a estrutura **EVP_PKEY** a ser fornecida à OpenSSL, o mecanismo no pacote **openssl-pkcs11** tentou buscar as informações da chave pública somente de objetos de chave pública correspondentes e ignorou os objetos certificados atuais.

Quando OpenSSL solicitou uma chave privada ECDSA do motor, a estrutura **EVP_PKEY** fornecida não continha a informação da chave pública se a chave pública não estivesse presente no dispositivo PKCS #11, mesmo quando um certificado correspondente que continha a chave pública estivesse disponível. Como consequência, uma vez que o servidor web Apache **httpd** chamou a função **X509_check_private_key()**, que requer a chave pública, em seu processo de inicialização, o **httpd** falhou em iniciar neste cenário. Este problema foi resolvido carregando a chave pública CE do certificado se o objeto chave pública não estiver disponível. Como resultado, o **httpd** agora inicia corretamente quando as chaves ECDSA são armazenadas em um dispositivo PKCS #11.

(BZ#1664807)

as remediações das regras de Auditoria agora funcionam corretamente

Anteriormente, o pacote de **guia de segurança do scap** continha uma combinação de remediação e uma verificação que poderia resultar em um dos seguintes cenários:

- remediação incorreta das regras de Auditoria
- avaliação de varredura contendo falsos positivos onde as regras aprovadas foram marcadas como falhadas

Conseqüentemente, durante o processo de instalação da RHEL, o escaneamento do sistema instalado relatou algumas regras de Auditoria como falhadas ou erradas.

Com esta atualização, as remediações foram corrigidas, e o escaneamento do sistema instalado com a política de segurança PCI-DSS não relata mais falsos positivos para as regras de Auditoria.

(BZ#1754919)

OpenSCAP agora fornece varredura offline de máquinas e recipientes virtuais

Anteriormente, a refatoração do codebase **OpenSCAP** fez com que certas sondas RPM falhassem na varredura de sistemas de arquivos VM e containers em modo off-line. Conseqüentemente, as seguintes ferramentas não podiam ser incluídas no pacote **openscap-utils: oscap-vm e oscap-chroot**. Além disso, o pacote **openscap-containers** foi completamente removido do RHEL 8. Com esta atualização, os problemas nas sondas foram resolvidos.

Como resultado, a RHEL 8 agora contém as ferramentas **oscap-podman, oscap-vm e oscap-chroot** no pacote **openscap-utils**.

(BZ#1618489)

OpenSCAP rpmverifypackage agora funciona corretamente

Anteriormente, as chamadas ao sistema **chdir** e **chroot** eram chamadas duas vezes pela sonda **rpmverifypackage**. Conseqüentemente, ocorreu um erro quando a sonda foi utilizada durante uma varredura **OpenSCAP** com conteúdo personalizado de Open Vulnerability and Assessment Language (OVAL). A sonda **rpmverifypackage** foi fixada para utilizar corretamente as chamadas de sistema **chdir** e **chroot**. Como resultado, o **rpmverifypackage** agora funciona corretamente.

(BZ#1646197)

8.6. TRABALHO EM REDE

O bloqueio na função `qdisc_run` agora não causa falha do núcleo

Anteriormente, uma condição de corrida quando a disciplina da fila **pfifo_fast** é reiniciada, enquanto o tráfego de decolagem levava à transmissão de pacotes após serem liberados. Como conseqüência, às vezes o kernel era terminado de forma inesperada. Com esta atualização, o bloqueio na função **qdisc_run** foi melhorado. Como resultado, o kernel não trava mais no cenário descrito.

(BZ#1744397)

As APIs Dbus em `org.fedoraproject.FirewallD1.config.service` funcionam como esperado

Anteriormente, o Dbus API **getIncludes**, **setIncludes** e **queryInclui** funções em **org.fedoraproject.FirewallD1** retornou uma mensagem de erro: **org.fedoraproject.FirewallD1.Exceção: índice de lista fora do intervalo** devido a má indexação. Com esta atualização, o Dbus API **getIncludes**, **setIncludes**, e **queryInclui** funções que funcionam como esperado.

(BZ#1737045)

A RHEL não registra mais um aviso de kernel ao descarregar o módulo `ipvs`

Anteriormente, o módulo servidor virtual IP(**ipvs**) usava uma contagem de referência incorreta, o que causava uma condição de corrida ao descarregar o módulo. Conseqüentemente, a RHEL registrou um aviso de kernel. Esta atualização corrige a condição de raça. Como resultado, o kernel não registra mais o aviso quando você descarrega o módulo **ipvs**.

(BZ#1687094)

A utilidade `nft` não interpreta mais os argumentos como opções de linha de comando após o primeiro argumento de não-opção

Anteriormente, a utilidade **nft** aceitava opções em qualquer lugar em um comando **nft**. Por exemplo, os administradores podiam usar opções entre ou após argumentos de não-opção. Como conseqüência, devido ao traço principal, **nft** interpretou valores de prioridade negativa como opções, e o comando falhou. O analisador da linha de comando do utilitário **nft** foi atualizado para não interpretar argumentos que começam com um traço após a leitura do primeiro argumento de não-opção. Como resultado, os administradores não precisam mais de soluções para passar valores de prioridade negativa para **nft**.

Note que devido a esta mudança, você deve agora passar todas as opções de comando a **nft** antes do primeiro argumento de não-opção. Antes de atualizar, verifique seus scripts nftables para que correspondam a este novo critério para assegurar que o script funcione como esperado após a instalação desta atualização.

[\(BZ#1778883\)](#)

Os arquivos `/etc/hosts.allow` e `/etc/hosts.deny` não contêm mais referências desatualizadas para remover `tcp_wrappers`

Anteriormente, os arquivos `/etc/hosts.allow` e `/etc/hosts.deny` continham informações desatualizadas sobre o pacote `tcp_wrappers`. Os arquivos são removidos no RHEL 8, pois não são mais necessários para o `tcp_wrappers` que é removido.

[\(BZ#1663556\)](#)

Um parâmetro de configuração foi adicionado ao `firewalld` para desativar a deriva da zona

Anteriormente, o serviço `firewalld` continha um comportamento indocumentado conhecido como "zone drifting". O RHEL 8.0 removeu este comportamento porque poderia ter um impacto negativo na segurança. Como consequência, nos hospedeiros que usavam este comportamento para configurar uma zona de "catch-all" ou "fallback", o serviço `firewalld` negava conexões que anteriormente eram permitidas. Esta atualização readiciona o comportamento de deriva da zona, mas como uma característica configurável. Como resultado, os usuários podem agora decidir usar o drifting de zona ou desativar o comportamento para uma configuração de firewall mais segura.

Por padrão, no RHEL 8.2, o novo parâmetro `AllowZoneDrifting` no arquivo `/etc/firewalld/firewalld.conf` está definido para `sim`. Observe que, se o parâmetro estiver ativado, os logs `firewalld`:

ADVERTÊNCIA: `AllowZoneDrifting` está ativado. Esta é considerada uma opção de configuração insegura. Ela será removida em um lançamento futuro. Por favor, considere desativá-lo agora.

[\(BZ#1772208\)](#)

8.7. KERNEL

O hotplug de memória da subseção é agora totalmente suportado

Anteriormente, algumas plataformas alinhavam regiões de memória física, tais como Módulos em linha duplos (DIMMs) e conjuntos de intercalação para limites de memória de 64MiB. Entretanto, como o subsistema hotplug Linux usa um tamanho de memória de 128MiB, novos dispositivos hot-plugging causaram sobreposição de múltiplas regiões de memória em uma única janela de memória hotplug. Consequentemente, isto causou falha na listagem dos espaços de nomes de memória persistentes disponíveis com o seguinte ou um traço de chamada similar:

```
WARNING: CPU: 38 PID: 928 at arch/x86/mm/init_64.c:850
add_pages+0x5c/0x60
[.]
RIP: 0010:add_pages+0x5c/0x60
[.]
Call Trace:
devm_memremap_pages+0x460/0x6e0
pmem_attach_disk+0x29e/0x680 [nd_pmem]
? nd_dax_probe+0xfc/0x120 [libnvdimm]
nvdimm_bus_probe+0x66/0x160 [libnvdimm]
```

Esta atualização corrige o problema e suporta o subsistema hotplug Linux para permitir que múltiplas regiões de memória compartilhem uma única janela de memória hotplug.

[\(BZ#1724969\)](#)

A corrupção de dados agora aciona um BUG em vez de uma mensagem WARN

Com este aprimoramento, a lista corrompe na **lib/list_debug.c** agora aciona um BUG, que gera um relatório com um **vmcore**. Anteriormente, ao encontrar uma corrupção de dados, era gerada uma simples WARN, que provavelmente passaria despercebida. Com o **conjunto CONFIG_BUG_ON_DATA_CORRUPTION**, o kernel agora cria uma falha e aciona um BUG em resposta à corrupção de dados. Isto evita mais danos e reduz o risco de segurança. O **kdump** agora gera um **vmcore**, o que melhora os relatórios de bugs de corrupção de dados.

(BZ#1714330)

Suporte para o cartão Intel Carlsville está disponível, mas não verificado no RHEL 8.2

O suporte ao cartão **Intel Carlsville** está disponível mas não foi testado no Red Hat Enterprise Linux 8.2.

(BZ#1720227)

RPS e XPS não colocam mais empregos em CPUs isoladas

Anteriormente, o mecanismo de fila de recepção de pacotes de direção (RPS) e o mecanismo de fila de transmissão de pacotes de direção (XPS) transmitem trabalhos alocados em todos os conjuntos de CPU, incluindo CPUs isoladas. Conseqüentemente, isto poderia causar um pico de latência inesperado em um ambiente em tempo real quando uma carga de trabalho sensível à latência estava usando a mesma CPU onde os trabalhos RPS ou XPS estavam sendo executados. Com esta atualização, a função **store_rps_map()** não inclui nenhuma CPUs isolada para fins de configuração RPS. Da mesma forma, os drivers do kernel usados para a configuração do XPS estão respeitando o isolamento da CPU. Como resultado, o RPS e o XPS não mais colocam trabalhos em CPUs isoladas no cenário descrito. Se você configurar uma CPU isolada no arquivo **/sys/devices/pci*/net/dev/queues/rx-*/rps_cpus**, o seguinte erro aparece:

```
Erro: "-bash: echo:write error": Argumento inválido..
```

Entretanto, a configuração manual de uma CPU isolada no arquivo **/sys/devices/pci*/net/dev/queues/tx-*/xps_cpus** aloca com sucesso trabalhos XPS na CPU isolada.

Observe que uma carga de trabalho em rede em um ambiente com CPUs isoladas provavelmente experimentará alguma variação de desempenho.

(BZ#1867174)

8.8. SISTEMAS DE ARQUIVO E ARMAZENAMENTO

Os drivers SCSI não usam mais uma quantidade excessiva de memória

Anteriormente, alguns drivers SCSI usavam uma quantidade maior de memória do que na RHEL 7. Em certos casos, como a criação de vPort em um adaptador de barramento host de canal de fibra (HBA), o uso de memória era excessivo, dependendo da configuração do sistema.

O aumento do uso de memória foi causado pela pré-alocação de memória na camada de bloco. Tanto a programação do dispositivo de blocos multifilas (BLK-MQ) quanto a pilha SCSI multifilas (SCSI-MQ) pré-alocação de memória para cada pedido de E/S, levando ao aumento do uso de memória.

Com esta atualização, a camada de bloco limita a quantidade de pré-alocação de memória e, como resultado, os drivers SCSI não usam mais uma quantidade excessiva de memória.

(BZ#1698297)

VDO pode agora suspender antes que a UDS tenha terminado a reconstrução

Anteriormente, o comando de **suspensão dmsetup** tornou-se insensível se você tentasse suspender um volume VDO enquanto o índice UDS estava sendo reconstruído. O comando só terminou após a reconstrução.

Com esta atualização, o problema foi resolvido. O comando de **suspensão dmsetup** pode terminar antes que a reconstrução do UDS seja feita sem ficar sem responder.

(BZ#1737639)

8.9. LINGUAGENS DE PROGRAMAÇÃO DINÂMICA, SERVIDORES WEB E DE BANCO DE DADOS

Os problemas no `mod_cgid` logging foram resolvidos

Antes desta atualização, se o módulo `mod_cgid` Apache `httpd` era usado sob um módulo de multiprocessamento (MPM) rosqueado, ocorreram os seguintes problemas de registro:

- A saída `stderr` do script CGI não foi prefixada com informações de timestamp padrão.
- A saída `stderr` do script CGI não foi redirecionada corretamente para um arquivo de log específico para o `VirtualHost`, se configurado.

Esta atualização corrige os problemas, e o `mod_cgid` logging agora funciona como esperado.

(BZ#1633224)

8.10. COMPILADORES E FERRAMENTAS DE DESENVOLVIMENTO

Objetos compartilhados não deslocados e não inicializados não mais resultam em falhas se o `dlopen` falhar

Anteriormente, se a chamada `dlopen` falhou, o linker dinâmico `glibc` não removia objetos compartilhados com a marca `NODELETE` antes de relatar o erro. Conseqüentemente, os objetos compartilhados não localizados e não inicializados permaneceram na imagem do processo, resultando eventualmente em falhas de afirmação ou travamentos. Com esta atualização, o carregador dinâmico usa um estado `NODELETE` pendente para remover objetos compartilhados em caso de falha de `dlopen`, antes de marcá-los como `NODELETE` permanentemente. Como resultado, o processo não deixa nenhum objeto não deslocado para trás. Além disso, falhas de amarração preguiçosas enquanto os construtores e destruidores ELF executam agora terminam o processo.

(BZ#1410154)

As funções avançadas SIMD na arquitetura ARM de 64 bits não mais se confundem quando resolvidas preguiçosamente

Anteriormente, o novo Padrão de Chamada de Procedimento Vetorial (PCS) para SIMD Avançado não salvava e restaurava corretamente certos registros salvos de calle quando resolvia preguiçosamente as funções do SIMD Avançado. Como consequência, os binários poderiam se comportar mal em tempo de execução. Com esta atualização, as funções vetoriais do SIMD Avançado e SVE na tabela de símbolos são marcadas com `.variant_pcs` e, como resultado, o linker dinâmico ligará tais funções mais cedo.

(BZ#1726641)

O roteiro do `sudo` wrapper agora analisa as opções

Anteriormente, o script `/opt/redhat/devtoolset*/root/usr/bin/sudo` wrapper não analisava corretamente as opções do `sudo`. Como consequência, algumas opções de `sudo` (por exemplo, `sudo -i`) não podiam ser executadas. Com esta atualização, mais opções `sudo` são corretamente analisadas e, como resultado, o script `sudo` wrapper funciona mais como `/usr/bin/sudo`.

(BZ#1774118)

O alinhamento das variáveis TLS na `glibc` foi fixado

Anteriormente, os dados do armazenamento local de fios alinhados (TLS) podiam, sob certas condições, se tornar instanciados sem o alinhamento esperado. Com esta atualização, o POSIX Thread Library `libpthread` foi melhorado para assegurar o alinhamento correto sob quaisquer condições. Como resultado, os dados TLS alinhados são agora instanciados corretamente para todas as roscas com o alinhamento correto.

(BZ#1764214)

As chamadas `pututxline` repetidas após erro `EINTR` ou `EAGAIN` não corrompem mais o arquivo `utmp`

Quando a função `pututxline` tenta adquirir uma trava e não consegue a tempo, a função retorna com código de erro `EINTR` ou `EAGAIN`. Anteriormente nesta situação, se a `pututxline` fosse chamada novamente imediatamente e conseguisse obter a trava, ela não usava um slot correspondente já alocado no arquivo `utmp`, mas acrescentava outra entrada em seu lugar. Como consequência, estas entradas não utilizadas aumentaram substancialmente o tamanho do arquivo de `utmp`. Esta atualização corrige o problema, e as entradas são agora adicionadas corretamente ao arquivo `utmp`.

(BZ#1749439)

`mtrace` não fica mais pendurado quando ocorrem falhas internas

Anteriormente, um defeito na implementação da ferramenta `mtrace` podia fazer com que o traçado da memória ficasse pendurado. Para resolver este problema, a implementação da ferramenta `mtrace` memory tracing foi tornada mais robusta para evitar o pendurar mesmo em face de falhas internas. Como resultado, os usuários podem agora chamar o `mtrace` e ele não fica mais pendurado, completando em tempo delimitado.

(BZ#1764235)

A função `garfo` evita certos bloqueios relacionados ao uso de `pthread_atfork`

Anteriormente, se um programa registrava um manipulador de `trabalho` e invocava o `garfo` de um manipulador de sinais assíncronos, um defeito na fechadura interna dependente da implementação poderia causar o congelamento do programa. Com esta atualização, a implementação do `garfo` e de seus manipuladores de `atfork` é ajustada para evitar o bloqueio em programas de rosca única.

(BZ#1746928)

`strstr` não retorna mais correspondências incorretas para um padrão truncado

Em certas plataformas IBM Z (z15, anteriormente conhecidas como arch13), a função `strstr` não atualizou corretamente um registro de CPU ao lidar com padrões de busca que cruzam os limites de uma página. Como consequência, `strstr` retornou correspondências incorretas. Esta atualização corrige o problema e, como resultado, `strstr` funciona como esperado no cenário mencionado.

(BZ#1777241)

C.UTF-8 locale fonte ellipsis expressões em `glibc` são fixas

Anteriormente, um defeito no local de origem C.UTF-8 resultava em todos os pontos de código Unicode acima de U 10000 sem pesos de colação. Como consequência, todos os pontos de código acima de U.10000 não foram agrupados como esperado. O locale fonte C.UTF-8 foi corrigido, e o locale binário recentemente compilado agora tem pesos de agrupamento para todos os pontos de código Unicode. O locale C.UTF-8 compilado é 5,3MiB maior, como resultado desta correção.

(BZ#1361965)

`glibc` não falha mais quando a `getpwent()` é chamada sem chamar `setpwent()`

Se seu arquivo `/etc/nsswitch.conf` apontar para o fornecedor da senha Berkeley DB (`db`), você poderia solicitar dados usando a função `getpwent()` sem primeiro chamar `setpwent()` apenas uma vez. Quando você chamou a função `endpwent()`, outras chamadas para `getpwent()` sem a primeira chamada `setpwent()` causaram a falha da `glibc` porque `endpwent()` não pôde redefinir os internos para permitir uma nova consulta. Esta atualização corrige o problema. Como resultado, após terminar uma consulta com `endpwent()`, novas chamadas para `getpwent()` iniciarão uma nova consulta mesmo que você não chame `setpwent()`.

(BZ#1747502)

`ltrace` pode agora rastrear chamadas de sistema em binários endurecidos

Anteriormente, o `ltrace` não produzia nenhum resultado em certos binários endurecidos, tais como binários de sistema, nas arquiteturas AMD e Intel 64-bit. Com esta atualização, o `ltrace` pode agora rastrear chamadas de sistema em binários endurecidos.

(BZ#1655368)

A falha da Intel no JCC não causa mais perda significativa de desempenho no compilador GCC

Certas CPUs da Intel são afetadas pelo bug do Jump Conditional Code (JCC), fazendo com que as instruções da máquina sejam executadas incorretamente. Conseqüentemente, as CPUs afetadas podem não executar os programas corretamente. A correção completa envolve a atualização do microcódigo das CPUs vulneráveis, o que pode causar uma degradação do desempenho. Esta atualização permite uma solução no assembler que ajuda a reduzir a perda de desempenho. A alternativa é `not` ativado por padrão.

Para aplicar o workaround, recompile um programa usando GCC com a opção `-Wa,-mbranches-within-32B-b-boundaries` command line. Um programa recompilado com esta opção de linha de comando não será afetado pela falha do JCC, mas a atualização do microcódigo ainda é necessária para proteger totalmente um sistema.

Note que a aplicação do workaround aumentará o tamanho do programa e ainda pode causar uma ligeira diminuição do desempenho, embora deva ser menor do que teria sido sem a recompilação.

(BZ#1777002)

não retarda mais quando utiliza construções paralelas

Anteriormente, enquanto funcionavam em construções paralelas, o `os` subprocessos podiam tornar-se temporariamente insensíveis quando esperavam sua vez de funcionar. Como consequência, as construções com altos valores `-j` abrandaram ou funcionaram com valores `-j` mais baixos efetivos. Com esta atualização, a lógica de controle de trabalho da `marca` é agora sem bloqueio. Como resultado, as construções com valores altos de `-j` rodam na velocidade `-j` total.

(BZ#1774790)

A ferramenta **ltrace** agora informa corretamente as chamadas de função

Devido a melhorias no endurecimento binário aplicadas a todos os componentes RHEL, a ferramenta **ltrace** anteriormente não conseguia detectar chamadas de função em arquivos binários provenientes de componentes RHEL. Como consequência, a saída do **ltrace** estava vazia porque não relatou nenhuma chamada detectada quando usada em tais arquivos binários. Esta atualização corrige a forma como o **ltrace** lida com as chamadas de função, o que evita a ocorrência do problema descrito.

(BZ#1618748)

8.11. GESTÃO DA IDENTIDADE

A utilidade **dsctl** não deixa mais de gerenciar instâncias com um hífen em seu nome

Anteriormente, o utilitário **dsctl** não analisava corretamente os hífens nos nomes das instâncias do Servidor de Diretório. Como consequência, os administradores não podiam usar o **dsctl** para gerenciar instâncias com um hífen em seu nome. Esta atualização corrige o problema e o **dsctl** agora funciona como esperado no cenário mencionado.

(BZ#1715406)

Nomes de instâncias de servidores de diretório podem agora ter até 103 caracteres

Quando um cliente LDAP estabelece uma conexão com o Directory Server, o servidor armazena informações relacionadas com o endereço do cliente em um buffer local. Anteriormente, o tamanho deste buffer era muito pequeno para armazenar um nome de caminho LDAP com mais de 46 caracteres. Por exemplo, este é o caso se o nome da instância do Servidor de Diretório for muito longo. Como consequência, o servidor terminou inesperadamente devido a um estouro de buffer. Esta atualização aumenta o tamanho do buffer para o tamanho máximo que a biblioteca Netscape Portable Runtime (NSPR) suporta para o nome do caminho. Como resultado, o Servidor de Diretório não trava mais no cenário mencionado.

Note que devido à limitação na biblioteca NSPR, um nome de instância pode ter no máximo 103 caracteres.

(BZ#1748016)

A utilidade do **pkidestroy** agora escolhe a instância correta

Anteriormente, o comando **pkidestroy --force** executado em uma instância semi-eliminada escolheu a instância **pki-tomcat** por padrão, independentemente do nome da instância especificada com a opção **-i instance**.

Como consequência, isto removeu a instância **pki-tomcat** em vez da instância pretendida, e a opção **--remove-logs** não removeu os logs da instância pretendida. **pkidestroy** agora aplica o nome correto da instância, removendo apenas os restos da instância pretendida.

(BZ#1698084)

A descrição do serviço **ldap_user_authorized_service** foi atualizada na página de manual **sssd-ldap**

A pilha de módulos de autenticação Pluggable (PAM) foi alterada no RHEL 8. Por exemplo, a sessão do usuário **do sistema** agora inicia uma conversa PAM usando o serviço PAM de **usuário do sistema**. Este serviço agora inclui recursivamente o serviço PAM **system-auth**, que pode incluir a interface

pam_sss.so. Isto significa que o controle de acesso SSSD é sempre chamado.

Você deve estar ciente desta mudança ao projetar regras de controle de acesso para os sistemas RHEL 8. Por exemplo, você pode adicionar o serviço **de usuário do sistema** à lista de serviços permitidos.

Observe que para alguns mecanismos de controle de acesso, tais como IPA HBAC ou AD GPOs, o serviço **de usuário do sistema** foi adicionado à lista de serviços permitidos por padrão e você não precisa tomar nenhuma ação.

A página de manual **sssdlldap** foi atualizada para incluir estas informações.

(BZ#1669407)

As informações sobre os registros DNS necessários são agora exibidas quando se permite o suporte à confiança do AD na IdM

Anteriormente, ao permitir o suporte à confiança do Active Directory (AD) na instalação do Red Hat Enterprise Linux Identity Management (IdM) com gerenciamento DNS externo, nenhuma informação sobre os registros DNS necessários era exibida. Ao entrar no **ipa dns-update-system-records --** o comando **secy-run** manualmente era necessário para obter uma lista de todos os registros DNS requeridos pelo IdM.

Com esta atualização, o comando **ipa-adtrust-install** lista corretamente os registros do serviço DNS para adição manual à zona DNS.

(BZ#1665051)

8.12. DESKTOP

O GNOME Shell no Wayland não funciona mais lentamente quando se usa um renderizador de software

Anteriormente, o Wayland back end do GNOME Shell não usava um framebuffer cacheable quando usava um renderizador de software. Como consequência, a Shell GNOME renderizada por software no Wayland era lenta em comparação com a Shell GNOME renderizada por software no back end do X.org.

Com esta atualização, um buffer de sombras intermediário foi adicionado no GNOME Shell on Wayland. Como resultado, a Shell GNOME Shell on Wayland agora tem o mesmo desempenho que a Shell GNOME no X.org.

(BZ#1737553)

8.13. VIRTUALIZAÇÃO

Iniciar um VM em um processador Intel Core de 10ª geração não falha mais

Anteriormente, a partida de uma máquina virtual (VM) falhou em um modelo host que usava um processador Intel Core de 10ª geração, também conhecido como Icelake-Server. Com esta atualização, **a libvirt** não tenta mais desativar o recurso de CPU **pconfig**, que não é suportado pelo QEMU. Como resultado, iniciar uma VM em um modelo host que usava um processador Intel de 10ª geração não falha mais.

(BZ#1749672)

A utilização de nuvens para o fornecimento de máquinas virtuais no Microsoft Azure agora funciona corretamente

Anteriormente, não era possível usar o utilitário de **nuvem** para fornecer uma máquina virtual RHEL 8 (VM) na plataforma Microsoft Azure. Esta atualização corrige o manuseio **com a nuvem** de dados dos pontos finais do Azure, e o provisionamento da RHEL 8 VMs no Azure agora prossegue como esperado.

(BZ#1641190)

As máquinas virtuais RHEL 8 nos hosts RHEL 7 podem ser visualizadas de forma confiável em resolução superior a 1920x1200

Anteriormente, ao utilizar uma máquina virtual RHEL 8 (VM) rodando em um sistema host RHEL 7, certos métodos de exibição da saída gráfica da VM, tais como rodar a aplicação em modo quiosque, não podiam utilizar uma resolução maior do que 1920x1200. Como consequência, exibir VMs usando esses métodos só funcionava em resoluções até 1920x1200, mesmo que o hardware do host suportasse resoluções mais altas. Esta atualização ajusta os drivers DRM e QXL de forma a evitar que o problema descrito ocorra.

(BZ#1635295)

A personalização de uma VM ESXi usando a **nuvem** e o reinício da VM agora funciona corretamente

Anteriormente, se o serviço **cloud-init** era utilizado para modificar uma máquina virtual (VM) rodando no VMware ESXi hypervisor para utilizar IP estático e a VM era então clonada, a nova VM clonada em alguns casos demorou muito tempo para reiniciar. Esta atualização modifica a **nuvem** - não para reescrever o IP estático da VM para DHCP, o que impede que o problema descrito ocorra.

(BZ#166666961, [BZ#1706482](#))

8.14. CONTÊINERES

Puxar imagens do registro do cais.io não leva mais a imagens não intencionais

Anteriormente, ter o registro de imagem do cais.io contentor listado na lista de busca padrão de registros fornecida em **/etc/containers/registries.conf** podia permitir que um usuário puxasse uma imagem falsificada ao usar um nome curto. Para corrigir este problema, o registro de imagem de container do cais.io foi removido da lista de busca padrão de registros em **/etc/containers/registries.conf**. Como resultado, puxar imagens do registro do **cais.io** agora requer que os usuários especifiquem o nome completo do repositório, como **quay.io/myorg/myimage**. O registro do cais.io pode ser adicionado de volta à lista de busca padrão de registros em **/etc/containers/registries.conf** para reativar a extração de imagens de contêineres usando nomes curtos, no entanto, isto não é recomendado, pois poderia criar um risco de segurança.

([BZ#1784267](#))

CAPÍTULO 9. ANTEVISÕES TECNOLÓGICAS

Esta parte fornece uma lista de todas as Análises de Tecnologia disponíveis no Red Hat Enterprise Linux 8.2.

Para informações sobre o escopo de suporte da Red Hat para recursos de Technology Preview, veja [Technology Preview Features Support Scope](#).

9.1. TRABALHO EM REDE

nmstate disponível como uma Pré-visualização Tecnológica

O Nmstate é um API de rede para hosts. Os pacotes **nmstate**, disponíveis como uma Technology Preview, fornecem uma biblioteca e o utilitário de linha de comando **nmstatectl** para gerenciar as configurações de rede do host de forma declarativa. O estado da rede é descrito por um esquema pré-definido. Os relatórios do estado atual e as mudanças para o estado desejado estão ambos de acordo com o esquema.

Para mais detalhes, consulte o arquivo `/usr/share/doc/nmstate/README.md` e os exemplos no diretório `/usr/share/doc/nmstate/examples`.

(BZ#1674456)

AF_XDP disponível como uma prévia tecnológica

O soquete **eXpress Data Path (AF_XDP)** da família de endereços foi projetado para o processamento de pacotes de alto desempenho. Ele acompanha o **XDP** e permite o redirecionamento eficiente de pacotes programmaticamente selecionados para aplicações de espaço do usuário para processamento posterior.

(BZ#1633143)

XDP disponível como uma prévia de tecnologia

O recurso eXpress Data Path (XDP), disponível como Technology Preview, fornece um meio de anexar programas Berkeley Packet Filter (eBPF) estendidos para processamento de pacotes de alto desempenho em um ponto inicial no caminho de entrada de dados do kernel, permitindo análise, filtragem e manipulação de pacotes programáveis eficientes.

(BZ#1503672)

KTLS disponível como uma prévia tecnológica

No Red Hat Enterprise Linux 8, a Kernel Transport Layer Security (KTLS) é fornecida como um Preview de Tecnologia. O KTLS trata os registros TLS usando a criptografia simétrica ou algoritmos de decodificação no kernel para a cifra AES-GCM. O KTLS também fornece a interface para descarregar a criptografia de registros TLS para os Controladores de Interface de Rede (NICs) que suportam esta funcionalidade.

(BZ#1570255)

O utilitário dracut agora suporta a criação de imagens initrd com suporte ao NetworkManager como uma pré-visualização tecnológica

Por padrão, o utilitário **dracut** usa um script shell para gerenciar a rede no disco RAM inicial (**initrd**). Em certos casos, isto pode causar problemas quando o sistema muda do disco RAM para o sistema operacional que usa o NetworkManager para configurar a rede. Por exemplo, o NetworkManager

poderia enviar outra solicitação DHCP, mesmo que o script no disco RAM já solicitasse um endereço IP. Esta solicitação do disco RAM poderia resultar em um intervalo de tempo.

Para resolver este tipo de problemas, o **dracut** em RHEL 8.2 pode agora usar o NetworkManager no disco RAM. Use os seguintes comandos para habilitar o recurso e recriar as imagens do disco RAM:

```
echo 'add_dracutmodules+=" network-manager "' > /etc/dracut.conf.d/enable-nm.conf
dracut -vf --regenerate-all
```

Note que a Red Hat não suporta recursos de previsão tecnológica. No entanto, para fornecer feedback sobre este recurso, por favor, entre em contato com o suporte da Red Hat.

(BZ#1626348)

O driver **mlx5_core** suporta o adaptador de rede Mellanox ConnectX-6 Dx como uma pré-visualização tecnológica

Este aprimoramento acrescenta as IDs PCI do adaptador de rede Mellanox ConnectX-6 Dx ao driver **mlx5_core**. Nos hosts que utilizam este adaptador, a RHEL carrega o driver **mlx5_core** automaticamente. Note que a Red Hat fornece este recurso como uma visualização da tecnologia não suportada.

(BZ#1687434)

O serviço de solução de sistema está agora disponível como uma Pré-visualização Tecnológica

O serviço **resolvido pelo sistema** fornece resolução de nomes para aplicações locais. O serviço implementa um resolvidor de stub DNS de cache e validação, uma Resolução de nomes Multicast local (LLMNR) e um resolvidor e respondedor DNS Multicast.

Observe que, mesmo que o pacote **systemd** ofereça **solução de sistema**, este serviço é uma Pré-visualização Tecnológica não suportada.

(BZ#1906489)

9.2. KERNEL

kexec reinicialização rápida como uma prévia de tecnologia

O recurso de **reinicialização rápida do kexec** continua disponível como uma Pré-visualização Tecnológica. A reinicialização é agora significativamente mais rápida graças à **reinicialização rápida do kexec**. Para usar este recurso, carregue o kexec manualmente, e então reinicialize o sistema operacional.

(BZ#1769727)

eBPF disponível como uma prévia de tecnologia

Extended Berkeley Packet Filter (eBPF) é uma máquina virtual in-kernel que permite a execução do código no espaço do kernel, no ambiente restrito do sandbox com acesso a um conjunto limitado de funções.

A máquina virtual inclui uma nova chamada de sistema **bpf()**, que suporta a criação de vários tipos de mapas, e também permite carregar programas em um código especial tipo montagem. O código é então carregado para o kernel e traduzido para o código da máquina nativa com compilação just-in-time. Note que o **bpf()** syscall só pode ser usado com sucesso por um usuário com a capacidade **CAP_SYS_ADMIN**, tal como o usuário root. Veja a página de manual **bpf(2)** para mais informações.

Os programas carregados podem ser anexados a uma variedade de pontos (soquetes, tracepoints, recepção de pacotes) para receber e processar dados.

Há numerosos componentes enviados pela Red Hat que utilizam a máquina virtual **eBPF**. Cada componente está em uma fase de desenvolvimento diferente e, portanto, nem todos os componentes são atualmente totalmente suportados. Todos os componentes estão disponíveis como uma Pré-visualização Tecnológica, a menos que um componente específico seja indicado como suportado.

Os seguintes componentes notáveis **eBPF** estão atualmente disponíveis como uma Pré-visualização Tecnológica:

- **bpfftrace**, uma linguagem de rastreamento de alto nível que utiliza a máquina virtual **eBPF**.
- O recurso eXpress Data Path (XDP), uma tecnologia de rede que permite o rápido processamento de pacotes no kernel usando a máquina virtual **eBPF**.

(BZ#1559616)

libbpf está disponível como uma prévia tecnológica

O pacote **da libbpf** está atualmente disponível como uma Pré-visualização Tecnológica. O pacote **libbpf** é crucial para aplicações relacionadas ao bpf como **bpfftrace** e desenvolvimento **bpf/xdp**.

É um espelho da árvore bpf-next linux **bpf-next/tools/lib/bpf** directory mais seus arquivos de cabeçalho de suporte. A versão do pacote reflete a versão da Interface Binária de Aplicação (ABI).

(BZ#1759154)

O motorista do igc disponível como uma Tecnologia de Pré-visualização para RHEL 8

O driver Intel Intel 2.5G Ethernet Linux com fio LAN está agora disponível em todas as arquiteturas para o RHEL 8 como uma prévia tecnológica. O utilitário **ethtool** também suporta as LANs com fio **igc**.

(BZ#1495358)

9.3. SISTEMAS DE ARQUIVO E ARMAZENAMENTO

O NVMe/TCP está disponível como uma prévia tecnológica

Acesso e compartilhamento do armazenamento de memória não volátil expressa (NVMe) através de redes TCP/IP (NVMe/TCP) e seus correspondentes módulos **nvme-tcp.ko** e **nvmet-tcp.ko** kernel foram adicionados como uma Pré-visualização tecnológica.

O uso do NVMe/TCP como cliente de armazenamento ou alvo é gerenciável com ferramentas fornecidas pelos pacotes **nvme-cli** e **nvmetcli**.

A Pré-visualização da Tecnologia alvo NVMe/TCP está incluída apenas para fins de teste e não está atualmente planejada para suporte total.

(BZ#1696451)

O sistema de arquivo DAX agora está disponível para ext4 e XFS como uma pré-visualização tecnológica

No Red Hat Enterprise Linux 8.2, o sistema de arquivo DAX do Red Hat está disponível como uma Pré-visualização Tecnológica. O DAX fornece um meio para um aplicativo mapear diretamente a memória persistente em seu espaço de endereços. Para usar DAX, um sistema deve ter alguma forma de memória persistente disponível, geralmente na forma de um ou mais NVDIMMs (Non-Volatile Dual In-

line Memory Modules), e um sistema de arquivo que suporte DAX deve ser criado no(s) NVDIMM(s). Além disso, o sistema de arquivo deve ser montado com a opção de montagem **por dax**. Então, um **mmap** de um arquivo no sistema de arquivo montado por eixo resulta em um mapeamento direto do armazenamento no espaço de endereços da aplicação.

(BZ#1627455)

OverlayFS

O OverlayFS é um tipo de sistema de arquivo sindical. Ele permite a sobreposição de um sistema de arquivos sobreposto a outro. As mudanças são registradas no sistema de arquivo superior, enquanto o sistema de arquivo inferior permanece inalterado. Isto permite que vários usuários compartilhem uma imagem do sistema de arquivo, como um container ou um DVD-ROM, onde a imagem base está em uma mídia somente de leitura. Consulte a documentação do kernel do Linux para obter informações adicionais: <https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt>.

A OverlayFS continua sendo uma Pré-visualização Tecnológica na maioria das circunstâncias. Como tal, o kernel registra avisos quando esta tecnologia é ativada.

O suporte completo está disponível para OverlayFS quando usado com motores de contêineres suportados (**podman**, **cri-o**, ou **buildah**) sob as seguintes restrições:

- O OverlayFS é suportado para uso apenas como um driver gráfico do motor do contêiner. Seu uso é suportado apenas para conteúdo de COW de contêineres, não para armazenamento persistente. Você deve colocar qualquer armazenamento persistente em volumes não-OverlayFS. Somente a configuração padrão do motor de contêiner pode ser usada; ou seja, um nível de overlay, um nível inferior, e ambos os níveis inferior e superior estão no mesmo sistema de arquivo.
- Atualmente, apenas o XFS é suportado para uso como um sistema de arquivo de camada inferior.

Além disso, as seguintes regras e limitações se aplicam ao uso do OverlayFS:

- O comportamento do kernel ABI e do espaço do usuário do OverlayFS não são considerados estáveis, e podem ver mudanças em futuras atualizações.
- A OverlayFS fornece um conjunto restrito de padrões POSIX. Teste sua aplicação completamente antes de implementá-la com OverlayFS. Os seguintes casos não são compatíveis com o POSIX:
 - Arquivos inferiores abertos com **O_RDONLY** não recebem atualizações **st_atime** quando os arquivos são lidos.
 - Arquivos inferiores abertos com **O_RDONLY**, depois mapeados com **MAP_SHARED** são inconsistentes com modificações subseqüentes.
 - Os valores **st_ino** ou **d_ino** totalmente compatíveis não são ativados por padrão no RHEL 8, mas você pode ativar a conformidade total do POSIX para eles com uma opção de módulo ou opção de montagem. Para obter uma numeração inode consistente, use a opção **xino=em** montagem.

Você também pode usar as opções **redirect_dir=on** e **index=on** para melhorar a conformidade POSIX. Estas duas opções tornam o formato da camada superior incompatível com uma sobreposição sem estas opções. Ou seja, você pode obter resultados inesperados ou erros se criar uma sobreposição com **redirect_dir=on** ou **index=on**, desmontar a sobreposição, e então montar a sobreposição sem estas opções.

- Comandos utilizados com XFS:
 - Os sistemas de arquivo XFS devem ser criados com a opção **-n ftype=1** habilitada para uso como um overlay.
 - Com os rootfs e qualquer sistema de arquivo criado durante a instalação do sistema, defina os parâmetros **--mkfsoptions=-n ftype=1** no kickstart do Anaconda.
 - Ao criar um novo sistema de arquivo após a instalação, execute o comando **# mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE**.
 - Para determinar se um sistema de arquivo existente é elegível para uso como uma sobreposição, execute o comando **# xfs_info /PATH/TO/DEVICE | grep ftype** para ver se a opção **ftype=1** está habilitada.
- As etiquetas de segurança SELinux são habilitadas por padrão em todos os motores de contêineres suportados com OverlayFS.
- Há vários problemas conhecidos associados ao OverlayFS neste lançamento. Para detalhes, veja *Non-standard behavior* na documentação do kernel Linux: <https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt>.

(BZ#1690207)

Stratis está agora disponível como uma Pré-visualização Tecnológica

Stratis é um novo gerente de armazenamento local. Ele fornece sistemas de arquivos gerenciados em cima de pools de armazenamento com características adicionais para o usuário.

Stratis permite realizar mais facilmente tarefas de armazenamento como, por exemplo

- Gerenciar snapshots e provisionamento fino
- Aumentar automaticamente os tamanhos dos sistemas de arquivo conforme necessário
- Manter sistemas de arquivo

Para administrar o armazenamento Stratis, use o utilitário **Stratis**, que se comunica com o serviço de fundo **Stratisd**.

Stratis é fornecido como uma Pré-visualização Tecnológica.

Para mais informações, consulte a documentação do Stratis: [Gerenciamento de armazenamento local em camadas com Stratis](#).

RHEL 8.2 atualiza o Stratis para a versão 2.0.0. Esta versão melhora a confiabilidade e a API do Stratis DBus. Para mais informações sobre a versão 2.0.0, veja as [Notas de Lançamento do Stratis 2.0.0](#).

(JIRA:RHELPLAN-1212)

IdM agora suporta a criação de um servidor Samba em um membro do domínio IdM como uma prévia tecnológica

Com esta atualização, você pode agora configurar um servidor Samba em um membro do domínio de Gerenciamento de Identidade (IdM). O novo utilitário **ipa-cliente-samba** fornecido pelo pacote com o mesmo nome adiciona um serviço Kerberos específico do Samba-principal à IdM e prepara o cliente

IdM. Por exemplo, o utilitário cria o `/etc/samba/smb.conf` com a configuração de mapeamento de ID para o back end do mapeamento de IDs **sss**. Como resultado, os administradores podem agora configurar o Samba em um membro do domínio IdM.

Devido aos controladores de confiança IdM que não suportam o serviço de catálogo global, os hosts do Windows inscritos no AD não podem encontrar usuários e grupos IdM no Windows. Além disso, os Controladores de Confiança IdM não suportam a resolução de grupos IdM usando os protocolos Ambiente de Computação Distribuída / Chamadas de Procedimento Remoto (DCE/RPC). Como consequência, os usuários AD só podem acessar os compartilhamentos e impressoras Samba dos clientes IdM.

Para detalhes, consulte [Configurando o Samba em um membro do domínio IdM](#).

(JIRA:RHELPLAN-13195)

9.4. ALTA DISPONIBILIDADE E CLUSTERS

Pacemaker podman bundles disponíveis como Technology Preview

Os pacotes de contêineres do Pacemaker agora rodam na plataforma de contêineres do **podman**, com o recurso de pacote de contêineres disponível como uma Pré-visualização Tecnológica. Há uma exceção a este recurso que é a Technology Preview: A Red Hat suporta totalmente o uso de pacotes de Pacemaker para o Red Hat Openstack.

(BZ#1619620)

Heurística em **corosync-qdevice** disponível como uma Pré-visualização Tecnológica

Heurísticas são um conjunto de comandos executados localmente na inicialização, mudança de membros do cluster, conexão bem sucedida com **corosync-qnetd**, e, opcionalmente, periodicamente. Quando todos os comandos terminam com sucesso no prazo (seu código de erro de retorno é zero), a heurística passou; caso contrário, falhou. O resultado heurístico é enviado para **corosync-qnetd** onde é usado nos cálculos para determinar qual partição deve ser quorada.

(BZ#1784200)

Novo agente de vedação-agentes-heurístico-ping agente de vedação

Como uma prévia de tecnologia, a Pacemaker agora suporta o agente de **vedação_heurística_ping**. Este agente visa abrir uma classe de agentes de vedação experimentais que não fazem cercas de verdade por si mesmos, mas, em vez disso, exploram o comportamento dos níveis de cercas de uma nova maneira.

Se o agente heurístico for configurado no mesmo nível da vedação que o agente que faz a vedação real, mas é configurado antes desse agente em seqüência, a vedação emite uma ação **fora de** ação sobre o agente heurístico antes de tentar fazê-lo sobre o agente que faz a vedação. Se o agente heurístico der um resultado negativo para a ação de **vedação**, já está claro que o nível de vedação não será bem sucedido, fazendo com que a vedação Pacemaker salte a etapa de emissão da ação **de** vedação no agente que faz a vedação. Um agente de heurística pode explorar este comportamento para impedir que o agente que faz a vedação real de cercar um nó sob certas condições.

Um usuário pode querer usar este agente, especialmente em um agrupamento de dois nós, quando não faria sentido para um nó cercar o par se ele pudesse saber de antemão que não seria capaz de assumir os serviços adequadamente. Por exemplo, pode não fazer sentido para um nó assumir os serviços se ele tiver problemas para alcançar o uplink de rede, tornando os serviços inacessíveis aos clientes, uma situação que um ping para um roteador pode detectar nesse caso.

(BZ#1775847)

9.5. GESTÃO DA IDENTIDADE

Gerenciamento da Identidade JSON-RPC API disponível como Technology Preview

Um API está disponível para Gerenciamento de Identidade (IdM). Para visualizar o API, o IdM também fornece um navegador API como Technology Preview (Visualização de Tecnologia).

No Red Hat Enterprise Linux 7.3, o IdM API foi melhorado para permitir múltiplas versões de comandos API. Anteriormente, os aprimoramentos podiam mudar o comportamento de um comando de forma incompatível. Os usuários agora são capazes de continuar usando ferramentas e scripts existentes mesmo que a API do IdM mude. Isto permite:

- Administradores para usar versões anteriores ou posteriores do IdM no servidor do que no cliente gestor.
- Desenvolvedores para usar uma versão específica de uma chamada IdM, mesmo que a versão IdM mude no servidor.

Em todos os casos, a comunicação com o servidor é possível, independentemente se um dos lados utiliza, por exemplo, uma versão mais recente que introduz novas opções para um recurso.

Para obter detalhes sobre o uso da API, consulte [Utilização da API de Gerenciamento de Identidade para Comunicação com o Servidor IdM \(PREVISÃO TECNOLÓGICA\)](#).

(BZ#1664719)

DNSSEC disponível como Technology Preview na IdM

Os servidores de Gerenciamento de Identidade (IdM) com DNS integrado agora suportam Extensões de Segurança DNS (DNSSEC), um conjunto de extensões para o DNS que aumentam a segurança do protocolo DNS. As zonas DNS hospedadas nos servidores IdM podem ser automaticamente assinadas usando DNSSEC. As chaves criptográficas são geradas e giradas automaticamente.

Os usuários que decidirem proteger suas zonas DNS com DNSSEC são aconselhados a ler e seguir estes documentos:

- DNSSEC Práticas Operacionais, Versão 2: <http://tools.ietf.org/html/rfc6781#section-2>
- Guia de implantação do Sistema de Nomes de Domínio Seguros (DNS): <http://dx.doi.org/10.6028/NIST.SP.800-81-2>
- Considerações sobre o tempo de prorrogação do DNSSEC: <http://tools.ietf.org/html/rfc7583>

Observe que os servidores IdM com DNS integrado utilizam DNSSEC para validar as respostas DNS obtidas de outros servidores DNS. Isto pode afetar a disponibilidade de zonas DNS que não são configuradas de acordo com as práticas de nomenclatura recomendadas.

(BZ#1664718)

A verificação da saúde geral de sua infra-estrutura de chave pública está agora disponível como uma Pré-visualização Tecnológica

Com esta atualização, a ferramenta Healthcheck de infra-estrutura de chave pública (PKI) informa a saúde do subsistema PKI à ferramenta Healthcheck de Gerenciamento de Identidade (IdM), que foi introduzida no RHEL 8.1. A execução do IdM Healthcheck invoca o PKI Healthcheck, que coleta e

devolve o relatório de saúde do subsistema PKI.

A ferramenta **pki-healthcheck** está disponível em qualquer servidor ou réplica implantada da RHEL IdM. Todas as verificações fornecidas pelo **pki-healthcheck** também são integradas à ferramenta **ipa-healthcheck**. **ipa-healthcheck** pode ser instalado separadamente do fluxo do módulo **idm:DL1**.

Note que o **pki-healthcheck** também pode funcionar em uma infra-estrutura autônoma do Sistema de Certificado Red Hat (RHCS).

(BZ#1303254)

9.6. DESKTOP

O Desktop GNOME no ARM está disponível como uma Pré-visualização Tecnológica

O ambiente de trabalho GNOME está agora disponível como uma prévia tecnológica sobre a arquitetura ARM de 64 bits. Os usuários que requerem uma sessão gráfica para configurar e gerenciar seus servidores podem agora conectar-se a uma sessão gráfica remota rodando o Desktop GNOME usando VNC.

(BZ#1724302)

GNOME para a arquitetura ARM de 64 bits disponível como Technology Preview

O ambiente de trabalho GNOME está agora disponível para a arquitetura ARM de 64 bits como uma prévia tecnológica. Isto permite aos administradores configurar e gerenciar servidores a partir de uma interface gráfica de usuário (GUI) remotamente, usando a sessão VNC.

Como consequência, novas aplicações administrativas estão disponíveis na arquitetura ARM de 64 bits. Por exemplo: **Disk Usage Analyzer (baobab)**, **Firewall Configuration (firewall-config)**, **Red Hat Subscription Manager (gerenciador de assinaturas)**, ou o navegador **Firefox**. Usando **Firefox**, os administradores podem se conectar ao daemon local do Cockpit remotamente.

(JIRA:RHELPLAN-27394, BZ#1667516, BZ#1667225)

9.7. INFRA-ESTRUTURAS GRÁFICAS

Console remoto VNC disponível como Technology Preview para a arquitetura ARM de 64 bits

Na arquitetura ARM de 64 bits, o console remoto da Virtual Network Computing (VNC) está disponível como uma pré-visualização tecnológica. Observe que o resto da pilha de gráficos não está atualmente verificada para a arquitetura ARM de 64 bits.

(BZ#1698565)

9.8. FUNÇÕES DO SISTEMA RED HAT ENTERPRISE LINUX

O papel post-fix do Sistema RHEL Papéis disponíveis como Previsão Tecnológica

As Funções do Sistema Red Hat Enterprise Linux fornecem uma interface de configuração para os subsistemas do Red Hat Enterprise Linux, o que facilita a configuração do sistema através da inclusão de Funções Ansíveis. Esta interface permite o gerenciamento das configurações do sistema em múltiplas versões do Red Hat Enterprise Linux, bem como a adoção de novos lançamentos principais.

Os pacotes **rhel-system-roles** são distribuídos através do repositório AppStream.

A função **pós-fixa** está disponível como uma Pré-visualização Tecnológica.

Os seguintes papéis são plenamente apoiados:

- **kdump**
- **rede**
- **selinux**
- **armazenagem**
- **timesync**

Para mais informações, consulte o artigo da Base de Conhecimento sobre [os Papéis do Sistema RHEL](#) .

(BZ#1812552)

rhel-system-roles-sap disponível como uma Pré-visualização Tecnológica

O pacote **rhel-system-roles-sap** fornece as funções do sistema Red Hat Enterprise Linux (RHEL) para SAP, que pode ser usado para automatizar a configuração de um sistema RHEL para executar cargas de trabalho SAP. Estas funções reduzem muito o tempo de configuração de um sistema para executar cargas de trabalho SAP, aplicando automaticamente as configurações ideais que são baseadas nas melhores práticas descritas nas Notas SAP relevantes. O acesso é limitado às ofertas da RHEL para soluções SAP. Favor entrar em contato com o Suporte ao Cliente da Red Hat se você precisar de assistência com sua assinatura.

Os seguintes novos papéis no pacote **rhel-system-roles-sap** estão disponíveis como uma Pré-visualização Tecnológica:

- **sap-preconfigure**
- **sap-netweaver-preconfigure**
- **sap-hana-preconfigure**

Para mais informações, veja as [funções do sistema Red Hat Enterprise Linux para SAP](#) .

Nota: A RHEL 8.2 para SAP Solutions está programada para ser validada para uso com SAP HANA na arquitetura Intel 64 e IBM POWER9. O suporte para outras aplicações SAP e produtos de banco de dados, por exemplo, SAP NetWeaver e SAP ASE, estão vinculados a versões GA, e os clientes podem usar os recursos do RHEL 8.2 em GA. Favor consultar as Notas SAP 2369910 e 2235581 para obter as últimas informações sobre lançamentos validados e suporte SAP.

(BZ#1660832)

9.9. VIRTUALIZAÇÃO

Selecione adaptadores de rede Intel agora suportam SR-IOV em convidados da RHEL no Hyper-V

Como uma prévia tecnológica, os sistemas operacionais convidados do Red Hat Enterprise Linux rodando em um Hyper-V hypervisor podem agora usar o recurso de virtualização de E/S de raiz única (SR-IOV) para adaptadores de rede Intel suportados pelos drivers **ixgbevf** e **i40evf**. Este recurso é ativado quando as seguintes condições são atendidas:

- O suporte SR-IOV está habilitado para o controlador de interface de rede (NIC)
- O suporte SR-IOV está habilitado para o NIC virtual
- O suporte SR-IOV está habilitado para a chave virtual
- A função virtual (VF) do NIC é anexada à máquina virtual.

O recurso é atualmente suportado com o Microsoft Windows Server 2019 e 2016.

(BZ#1348508)

A virtualização da KVM é utilizável nas máquinas virtuais RHEL 8 Hyper-V

Como uma prévia de tecnologia, a virtualização KVM aninhada pode agora ser usada no hipervisor Microsoft Hyper-V. Como resultado, você pode criar máquinas virtuais em um sistema RHEL 8 para convidados rodando em um host Hyper-V.

Note que atualmente, esta característica só funciona em sistemas Intel. Além disso, a virtualização aninhada não está, em alguns casos, habilitada por padrão no Hyper-V. Para habilitá-la, veja a seguinte documentação da Microsoft:

<https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization>

(BZ#1519039)

AMD SEV para máquinas virtuais KVM

Como uma prévia de tecnologia, a RHEL 8 introduz o recurso Secure Encrypted Virtualization (SEV) para máquinas host AMD EPYC que utilizam o hipervisor KVM. Se ativada em uma máquina virtual (VM), a SEV criptografa a memória da VM para que o host não possa acessar os dados na VM. Isto aumenta a segurança da VM se o host for infectado com sucesso por malware.

Observe que o número de VMs que podem usar este recurso de cada vez em um único host é determinado pelo hardware do host. Os processadores AMD EPYC atuais suportam até 509 VMs rodando usando SEV.

Observe também que para VMs com SEV configuradas para poder inicializar, você também deve configurar a VM com um limite de memória dura. Para isso, adicione o seguinte à configuração XML da VM:

```
<memtune>
<hard_limit unit='KiB'>N</hard_limit>
</memtune>
```

O valor recomendado para N é igual ou maior que o RAM 256 MiB do convidado. Por exemplo, se ao convidado for atribuído 2 RAM GiB, N deve ser 2359296 ou maior.

(BZ#1501618, BZ#1501607, JIRA:RHELPLAN-7677)

Intel vGPU

Como uma prévia de tecnologia, agora é possível dividir um dispositivo físico Intel GPU em múltiplos dispositivos virtuais chamados de **dispositivos mediados**. Estes dispositivos mediados podem então ser atribuídos a múltiplas máquinas virtuais (VMs) como GPUs virtuais. Como resultado, estas VMs compartilham a performance de uma única GPU física da Intel.

Observe que apenas as GPUs Intel selecionadas são compatíveis com o recurso vGPU. Além disso, atribuir uma GPU física às VMs torna impossível para o host utilizar a GPU, e pode impedir que a saída de exibição gráfica no host funcione.

(BZ#1528684)

9.10. CONTÊINERES

a imagem do contêiner **skopeo** está disponível como uma Pré-visualização Tecnológica

A imagem do contêiner **registry.redhat.io/rhel8/skopeo** é uma implementação contentorizada do pacote **skopeo**. O **skopeo** é uma ferramenta de linha de comando que realiza várias operações em imagens de contêineres e repositórios de imagens. Esta imagem de contêiner permite inspecionar e copiar imagens de contêineres de um registro de contêineres não autenticado para outro.

(BZ#1627900)

a imagem do container **buildah** está disponível como uma Technology Preview

A imagem do container **registry.redhat.io/rhel8/buildah** é uma implementação em container do pacote **buildah**. O **buildah** é uma ferramenta que facilita a construção de imagens de contêineres OCI. Esta imagem de container permite que você construa imagens de container sem a necessidade de instalar o pacote **buildah** em seu sistema. O caso de uso não cobre a execução desta imagem no modo rootless como um usuário não-root.

(BZ#1627898)

CAPÍTULO 10. FUNCIONALIDADE DEPRECIADA

Esta parte fornece uma visão geral da funcionalidade que tem sido *deprecated* no Red Hat Enterprise Linux 8.2.

A funcionalidade *deprecated* continua a ser suportada até o final da vida útil do Red Hat Enterprise Linux 8. A funcionalidade *deprecated* provavelmente não será suportada em futuros lançamentos importantes deste produto e não é recomendada para novas implementações. Para a lista mais recente de funcionalidades obsoletas dentro de um lançamento principal em particular, consulte a versão mais recente da documentação de lançamento.

Os componentes de hardware obsoletos não são recomendados para novas implementações nos principais lançamentos atuais ou futuros. As atualizações de drivers de hardware são limitadas apenas à segurança e reparos críticos. A Red Hat recomenda a substituição deste hardware tão logo seja razoavelmente viável.

Um pacote pode ser depreciado e não recomendado para uso posterior. Sob certas circunstâncias, uma embalagem pode ser retirada de um produto. A documentação do produto identifica então pacotes mais recentes que oferecem funcionalidade semelhante, idêntica ou mais avançada que a depreciada, e fornece outras recomendações.

Para informações sobre funcionalidades que estão presentes no RHEL 7, mas que foram *removed* no RHEL 8, veja [Considerações sobre a adoção do RHEL 8](#).

10.1. INSTALADOR E CRIAÇÃO DE IMAGEM

Vários comandos e opções de Kickstart foram depreciados

Usando os seguintes comandos e opções nos arquivos Kickstart RHEL 8, será impresso um aviso nos logs.

- **auth** ou **authconfig**
- **dispositivo**
- **deviceprobe**
- **dmraid**
- **instalar**
- **lilo**
- **lilocheck**
- **mouse**
- **multipath**
- **bootloader - atualização**
- **ignorados --interactivos**
- **partição --ativa**
- **reinicialização --kexec**

Onde apenas opções específicas são listadas, o comando base e suas outras opções ainda estão disponíveis e não são depreciadas.

Para mais detalhes e mudanças relacionadas ao Kickstart, consulte a seção [Kickstart changes](#) do documento *Considerations in adopting RHEL 8*.

(BZ#1642765)

A opção `--interativa` do comando Kickstart ignorado foi depreciada

O uso da **opção `--interativa`** em futuros lançamentos do Red Hat Enterprise Linux resultará em um erro fatal de instalação. É recomendado modificar seu arquivo Kickstart para remover a opção.

(BZ#1637872)

10.2. GESTÃO DE SOFTWARE

`rpmbuild --sign` é depreciado

Com esta atualização, o comando **`rpmbuild --sign`** tornou-se depreciado. O uso deste comando em futuros lançamentos do Red Hat Enterprise Linux pode resultar em um erro. É recomendado que você use o comando **`rpmsign`** em seu lugar.

(BZ#1688849)

10.3. SEGURANÇA

As cifras doNSS SEED são depreciadas

A biblioteca do Mozilla Network Security Services(**NSS**) não suportará os conjuntos de cifras TLS que usam uma cifra SEED em um lançamento futuro. Para implantações que dependem de cifras SEED, a Red Hat recomenda habilitar o suporte para outras suítes de cifras. Desta forma, você garante transições suaves quando o NSS removerá o suporte a elas.

Observe que as cifras SEED já estão desativadas por padrão na RHEL.

(BZ#1817533)

TLS 1.0 e TLS 1.1 são depreciados

Os protocolos TLS 1.0 e TLS 1.1 estão desabilitados no nível da política criptográfica do sistema **DEFAULT**. Se seu cenário, por exemplo, uma aplicação de videoconferência no navegador Firefox, exigir o uso dos protocolos depreciados, mude a política criptográfica de todo o sistema para o nível **LEGACY**:

```
# update-crypto-policies --set LEGACY
```

Para mais informações, veja o artigo da base de conhecimento [Strong crypto defaults no RHEL 8 e a depreciação de algoritmos criptográficos fracos](#) no Portal do Cliente da Red Hat e a página man **`update-crypto-policies(8)`**.

(BZ#1660839)

A DSA é depreciada no RHEL 8

O Algoritmo de Assinatura Digital (DSA) é considerado depreciado no Red Hat Enterprise Linux 8. Os mecanismos de autenticação que dependem das chaves DSA não funcionam na configuração default.

Note que os clientes **OpenSSH** não aceitam chaves de host DSA mesmo no nível da política criptográfica do sistema **LEGACY**.

(BZ#1646541)

SSL2 Cliente Olá foi depreciado no NSS

A versão 1.2 e anterior do protocolo Transport Layer Security(**TLS**) permite iniciar uma negociação com um **Cliente** Mensagem de **Alô** formatada de forma retrocompatível com o protocolo Secure Sockets Layer(**SSL**) versão 2. O suporte a este recurso na biblioteca de Serviços de Segurança de Rede (**NSS**) foi depreciado e está desativado por padrão.

As aplicações que requerem suporte para este recurso precisam usar a nova API **SSL_ENABLE_V2_COMPATIBLE_HELLO** API para habilitá-la. O suporte para este recurso pode ser removido completamente em futuros lançamentos do Red Hat Enterprise Linux 8.

(BZ#1645153)

TPM 1.2 é depreciado

A versão padrão do processador criptográfico seguro Trusted Platform Module (TPM) foi atualizada para a versão 2.0 em 2016. O TPM 2.0 oferece muitas melhorias em relação ao TPM 1.2, e não é retrocompatível com a versão anterior. O TPM 1.2 é depreciado no RHEL 8, e pode ser removido no próximo grande lançamento.

(BZ#1657927)

10.4. TRABALHO EM REDE

Os roteiros de rede são depreciados no RHEL 8

Os scripts de rede são depreciados no Red Hat Enterprise Linux 8 e não são mais fornecidos por default. A instalação básica fornece uma nova versão dos scripts **ifup** e **ifdown** que chamam o serviço **NetworkManager** através da ferramenta **nmcli**. No Red Hat Enterprise Linux 8, para rodar os scripts **ifup** e **ifdown**, o NetworkManager deve estar rodando.

Observe que comandos personalizados em **/sbin/ifup-local**, **ifdown-pre-local** e **ifdown-local** scripts não são executados.

Se algum destes scripts for necessário, a instalação dos scripts de rede depreciados no sistema ainda é possível com o seguinte comando:

```
~]# yum instalar os roteiros de rede
```

Os scripts **ifup** e **ifdown** se ligam aos scripts de rede legados instalados.

Chamando os scripts da rede legada mostra um aviso sobre sua desvalorização.

(BZ#1647725)

10.5. KERNEL

A instalação do RHEL para Real Time 8 usando a bota sem disco é agora depreciada

A inicialização sem disco permite que vários sistemas compartilhem um sistema de arquivos raiz através da rede. Embora conveniente, o diskless boot é penoso a introduzir a latência da rede em cargas de

trabalho em tempo real. Com uma atualização menor futura do RHEL para Real Time 8, o recurso de inicialização diskless não será mais suportado.

(BZ#1748980)

O motorista **qla3xxx** é depreciado

O driver **qla3xxx** foi depreciado no RHEL 8. O driver provavelmente não será suportado em futuros lançamentos importantes deste produto e, portanto, não é recomendado para novas implantações.

(BZ#1658840)

Os motoristas **dl2k**, **dnet**, **ethoc**, e **dlci** são depreciados

Os motoristas **dl2k**, **dnet**, **ethoc** e **dlci** foram depreciados no RHEL 8. Os motoristas provavelmente não serão apoiados em grandes lançamentos futuros deste produto e, portanto, não são recomendados para novas implantações.

(BZ#1660627)

10.6. SISTEMAS DE ARQUIVO E ARMAZENAMENTO

O parâmetro da linha de comando do kernel **do elevador** é depreciado

O parâmetro de linha de comando do kernel **do elevador** foi usado em versões anteriores do RHEL para definir o programador de discos para todos os dispositivos. No RHEL 8, o parâmetro é depreciado.

O kernel Linux a montante removeu o suporte para o parâmetro **elevador**, mas ainda está disponível no RHEL 8 por razões de compatibilidade.

Observe que o kernel seleciona um programador de disco padrão com base no tipo de dispositivo. Esta é tipicamente a configuração ideal. Se você precisar de um agendador diferente, a Red Hat recomenda que você use as regras do **udev** ou o serviço Tuned para configurá-lo. Combine os dispositivos selecionados e troque o agendador somente para esses dispositivos.

Para mais informações, consulte [Ajuste do agendador de discos](#).

(BZ#1665295)

O espelho LVM é depreciado

O tipo de segmento **espelho** LVM está agora depreciado. O suporte ao **espelho** será removido em um futuro grande lançamento da RHEL.

A Red Hat recomenda que você use dispositivos LVM RAID 1 com um segmento tipo de **raid1** ao invés de **espelho**. O tipo de segmento **raid1** é o tipo de configuração RAID padrão e substitui o **espelho** como a solução recomendada.

Para converter dispositivos **espelhados** em **raid1**, veja [Conversão de um dispositivo LVM espelhado em um dispositivo RAID1](#).

O **espelho** LVM tem vários problemas conhecidos. Para detalhes, veja os [problemas conhecidos em sistemas de arquivos e armazenamento](#).

(BZ#1827628)

O NFSv3 sobre UDP foi desativado

O servidor NFS não abre mais ou escuta em um soquete do User Datagram Protocol (UDP) por padrão. Esta mudança afeta apenas a versão 3 do NFS porque a versão 4 requer o Protocolo de Controle de Transmissão (TCP).

O NFS sobre o UDP não é mais suportado no RHEL 8.

(BZ#1592011)

10.7. DESKTOP

A biblioteca de pirâmides de librogênios foi desativada

A biblioteca **libgnome-keyring** foi depreciada em favor da biblioteca **libsecret**, pois a **libgnome-keyring** não é mantida a montante, e não segue as políticas criptográficas necessárias para a RHEL. A nova biblioteca **libsecret** é a substituição que segue os padrões de segurança necessários.

(BZ#1607766)

10.8. INFRA-ESTRUTURAS GRÁFICAS

As placas gráficas AGP não são mais suportadas

Placas gráficas usando o barramento Accelerated Graphics Port (AGP) não são suportadas no Red Hat Enterprise Linux 8. Use as placas gráficas com o barramento PCI-Express como a substituição recomendada.

(BZ#1569610)

10.9. O CONSOLE WEB

O console web não suporta mais traduções incompletas

O console web RHEL não fornece mais traduções para os idiomas que têm traduções disponíveis para menos de 50% das cordas traduzíveis do Console. Se o navegador solicitar a tradução para tal idioma, a interface do usuário será em inglês.

(BZ#1666722)

10.10. VIRTUALIZAÇÃO

virt-manager foi depreciado

O aplicativo Virtual Machine Manager, também conhecido como **virt-manager**, foi desativado. O console web RHEL 8, também conhecido como **Cockpit**, tem a intenção de se tornar seu substituto em um lançamento posterior. É, portanto, recomendado que você utilize o console web para gerenciar a virtualização em uma GUI. Observe, entretanto, que alguns recursos disponíveis em **virt-manager** podem ainda não estar disponíveis no console web RHEL 8.

(JIRA:RHELPLAN-10304)

Snapshots de máquinas virtuais não são devidamente suportados no RHEL 8

O atual mecanismo de criação de instantâneos de máquinas virtuais (VM) foi depreciado, pois não está funcionando de forma confiável. Como consequência, recomenda-se não utilizar instantâneos de VM no RHEL 8.

Observe que um novo mecanismo de instantâneo da VM está em desenvolvimento e será totalmente implementado em um futuro lançamento menor da RHEL 8.

([BZ#1686057](#))

O tipo de GPU virtual Cirrus VGA foi depreciado

Com uma futura grande atualização do Red Hat Enterprise Linux, o dispositivo GPU **Cirrus VGA** não será mais suportado nas máquinas virtuais KVM. Portanto, a Red Hat recomenda o uso dos dispositivos **stdvga**, **virtio-vga**, ou **qxl** ao invés do Cirrus VGA.

(BZ#1651994)

O modelo de CPU **cpu64-rhel6** foi depreciado e removido

O modelo de CPU virtual **cpu64-rhel6** QEMU foi depreciado na RHEL 8.1, e foi removido da RHEL 8.2. Recomenda-se o uso dos outros modelos de CPU fornecidos pela QEMU e libvirt, de acordo com a CPU presente na máquina hospedeira.

(BZ#1741346)

10.11. PACOTES DEPRECIADOS

Os seguintes pacotes foram depreciados e provavelmente não serão incluídos em um futuro grande lançamento do Red Hat Enterprise Linux:

- 389-ds-base-legacy-tools
- authd
- custodia
- hostname
- libidn
- net-tools
- textos em rede
- nss-pam-ldapd
- sendmail
- yp-tools
- ypbind
- ypserv

CAPÍTULO 11. PROBLEMAS CONHECIDOS

Esta parte descreve questões conhecidas no Red Hat Enterprise Linux 8.2.

11.1. INSTALADOR E CRIAÇÃO DE IMAGEM

Os comandos `auth` e `authconfig` Kickstart requerem o repositório AppStream

O pacote `authselect-compat` é exigido pelos comandos `auth` e `authconfig` Kickstart durante a instalação. Sem este pacote, a instalação falha se o `auth` ou `authconfig` forem usados. Entretanto, por projeto, o pacote `authselect-compat` está disponível apenas no repositório AppStream.

Para contornar este problema, verifique se os repositórios BaseOS e AppStream estão disponíveis para o instalador ou use o comando Kickstart `authselect` durante a instalação.

(BZ#1640697)

Os comandos `reboot --kexec` e `inst.kexec` não fornecem um estado previsível do sistema

Realizar uma instalação RHEL com o comando de **reinicialização** `--kexec` Kickstart ou os parâmetros de inicialização do kernel `inst.kexec` não fornecem o mesmo estado previsível do sistema que uma reinicialização completa. Como consequência, mudar para o sistema instalado sem reinicialização pode produzir resultados imprevisíveis.

Note que a característica `kexec` é depreciada e será removida em um futuro lançamento do Red Hat Enterprise Linux.

(BZ#1697896)

A instalação do Anaconda inclui baixos limites de recursos mínimos para a definição dos requisitos

O Anaconda inicia a instalação em sistemas com o mínimo de recursos necessários disponíveis e não fornece aviso prévio de mensagens sobre os recursos necessários para realizar a instalação com sucesso. Como resultado, a instalação pode falhar e os erros de saída não fornecem mensagens claras para uma possível depuração e recuperação. Para contornar este problema, certifique-se de que o sistema tenha as configurações mínimas de recursos necessários para a instalação: 2GB de memória em PPC64(LE) e 1GB em x86_64. Como resultado, deve ser possível realizar uma instalação bem sucedida.

(BZ#1696609)

A instalação falha ao usar o comando `reboot --kexec`

A instalação do RHEL 8 falha ao utilizar um arquivo Kickstart que contém o comando `reboot --kexec`. Para evitar o problema, use o comando `reboot` ao invés de `reiniciar --kexec` em seu arquivo Kickstart.

(BZ#1672405)

A configuração inicial do RHEL 8 não pode ser feita via SSH

Atualmente, a interface de configuração inicial do RHEL 8 não é exibida quando conectado ao sistema usando SSH. Como consequência, é impossível realizar a configuração inicial em uma máquina RHEL 8 gerenciada via SSH. Para contornar este problema, realize a configuração inicial no console principal do sistema (ttySO) e, posteriormente, efetue o log in usando SSH.

(BZ#1676439)

O acesso à rede não é habilitado por padrão no programa de instalação

Vários recursos de instalação exigem acesso à rede, por exemplo, registro de um sistema usando a Rede de Entrega de Conteúdo (CDN), suporte ao servidor NTP e fontes de instalação de rede. Entretanto, o acesso à rede não é habilitado por padrão e, como resultado, estes recursos não podem ser usados até que o acesso à rede seja habilitado.

Para contornar este problema, adicione **ip=dhcp** às opções de inicialização para permitir o acesso à rede quando a instalação for iniciada. Opcionalmente, a passagem de um arquivo Kickstart ou um repositório localizado na rede usando opções de inicialização também resolve o problema. Como resultado, os recursos de instalação baseados na rede podem ser usados.

(BZ#1757877)

O registro falha para contas de usuários que pertencem a múltiplas organizações

Atualmente, quando você tenta registrar um sistema com uma conta de usuário que pertence a várias organizações, o processo de registro falha com a mensagem de erro **You must specify an organization for new units**.

Para contornar este problema, você pode trabalhar em ambos:

- Use uma conta de usuário diferente que não pertença a múltiplas organizações.
- Use o método de autenticação **Activation Key** disponível no recurso Connect to Red Hat para instalações GUI e Kickstart.
- Pule a etapa de registro em Connect to Red Hat e use o Subscription Manager para registrar seu sistema pós-instalação.

(BZ#1822880)

Uma instalação GUI utilizando a imagem ISO do DVD Binário às vezes não pode prosseguir sem o registro CDN

Ao executar uma instalação GUI usando o arquivo de imagem ISO do DVD Binário, uma condição de corrida no instalador pode, às vezes, impedir que a instalação prossiga até que você registre o sistema usando o recurso Conectar à Red Hat. Para contornar este problema, complete os seguintes passos:

1. Selecione **Installation Source** na janela **Installation Summary** da instalação da GUI.
2. Verifique se **Auto-detected installation media** está selecionado.
3. Clique em **Done** para confirmar a seleção e retornar à janela **Installation Summary**.
4. Verifique se **Local Media** é exibido como o status **Installation Source** na janela **Installation Summary**.

Como resultado, você pode prosseguir com a instalação sem registrar o sistema usando o recurso Conectar à Red Hat.

(BZ#1823578)

Copiar o conteúdo do arquivo Binário DVD.iso para uma partição omite os arquivos **.treeinfo** e **.discinfo**

Durante a instalação local, ao copiar o conteúdo do DVD.iso binário RHEL 8 para uma partição, o * no comando **cp <path>/^* <mounted partition>/dir** não copia os arquivos **.treeinfo** e **.discinfo**. Estes

arquivos são necessários para uma instalação bem sucedida. Como resultado, os repositórios BaseOS e AppStream não são carregados, e uma mensagem de log relacionada a depuração no arquivo **anaconda.log** é o único registro do problema.

Para contornar o problema, copie os arquivos **.treeinfo** e **.discinfo** que faltam para a partição.

(BZ#1687747)

O servidor HTTPS autoassinado não pode ser usado na instalação Kickstart

Atualmente, o instalador falha na instalação a partir de um servidor https autoassinado quando a fonte de instalação é especificada no arquivo kickstart e a opção **--noverifyssl** é utilizada:

```
url --url=https://SERVER/PATH --noverifyssl
```

Para contornar este problema, anexe o parâmetro **inst.noverifyssl** à linha de comando do kernel ao iniciar a instalação do kickstart.

Por exemplo:

```
inst.ks=<URL> inst.noverifyssl
```

(BZ#1745064)

A instalação da GUI pode falhar se for feita uma tentativa de cancelar o registro usando o CDN antes que a atualização do repositório seja concluída

No RHEL 8.2, ao registrar seu sistema e anexar assinaturas usando a Rede de Entrega de Conteúdo (CDN), uma atualização dos metadados do repositório é iniciada pelo programa de instalação da GUI. O processo de atualização não faz parte do processo de registro e assinatura, e como consequência, o botão **Unregister** é habilitado na janela **Connect to Red Hat**. Dependendo da conexão de rede, o processo de atualização pode levar mais de um minuto para ser concluído. Se você clicar no botão **Unregister** antes de concluir o processo de atualização, a instalação da GUI pode falhar, pois o processo de não registro remove os arquivos do repositório CDN e os certificados exigidos pelo programa de instalação para se comunicar com o CDN.

Para contornar este problema, complete as seguintes etapas na instalação da GUI depois de clicar no botão **Register** na janela **Connect to Red Hat**:

1. A partir da janela **Connect to Red Hat**, clique **Done** para retornar à janela **Installation Summary**.
2. A partir da janela **Installation Summary**, verifique se as mensagens de status em itálico **Installation Source** e **Software Selection** não estão exibindo nenhuma informação de processamento.
3. Quando as categorias Fonte de Instalação e Seleção de Software estiverem prontas, clique em **Connect to Red Hat**.
4. Clique no botão **Unregister**.

Depois de executar estas etapas, você pode desregistrar o sistema com segurança durante a instalação da GUI.

(BZ#1821192)

11.2. GESTÃO DE ASSINATURAS

os addons syspurpose addons não têm efeito sobre o gerenciador de assinaturas anexar --auto saída.

No Red Hat Enterprise Linux 8, quatro atributos da ferramenta de linha de comando **syspurpose** foram adicionados: **role,use, service_level_agreement** e **addons**. Atualmente, apenas **role, usage** e **service_level_agreement** afetam a saída da execução do **gerenciador de assinatura anexado --auto** comando. Os usuários que tentarem definir valores para o argumento **dos addons** não observarão qualquer efeito nas assinaturas que são auto-atribuídas.

([BZ#1687900](#))

Os dados dos dispositivos de armazenamento multi-path são perdidos ao instalar o RHEL usando um arquivo Kickstart

Os dados dos dispositivos de armazenamento multi-path que estão conectados a um host são perdidos ao instalar o RHEL usando um arquivo Kickstart. Este problema ocorre porque o instalador não ignora os dispositivos de armazenamento multi-path que você especifica usando o comando **ignoredisk --drives**. Como resultado, os dados sobre os dispositivos são perdidos.

Para contornar este problema, desprenda os dispositivos antes da instalação, ou use o comando de **uso ignorado -- somente para** especificar os dispositivos para instalação.

([BZ#1862131](#))

11.3. CONCHAS E FERRAMENTAS DE LINHA DE COMANDO

As aplicações que utilizam o protocolo Wayland não podem ser encaminhadas para servidores de exibição remota

No Red Hat Enterprise Linux 8, a maioria das aplicações usa o protocolo Wayland por default ao invés do protocolo X11. Como consequência, o servidor ssh não pode encaminhar as aplicações que usam o protocolo Wayland, mas é capaz de encaminhar as aplicações que usam o protocolo X11 para um servidor de exibição remota.

Para contornar este problema, defina a variável de ambiente **GDK_BACKEND=x11** antes de iniciar as aplicações. Como resultado, a aplicação pode ser encaminhada para servidores de exibição remota.

([BZ#1686892](#))

systemd-resolved.service não inicia na inicialização

O serviço **resolvido pelo sistema** ocasionalmente não inicia na inicialização. Se isto acontecer, reinicie o serviço manualmente após o boot terminar, usando o seguinte comando:

```
# systemctl start sistema-resolvido
```

No entanto, a falha do **sistema resolvido** na inicialização não afeta nenhum outro serviço.

([BZ#1640802](#))

11.4. SEGURANÇA

Relógios executáveis de auditoria em links simbólicos não funcionam

O monitoramento de arquivos fornecido pela opção **-w** não pode rastrear diretamente um caminho. Ele tem que resolver o caminho para um dispositivo e um inode para fazer uma comparação com o programa executado. Um relógio monitorando um symlink executável monitora o dispositivo e um inode do próprio symlink ao invés do programa executado em memória, que é encontrado a partir da resolução do symlink. Mesmo que o relógio resolva o link simbólico para obter o programa executável resultante, a regra aciona em qualquer binário de chamadas múltiplas chamado de um link simbólico diferente. Isto resulta em registros de inundação com falsos positivos. Conseqüentemente, os relógios executáveis de auditoria em links simbólicos não funcionam.

Para contornar o problema, monte um relógio para o caminho resolvido do executável do programa e filtre as mensagens de registro resultantes usando o último componente listado nos campos **comm=** ou **proctitle=**.

(BZ#1846345)

SELINUX=desabilitado em /etc/selinux/config não funciona corretamente

Desabilitar o SELinux utilizando a opção **SELINUX=disabled** no **/etc/selinux/config** resulta em um processo no qual o kernel inicia com o SELinux habilitado e muda para o modo desabilitado mais tarde no processo de inicialização. Isto pode causar vazamentos de memória e condições de corrida e, conseqüentemente, também pânico no kernel.

Para contornar este problema, desative o SELinux adicionando o parâmetro **selinux=0** à linha de comando do kernel, conforme descrito na seção [Mudando os modos SELinux no momento da inicialização](#) da seção [Utilizando](#) o título [SELinux](#), se seu cenário realmente precisar desativar completamente o SELinux.

(JIRA:RHELPLAN-34199)

libselinux-python só está disponível através de seu módulo

O pacote **libselinux-python** contém apenas ligas Python 2 para o desenvolvimento de aplicações SELinux e é usado para compatibilidade retroativa. Por esta razão, **libselinux-python** não está mais disponível nos repositórios padrão RHEL 8 através do comando **dnf install libselinux-python**.

Para contornar este problema, habilite os módulos **libselinux-python** e **python27**, e instale o pacote **libselinux-python** e suas dependências com os seguintes comandos:

```
# dnf module enable libselinux-python
# dnf install libselinux-python
```

Alternativamente, instale **libselinux-python** usando seu perfil de instalação com um único comando:

```
# módulo dnf instalar libselinux-python:2.8/comum
```

Como resultado, você pode instalar **libselinux-python** usando o respectivo módulo.

(BZ#1666328)

udica processa recipientes UBI 8 somente quando iniciada com --env container=podman

Os recipientes Red Hat Universal Base Image 8 (UBI 8) definem a variável de ambiente do **recipiente** para o valor **oci** ao invés do valor **podman**. Isto impede que a ferramenta **udica** analise um arquivo JavaScript Object Notation (JSON) de um recipiente.

Para contornar este problema, inicie um container UBI 8 usando um comando **podman** com o parâmetro **--env container=podman**. Como resultado, **a udica** pode gerar uma política SELinux para um contêiner UBI 8 somente quando você utiliza o workaround descrito.

(BZ#1763210)

A remoção da embalagem **rpm-plugin-selinux** leva à remoção de todas as embalagens de **selinux-policy** do sistema

A remoção do pacote **rpm-plugin-selinux** desabilita a SELinux na máquina. Também remove todas as embalagens de **selinux-policy** do sistema. Instalação repetida do pacote **rpm-plugin-selinux**, então instala a política **SELinux-policy-minimum** SELinux, mesmo que a política **selinux-policy-target** estivesse previamente presente no sistema. Entretanto, a instalação repetida não atualiza o arquivo de configuração do SELinux para contabilizar a mudança na política. Como consequência, o SELinux é desativado mesmo após a reinstalação do pacote **rpm-plugin-selinux**.

Trabalhar em torno deste problema:

1. Digite o comando **umount /sys/fs/selinux/**.
2. Instalar manualmente o pacote **de selinux** que faltava.
3. Edite o arquivo **/etc/selinux/config** para que a política seja igual a **SELINUX=enforcing**.
4. Digite o comando **load_policy -i**.

Como resultado, a SELinux está habilitada e executando a mesma política que antes.

(BZ#1641631)

SELinux impede que o **systemd-journal-gatewayd** chame **newfstat()** em arquivos de memória compartilhada criados pela **corosync**

A política SELinux não contém uma regra que permita que o daemon do **systema-journal-gatewayd** tenha acesso aos arquivos criados pelo serviço **corosync**. Como consequência, o SELinux nega a função **systemd-journal-gatewayd** para chamar a função **newfstat()** nos arquivos de memória compartilhada criados pela **corosync**.

Para contornar este problema, crie um módulo de política local com uma regra de permissão que possibilite o cenário descrito. Consulte a página de manual **audit2allow(1)** para mais informações sobre como gerar a política SELinux *allow* e *dontaudit* regras. Como resultado do trabalho anterior, o **systemd-journal-gatewayd** pode chamar a função em arquivos de memória compartilhada criados pela **corosync** com o SELinux em modo de aplicação.

(BZ#1746398)

SELinux impede que a auditoria interrompa ou desligue o sistema

A política SELinux não contém uma regra que permita que o daemon de Auditoria inicie uma unidade do **systema power_unit_file_t**. Conseqüentemente, **a Auditd** não pode parar ou desligar o sistema mesmo quando configurada para fazê-lo em casos como o de não sobrar espaço em uma partição de disco de registro.

Para contornar este problema, crie um módulo de política SELinux personalizado. Como resultado, **a auditoria** pode parar ou desligar corretamente o sistema somente se você aplicar a solução.

(BZ#1826788)

os usuários podem executar comandos `sudo` como usuários bloqueados

Em sistemas onde as permissões **dos sudoers** são definidas com a palavra-chave **ALL**, os usuários **sudo** com permissões podem executar comandos **sudo** como usuários cujas contas estão bloqueadas. Conseqüentemente, as contas bloqueadas e expiradas ainda podem ser usadas para executar comandos.

Para contornar este problema, habilite a opção **runas_check_shell** recentemente implementada junto com as configurações apropriadas de shells válidas em **/etc/shells**. Isto impede que os atacantes executem comandos sob contas de sistema, como **bin**.

(BZ#1786990)

Efeitos negativos da configuração padrão de registro sobre o desempenho

A configuração padrão do ambiente de registro pode consumir 4 GB de memória ou até mais e os ajustes dos valores limite de taxa são complexos quando o **sistema-journald** está rodando com o **rsyslog**.

Veja os [efeitos negativos da configuração de registro padrão da RHEL sobre o desempenho e suas mitigações](#) Artigo da Base de Conhecimento para mais informações.

(JIRA:RHELPLAN-10431)

Parâmetro erro não conhecidos na saída do `rsyslog` com `config.enabled`

Na saída do **rsyslog**, ocorre um erro inesperado no processamento da configuração usando a diretiva **config.enabled**. Como conseqüência, os erros **não conhecidos** são exibidos durante o uso da diretiva **config.enabled**, exceto para as instruções **include()**.

Para contornar este problema, defina **config.enabled=on** ou use as declarações **()**.

(BZ#1659383)

Certas cordas prioritárias `rsyslog` não funcionam corretamente

O suporte para a cadeia de prioridade **GnuTLS** para **imtcp** que permite um controle fino sobre a criptografia não está completo. Conseqüentemente, as seguintes cadeias de prioridade não funcionam corretamente no **rsyslog**:

```
NENHUMA: VERS-ALL:-VERS-TLS1.3: MAC-ALL: DHE-RSA: AES-256-GCM: SIGN-RSA-SHA384:
COMP-ALL: GROUP-ALL
```

Para contornar este problema, use apenas cordas de prioridade que funcionem corretamente:

```
NENHUMA: VERS-ALL:-VERS-TLS1.3: MAC-ALL: ECDHE-RSA: AES-128-CBC: SIGN-RSA-SHA1:
COMP-ALL: GROUP-ALL
```

Como resultado, as configurações atuais devem ser limitadas às cordas que funcionam corretamente.

(BZ#1679512)

As conexões a servidores com assinaturas SHA-1 não funcionam com **GnuTLS**

As assinaturas SHA-1 nos certificados são rejeitadas pela biblioteca de comunicações seguras **GnuTLS** como inseguras. Conseqüentemente, as aplicações que usam **GnuTLS** como backend TLS não podem estabelecer uma conexão TLS com os colegas que oferecem tais certificados. Este comportamento é

inconsistente com outras bibliotecas criptográficas do sistema. Para contornar este problema, atualize o servidor para usar certificados assinados com SHA-256 ou hash mais forte, ou mude para a política LEGACY.

(BZ#1628553)

TLS 1.3 não funciona em NSS no modo FIPS

O TLS 1.3 não é suportado em sistemas que funcionam no modo FIPS. Como resultado, as conexões que requerem o TLS 1.3 para interoperabilidade não funcionam em um sistema que trabalha em modo FIPS.

Para ativar as conexões, desabilite o modo FIPS do sistema ou habilite o suporte para TLS 1.2 no par.

(BZ#1724250)

OpenSSL manipula incorretamente as fichas PKCS #11 que não suportam assinaturas RSA ou RSA-PSS brutas

A biblioteca **OpenSSL** não detecta as capacidades relacionadas às chaves de fichas PKCS #11. Conseqüentemente, o estabelecimento de uma conexão TLS falha quando uma assinatura é criada com um token que não suporta assinaturas RSA ou RSA-PSS brutas.

Para contornar o problema, adicione as seguintes linhas após a linha **.include** no final da seção **crypto_policy** no arquivo **/etc/pki/tls/openssl.cnf**:

```
SignatureAlgorithms =  
RSA+SHA256:RSA+SHA512:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA512:ECDSA+SHA384  
MaxProtocol = TLSv1.2
```

Como resultado, uma conexão TLS pode ser estabelecida no cenário descrito.

(BZ#1685470)

OpenSSL gera uma extensão de **status_request** malformado na mensagem **CertificateRequest** no TLS 1.3

Os servidores OpenSSL enviam uma extensão mal-formada **status_request** na mensagem **CertificateRequest** se o suporte para a extensão **status_request** e autenticação baseada no certificado do cliente estiverem habilitados. Nesse caso, o OpenSSL não interopera com implementações que estejam em conformidade com o protocolo **RFC 8446**. Como resultado, os clientes que verificam corretamente as extensões na mensagem **CertificateRequest** abortam as conexões com o servidor OpenSSL. Para contornar este problema, desabilite o suporte para o protocolo TLS 1.3 em ambos os lados da conexão ou desabilite o suporte para **status_request** no servidor OpenSSL. Isto evitará que o servidor envie mensagens mal-formadas.

(BZ#1749068)

o **ssh-keyscan** não pode recuperar chaves RSA de servidores em modo FIPS

O algoritmo **SHA-1** é desativado para assinaturas RSA no modo FIPS, o que impede que o utilitário **ssh-keyscan** recupere chaves RSA de servidores que operam nesse modo.

Para contornar este problema, use chaves ECDSA, ou recupere as chaves localmente do arquivo **/etc/ssh/ssh_host_rsa_chave.pub** no servidor.

(BZ#1744108)

Libreswan não funciona corretamente com `seccomp=enabled` em todas as configurações

O conjunto de syscalls permitidos na implementação do suporte de **Libreswan** SECCOMP não está atualmente completo. Conseqüentemente, quando o SECCOMP é habilitado no arquivo `ipsec.conf`, a filtragem de chamadas do syscall rejeita até mesmo as chamadas necessárias para o bom funcionamento do daemon **pluto**; o daemon é morto e o serviço **ipsec** é reiniciado.

Para contornar este problema, coloque a opção `seccomp=` de volta ao estado de **incapacidade**. O suporte da SECCOMP deve permanecer desabilitado para executar o **ipsec** corretamente.

(BZ#1777474)

Certos conjuntos de regras interdependentes no SSG podem falhar

A remediação das regras do **Guia de Segurança SCAP** (SSG) em um padrão de referência pode falhar devido à ordenação indefinida das regras e suas dependências. Se duas ou mais regras precisam ser executadas em uma determinada ordem, por exemplo, quando uma regra instala um componente e outra regra configura o mesmo componente, elas podem ser executadas na ordem errada e a remediação informa um erro. Para contornar este problema, execute a correção duas vezes e a segunda execução corrige as regras dependentes.

(BZ#1750755)

SCAP Workbench não gera remediações baseadas em resultados a partir de perfis personalizados

O seguinte erro ocorre quando se tenta gerar funções de remediação baseadas em resultados a partir de um perfil personalizado usando a ferramenta **SCAP Workbench**:

```
Erro gerando papel de remediação .../remediação.sh: Código de saída da oscap foi 1: [saída truncada]
```

Para contornar este problema, use o comando **oscap** com a opção `--tailoring-file`.

(BZ#1640715)

Kickstart usa `org_fedora_oscap` em vez de `com_redhat_oscap` no RHEL 8

O Kickstart faz referência ao Protocolo de Automação de Conteúdo de Segurança Aberta (OSCAP) Anaconda add-on como **org_fedora_oscap** em vez de **com_redhat_oscap**, o que pode causar confusão. Isto é feito para preservar a retrocompatibilidade com o Red Hat Enterprise Linux 7.

(BZ#1665082)

OSCAP Anaconda Addon não instala todos os pacotes em modo texto

O plugin **OSCAP Anaconda Addon** não pode modificar a lista de pacotes selecionados para instalação pelo instalador do sistema se a instalação estiver rodando em modo texto. Conseqüentemente, quando um perfil de política de segurança é especificado usando Kickstart e a instalação está rodando em modo texto, quaisquer pacotes adicionais exigidos pela política de segurança não são instalados durante a instalação.

Para contornar este problema, execute a instalação em modo gráfico ou especifique todos os pacotes que são exigidos pelo perfil da política de segurança na seção `%packages` em seu arquivo Kickstart.

Como resultado, os pacotes que são exigidos pelo perfil de política de segurança não são instalados durante a instalação da RHEL sem uma das soluções descritas, e o sistema instalado não está de acordo com o perfil de política de segurança dado.

(BZ#1674001)

OSCAP Anaconda Addon não lida corretamente com perfis personalizados

O plug-in **OSCAP Anaconda Addon** não lida adequadamente com perfis de segurança com personalizações em arquivos separados. Conseqüentemente, o perfil personalizado não está disponível na instalação gráfica RHEL, mesmo quando você o especifica corretamente na seção Kickstart correspondente.

Para contornar este problema, siga as instruções na seção [Criação de um único fluxo de dados SCAP a partir de um DS original e de um](#) artigo de base de conhecimento de [arquivo de personalização](#). Como resultado deste trabalho, você pode usar um perfil SCAP personalizado na instalação gráfica RHEL.

(BZ#1691305)

GnuTLS falha em retomar a sessão atual com o servidor NSS

Ao retomar uma sessão TLS (Transport Layer Security) 1,3, o cliente **GnuTLS** espera 60 milissegundos mais um tempo estimado de ida e volta para o servidor enviar os dados de retomada da sessão. Se o servidor não enviar os dados de retomada dentro deste tempo, o cliente cria uma nova sessão em vez de retomar a sessão atual. Isto não causa efeitos adversos sérios, exceto por um pequeno impacto de desempenho em uma negociação de sessão regular.

(BZ#1677754)

O utilitário oscap-ssh falha ao digitalizar um sistema remoto com --sudo

Ao realizar um scan do Protocolo de Automação de Conteúdo de Segurança (SCAP) de um sistema remoto usando a ferramenta **oscap-ssh** com a opção **--sudo**, a ferramenta **oscap** no sistema remoto salva os arquivos de resultados do scan e informa os arquivos em um diretório temporário como usuário **root**. Se as configurações **umask** na máquina remota tiverem sido alteradas, **o oscap-ssh** pode não ter acesso a estes arquivos. Para contornar este problema, modificar a ferramenta **oscap-ssh**, como descrito nesta solução. O "**oscap-ssh --sudo**" [não consegue recuperar os arquivos de resultados com o "scp: Erro "Permissão negada"](#). Como resultado, **o oscap** salva os arquivos como usuário alvo, e **o oscap-ssh** acessa os arquivos normalmente.

(BZ#1803116)

OpenSCAP produz falsos positivos causados pela remoção de linhas em branco das cordas multi-linhas da YAML

Quando o OpenSCAP gera remediações possíveis a partir de um fluxo de dados, ele remove linhas em branco das cordas multi-linhas da YAML. Como algumas remediações possíveis contêm conteúdo de arquivo de configuração literal, a remoção de linhas em branco afeta as remediações correspondentes. Isto faz com que o utilitário **openscap** falhe as correspondentes verificações de Vulnerabilidade Aberta e Linguagem de Avaliação (OVAL), mesmo que as linhas em branco não tenham qualquer efeito. Para contornar este problema, verifique as descrições das regras e pule os resultados da varredura que falharam por falta de linhas em branco. Alternativamente, use remediações Bash em vez de Remediações Ansíveis, porque as remediações Bash não produzem estes resultados falsos positivos.

(BZ#1795563)

Os perfis baseados em OSPP são incompatíveis com os grupos de pacotes GUI.

Os pacotes **GNOME** instalados pelo grupo de pacotes *Server with GUI* requerem o pacote **nfs-utils** que não esteja em conformidade com o Perfil de Proteção do Sistema Operacional (OSPP). Como conseqüência, a seleção do grupo de pacotes *Server with GUI* durante a instalação de um sistema com perfis baseados em OSPP ou OSPP, por exemplo, Guia de Implementação Técnica de Segurança

(STIG), aborta a instalação. Se o perfil baseado em OSPP for aplicado após a instalação, o sistema não é inicializável. Para contornar este problema, não instale o grupo de pacotes *Server with GUI* ou qualquer outro grupo que instale a GUI ao usar o perfil baseado em OSPP e perfis baseados em OSPP. Ao utilizar os grupos de pacotes *Server* ou *Minimal Install*, o sistema se instala sem problemas e funciona corretamente.

[\(BZ#1787156\)](#)

O sistema RHEL8 com o grupo de pacotes *Server with GUI* não pode ser remediado usando o perfil do e8

O uso do OpenSCAP Anaconda Add-on para endurecer o sistema no grupo de pacotes *Server With GUI* com perfis que selecionam regras do grupo *Verify Integrity with RPM* requer uma quantidade extrema de RAM no sistema. Este problema é causado pelo scanner do OpenSCAP; para mais detalhes, veja [Digitalizando grandes números de arquivos com o OpenSCAP faz com que os sistemas fiquem sem memória](#). Como consequência, o endurecimento do sistema usando o perfil RHEL8 Essencial Eight (e8) não é bem sucedido. Para contornar este problema, escolha um grupo menor de pacotes, por exemplo, *Servidor*, e instale pacotes adicionais necessários após a instalação. Como resultado, o sistema terá um número menor de pacotes, a varredura exigirá menos memória e, portanto, o sistema pode ser endurecido automaticamente.

[\(BZ#1816199\)](#)

A digitalização de grandes números de arquivos com OpenSCAP faz com que os sistemas fiquem sem memória

O scanner OpenSCAP armazena todos os resultados coletados na memória até que a varredura termine. Como consequência, o sistema pode ficar sem memória em sistemas com pouca memória RAM ao digitalizar um grande número de arquivos, por exemplo, dos grandes grupos de pacotes *Server with GUI* e *Workstation*. Para contornar este problema, utilize grupos de pacotes menores, por exemplo, *Server* e *Minimal Install* em sistemas com pouca memória RAM. Se você precisar usar grandes grupos de pacotes, você pode testar se seu sistema tem memória suficiente em um ambiente virtual ou de encenação. Alternativamente, você pode adaptar o perfil de escaneamento para desmarcar as regras que envolvem recorrência sobre todo o sistema / de arquivos:

- **rpm_verify_hashes**
- **rpm_verify_permissions**
- **rpm_verify_ownership**
- **file_permissions_unauthorized_world_writable**
- **não_files_de_utilizador_de_propriedade_por_utilizador**
- **dir_perms_world_writable_system_owned**
- **file_permissions_unauthorized_suid**
- **file_permissions_unauthorized_sgid**
- **file_permissions_ungroupowned**
- **dir_perms_world_writable_sticky_bits**

Isto evitará que a varredura do OpenSCAP faça com que o sistema fique sem memória.

[\(BZ#1824152\)](#)

11.5. TRABALHO EM REDE

O tráfego de rede IPsec falha durante a descarga de IPsec quando o GRO é desativado

Não se espera que a descarga IPsec funcione quando a descarga de recepção genérica (GRO) estiver desativada no dispositivo. Se o descarregamento de IPsec estiver configurado em uma interface de rede e o GRO estiver desabilitado nesse dispositivo, o tráfego de rede IPsec falha.

Para contornar este problema, mantenha o GRO ativado no dispositivo.

(BZ#1649647)

iptables não solicita o carregamento de módulos para comandos que atualizam uma cadeia se o tipo de cadeia especificado não for conhecido

Nota: Este problema causa erros espúrios sem nenhuma implicação funcional ao interromper o serviço **iptables systemd** se você estiver usando a configuração padrão dos serviços.

Ao definir uma política de corrente com o **iptables-nft**, o comando de corrente de atualização resultante enviado ao kernel falhará se o módulo do kernel associado ainda não estiver carregado. Para contornar o problema, use os seguintes comandos para fazer com que os módulos sejam carregados:

```
# iptables -t nat -n -L
# iptables -t mangle -n -L
```

(BZ#1812666)

O carregamento automático dos módulos back end LOG específicos da família de endereços pelo módulo nft_compat pode ser pendurado

Quando o módulo **nft_compat** carrega o alvo **LOG** específico de uma família, enquanto uma operação em espaços de nomes de rede (**netns**) acontece em paralelo, pode ocorrer uma colisão com cadeado. Como consequência, o carregamento do alvo **LOG** específico da família de endereços pode ficar suspenso. Para contornar o problema, carregue manualmente os back ends de alvo **LOG** relevantes, tais como **nf_log_ipv4.ko** e **nf_log_ipv6.ko**, antes de executar o utilitário **iptables-restore**. Como resultado, o carregamento dos back ends dos alvos **LOG** não fica pendurado. Entretanto, se o problema aparecer durante a inicialização do sistema, não há nenhuma solução de trabalho disponível.

Observe que outros serviços, como o **libvirtd**, também executam comandos **iptables**, o que pode causar o problema.

(BZ#1757933)

11.6. KERNEL

A remoção acidental do patch faz com que o enorme_page_setup_helper.py mostre erro

Um adesivo que atualiza o **enorme_página_setup_helper.py** script, foi removido acidentalmente. Consequentemente, após a execução do script **huge_page_setup_helper.py**, aparece a seguinte mensagem de erro:

```
SintaxeError: Parênteses em falta na chamada para "imprimir
```

Para contornar este problema, copie o **enorme_página_setup_helper.py** script da RHEL 8.1 e instale-o no diretório **/usr/bin/**:

1. Faça o download do pacote **libhugetlbfs-utils-2.21-3.el8.x86_64.rpm** da mídia de instalação RHEL-8.1.0 ou do [Portal do Cliente da Red Hat](#).
2. Executar o comando **rpm2cpio**:

```
# rpm2cpio libhugetlbfs-utils-2.21-3.el8.x86_64.rpm | cpio -D / -iduv  
*/huge_page_setup_helper.py'
```

O comando extrai o **enorme_página_setup_helper.py** script do RHEL 8.1 RPM e o salva no diretório **/usr/bin/**.

Como resultado, o **enorme_página_setup_helper.py** script funciona corretamente.

(BZ#1823398)

Sistemas com uma grande quantidade de experiências de memória persistente atrasam durante o processo de inicialização

Sistemas com uma grande quantidade de memória persistente levam muito tempo para arrancar porque a inicialização da memória é feita em série. Consequentemente, se houver sistemas de arquivo de memória persistente listados no arquivo **/etc/fstab**, o sistema pode demorar enquanto espera que os dispositivos fiquem disponíveis. Para contornar este problema, configure a opção **DefaultTimeoutStartSec** no arquivo **/etc/systemd/system.conf** para um valor suficientemente grande.

(BZ#1666538)

A KSM às vezes ignora as políticas de memória NUMA

Quando o recurso de memória compartilhada do kernel (KSM) é ativado com o parâmetro **merge_across_nodes=1**, o KSM ignora as políticas de memória definidas pela função `mbind()`, e pode fundir páginas de algumas áreas de memória com nós de Acesso Não-Uniforme à Memória (NUMA) que não correspondem às políticas.

Para contornar este problema, desative o KSM ou configure o parâmetro **merge_across_nodes** para **0** se estiver usando a ligação de memória NUMA com QEMU. Como resultado, as políticas de memória NUMA configuradas para a KVM VM funcionarão como esperado.

(BZ#1153521)

O núcleo de depuração não inicia no ambiente de captura de falhas no RHEL 8

Devido à natureza exigente de memória do núcleo de depuração, ocorre um problema quando o núcleo de depuração está em uso e um pânico do núcleo é desencadeado. Como consequência, o kernel debug não é capaz de inicializar como o kernel de captura, e em seu lugar é gerado um traço de pilha. Para contornar este problema, aumente a memória do kernel debug de acordo. Como resultado, o kernel debug arranca com sucesso no ambiente de captura de falhas.

(BZ#1659609)

zlib pode retardar uma captura de vmcore em algumas funções de compressão

O arquivo de configuração **kdump** usa o formato de compressão **lzo(makedumpfile -l)** por padrão. Ao modificar o arquivo de configuração usando o formato de compressão **zlib(makedumpfile -c)**, é provável que ele traga um fator de compressão melhor às custas de retardar o processo de captura do **vmcore**. Como consequência, o **kdump** leva até quatro vezes mais tempo para capturar um **vmcore** com **zlib**, em comparação com o **lzo**.

Como resultado, a Red Hat recomenda o uso do **lzo** padrão para os casos em que a velocidade é o principal fator de condução. Entretanto, se a máquina alvo estiver com pouco espaço disponível, a **zlib** é uma opção melhor.

(BZ#1790635)

Uma captura vmcore falha após a operação de hot-plug de memória ou de desconectar a tomada

Após realizar a operação hot-plug ou hot-unplug de memória, o evento vem após a atualização da árvore do dispositivo que contém informações sobre o layout da memória. Assim, o utilitário **makedump** tenta acessar um endereço físico inexistente. O problema aparece se todas as seguintes condições forem atendidas:

- Uma variante um pouco endiana do IBM Power System executa o RHEL 8.
- O serviço **kdump** ou **fadump** está habilitado no sistema.

Conseqüentemente, o kernel de captura não consegue salvar o **vmcore** se uma falha no kernel for acionada após a operação hot-plug ou hot-unplug da memória.

Para contornar este problema, reinicie o serviço **kdump** após o hot-plug ou hot-unplug:

```
# systemctl restart kdump.service
```

Como resultado, o **vmcore** é salvo com sucesso no cenário descrito.

(BZ#1793389)

O mecanismo fadump dumping renomeia a interface da rede para kdump-<interface-name>

Ao utilizar o lixão assistido por firmwares (**fadump**) para capturar um **vmcore** e armazená-lo em uma máquina remota usando o protocolo SSH ou NFS, renomeia a interface de rede para **kdump-<interface-name>**. A renomeação acontece quando o **<interface-name>** é genérico, por exemplo, ***eth#**, ou **net#** e assim por diante. Este problema ocorre porque os scripts de captura do **vmcore** no disco RAM inicial (**initrd**) adicionam o prefixo **kdump-** ao nome da interface de rede para garantir a nomeação persistente. Como o mesmo **initrd** também é usado para uma inicialização regular, o nome da interface é alterado também para o kernel de produção.

(BZ#1745507)

O sistema entra no modo de emergência no momento da inicialização quando o fadump é ativado

O sistema entra no modo de emergência quando **fadump** (**kdump**) ou **dracut** o módulo **squash** é ativado no esquema **initramfs** porque o gerente **systemd** não consegue pegar as informações de montagem e configurar a partição LV para montar. Para contornar este problema, adicione o seguinte parâmetro de linha de comando do kernel **rd.lvm.lv=<VG>/<LV>** para descobrir e montar a partição LV falhada de forma apropriada. Como resultado, o sistema inicializará com sucesso no cenário descrito.

(BZ#1750278)

O uso do irqpoll causa falha na geração de vmcore

Devido a um problema existente com o driver **nvme** nas arquiteturas ARM de 64 bits que rodam nas plataformas de nuvem Amazon Web Services (AWS), a geração **vmcore** falha quando você fornece o parâmetro de linha de comando do kernel **irqpoll** para o primeiro kernel. Conseqüentemente, nenhum

arquivo **vmcore** é despejado no diretório **/var/crash/** após uma falha do kernel. Para contornar este problema:

1. Adicionar **irqpoll** à chave **KDUMP_COMMANDLINE_REMOVE** no arquivo **/etc/sysconfig/kdump**.
2. Reinicie o serviço **kdump** executando o comando **systemctl restart kdump**.

Como resultado, espera-se que o primeiro kernel boots corretamente e o arquivo **vmcore** sejam capturados na falha do kernel.

Note que o serviço **kdump** pode usar uma quantidade significativa de memória do kernel para despejar o arquivo **vmcore**. Certifique-se de que o kernel de captura tenha memória suficiente disponível para o serviço de **kdump**.

(BZ#1654962)

O uso da memória vPMEM como alvo de despejo atrasa o processo de captura de falhas do kernel

Quando você usa a Memória Virtual Persistente (vPEM) como alvo **kdump** ou **fadump**, o módulo **papr_scm** é forçado a desenhar e refazer a memória com o respaldo do vPMEM e readicionar a memória em seu mapa linear. Conseqüentemente, este comportamento aciona as chamadas Hypervisor (HCalls) para o Hypervisor POWER, e o tempo total gasto, retarda consideravelmente a inicialização do kernel de captura. Portanto, recomenda-se não usar os espaços de nomes vPMEM como alvo de despejo para **kdump** ou **fadump**.

Se você precisar usar o vPMEM, para contornar este problema, execute os seguintes comandos:

1. Criar o arquivo **/etc/dracut.conf.d/99-pmem-workaround.conf** e adicionar:

```
add_drivers == "nd_pmem nd_btt libnvdimm papr_scm"
```

2. Reconstruir o sistema de arquivo inicial do disco RAM (initrd):

```
# touch /etc/kdump.conf
# systemctl restart kdump.service
```

(BZ#1792125)

O cão de guarda HP NMI nem sempre gera um depósito de lixo

Em certos casos, o motorista **hpwdt** para o cão de guarda HP NMI não é capaz de reivindicar uma interrupção não-máscara (NMI) gerada pelo temporizador HPE porque o NMI foi consumido pelo motorista **perfmon**.

O NMI em falta é iniciado por uma de duas condições:

1. O botão **Generate NMI** no software de gerenciamento do servidor Lights-Out (iLO) integrado. Este botão é acionado por um usuário.
2. O cão de guarda **hpwdt**. A expiração por padrão envia um NMI para o servidor.

Ambas as seqüências tipicamente ocorrem quando o sistema não responde. Em circunstâncias normais, o manipulador do NMI para estas duas situações chama a função **kernel panic()** e se configurado, o serviço **kdump** gera um arquivo **vmcore**.

Devido à falta de MNI, no entanto, o **pânico no núcleo**() não é chamado e o **vmcore** não é coletado.

No primeiro caso (1.), se o sistema não reagiu, ele permanece assim. Para contornar este cenário, use o botão virtual **Power** para reinicializar ou ligar o servidor.

No segundo caso (2.), o NMI em falta é seguido 9 segundos depois por um reset do ASR (Automated System Recovery).

A linha de servidores HPE Gen9 experimenta este problema em porcentagens de um dígito. O Gen10 em uma frequência ainda menor.

(BZ#1602962)

O comando **powersave de perfil afinado** faz com que o sistema não responda

A execução do comando **powersave de perfil tuned-adm** leva a um estado não responsivo dos sistemas de 2-socket Penguin Valkyrie 2000 com os processadores Thunderx (CN88xx) mais antigos. Conseqüentemente, reinicialize o sistema para retomar o funcionamento. Para contornar este problema, evite usar o perfil **powersave** se seu sistema estiver de acordo com as especificações mencionadas.

(BZ#1609288)

O driver **cxgb4** causa uma falha no **kdump kernel**

O **kdump** kernel quebra ao tentar salvar informações no arquivo **vmcore**. Conseqüentemente, o driver **cxgb4** impede que o **kdump** kernel salve um núcleo para análise posterior. Para contornar este problema, adicione o parâmetro **novmcoredd** à linha de comando do **kdump kernel** para permitir salvar arquivos do núcleo.

(BZ#1708456)

A tentativa de adicionar a porta NIC do driver **ICE** a um modo 5(**balance-tlb**) de ligação da interface mestre pode levar a falhas

Tentar adicionar a porta NIC do driver **ICE** a uma interface mestre de ligação modo 5 (**balance-tlb**) pode levar a uma falha com um erro **Master 'bond0', Slave 'ens1f0': Erro: Ens1f0': Erro: Falha no escravo**. Conseqüentemente, você experimenta uma falha intermitente ao adicionar a porta NIC à interface mestre de colagem. Para solucionar este problema, tente tentar novamente adicionar a interface.

(BZ#1791664)

Anexar a Função Virtual à máquina virtual com interface **tipo='hostdev'** pode falhar em alguns momentos

Anexar uma função virtual (VF) a uma máquina virtual usando um arquivo .XML, seguindo o método **Assignment with <interface type='hostdev'>**, pode falhar em alguns momentos. Isto ocorre porque a utilização do método **Assignment with <interface type='hostdev'>** impede a VM de anexar a VF NIC apresentada a esta máquina virtual. Para resolver este problema, anexe a VF à VM usando o arquivo .XML, usando o método **Assignment with <hostdev>**. Como resultado, o comando **virsh attach-device** é bem sucedido sem erros. Para mais detalhes sobre a diferença entre **Assignment with <hostdev>** e **Assignment with <interface type='hostdev'>** (somente dispositivos SRIOV), veja [PCI Passthrough de dispositivos de rede host](#).

(BZ#1792691)

11.7. SISTEMAS DE ARQUIVO E ARMAZENAMENTO

O sistema de arquivo **/boot** não pode ser colocado na LVM

Você não pode colocar o sistema de arquivo **/boot** em um volume lógico LVM. Esta limitação existe pelas seguintes razões:

- Nos sistemas EFI, o *EFI System Partition* convencionalmente serve como o sistema de arquivo **/boot**. O padrão uEFI requer um tipo específico de partição GPT e um tipo específico de sistema de arquivo para esta partição.
- A RHEL 8 usa o *Boot Loader Specification* (BLS) para as entradas de inicialização do sistema. Esta especificação requer que o sistema de arquivos **/boot** seja legível pelo firmware da plataforma. Nos sistemas EFI, o firmware da plataforma pode ler somente a configuração **/boot** definida pelo padrão uEFI.
- O suporte para os volumes lógicos LVM no carregador de inicialização do GRUB 2 está incompleto. A Red Hat não planeja melhorar o suporte porque o número de casos de uso do recurso está diminuindo devido a padrões como o uEFI e o BLS.

A Red Hat não planeja **apoiar/botar** na LVM. Ao invés disso, a Red Hat fornece ferramentas para gerenciar instantâneos e rollback do sistema que não precisam que o sistema de arquivo **/boot** seja colocado em um volume lógico LVM.

(BZ#1496229)

LVM não mais permite criar grupos de volume com blocos de tamanhos mistos

As utilidades LVM como **vgcreate** ou **vgextend** não permitem mais a criação de grupos de volume (VGs) onde os volumes físicos (PVs) têm tamanhos de blocos lógicos diferentes. O LVM adotou esta mudança porque os sistemas de arquivo não conseguem montar se você estender o volume lógico subjacente (LV) com um PV de um bloco de tamanho diferente.

Para reativar a criação de VGs com tamanhos de blocos mistos, defina a opção **allow_mixed_block_sizes=1** no arquivo **lvm.conf**.

(BZ#1768536)

DM Multipath pode não começar quando muitos LUNs estiverem conectados

O serviço **multipathd** poderá ficar sem tempo e não começar se muitas unidades lógicas (LUNs) estiverem conectadas ao sistema. O número exato de LUNs que causam o problema depende de vários fatores, incluindo o número de dispositivos, o tempo de resposta da matriz de armazenamento, a configuração da memória e da CPU, e a carga do sistema.

Para contornar o problema, aumente o valor do timeout no arquivo da unidade **multipathd**:

1. Abra a unidade **multipathd** no editor da unidade:

```
# systemctl editar multipathd
```

2. Digite a seguinte configuração para anular o valor de timeout:

```
[Service]  
TimeoutSec=300
```

A Red Hat recomenda aumentar o valor para 300 a partir do padrão 90, mas você também pode testar outros valores acima de 90.

3. Salvar o arquivo no editor.
4. Recarregar unidades **do sistema** para aplicar a mudança:

```
# systemctl daemon-reload
```

Como resultado, o **multipathd** pode agora começar com sucesso com um número maior de LUNs.

(BZ#1797660)

Limitações da LVM **writecache**

O método de cache **writecache** LVM tem as seguintes limitações, que não estão presentes no método de **cache**:

- Não é possível tirar um instantâneo de um volume lógico enquanto o volume lógico estiver usando o **writecache**.
- Não é possível anexar ou descolar **a dor de escrita** enquanto um volume lógico estiver ativo.
- Ao anexar o **writecache** a um volume lógico inativo, você deve usar um tamanho de bloco **writecache** que corresponda ao tamanho do bloco do sistema de arquivos existente. Para detalhes, consulte a página de manual **lvmdcache(7)**.
- Não é possível redimensionar um volume lógico enquanto o **writecache** estiver anexado a ele.
- Você não pode usar comandos **pvmove** em dispositivos que são usados com **writecache**.
- Não é possível utilizar volumes lógicos com **writecache** em combinação com piscinas finas ou VDO.

(JIRA:RHELPLAN-27987, [BZ#1798631](#), BZ#1808012)

Os dispositivos espelhos LVM que armazenam um volume LUKS às vezes se tornam insensíveis

Dispositivos LVM espelhados com um tipo de segmento de **espelho** que armazenam um volume LUKS pode se tornar insensível sob certas condições. Os dispositivos que não respondem rejeitam todas as operações de E/S.

Para contornar o problema, a Red Hat recomenda que você use dispositivos LVM RAID 1 com um tipo de segmento de **raid1** em vez de **espelho**, se você precisar empilhar volumes LUKS em cima de armazenamento resiliente definido por software.

O tipo de segmento **raid1** é o tipo de configuração RAID padrão e substitui o **espelho** como a solução recomendada.

Para converter dispositivos **espelhados** em **raid**, consulte [Conversão de um dispositivo LVM espelhado em um dispositivo RAID1](#).

(BZ#1730502)

Um patch NFS 4.0 pode resultar em um desempenho reduzido sob uma carga de trabalho pesada e aberta

Anteriormente, foi corrigido um bug que, em alguns casos, poderia fazer com que uma operação NFS aberta ignorasse o fato de que um arquivo tinha sido removido ou renomeado no servidor. Entretanto, a correção pode causar um desempenho mais lento com cargas de trabalho que requerem muitas

operações abertas. Para contornar este problema, poderia ajudar a usar a versão 4.1 ou superior do NFS, que foi melhorada para conceder delegações aos clientes em mais casos, permitindo aos clientes realizar operações abertas localmente, de forma rápida e segura.

(BZ#1748451)

11.8. LINGUAGENS DE PROGRAMAÇÃO DINÂMICA, SERVIDORES WEB E DE BANCO DE DADOS

getpwnam() pode falhar quando chamado por uma aplicação de 32 bits

Quando um usuário do NIS usa uma aplicação de 32 bits que chama a função **getpwnam()**, a chamada falha se o pacote **nss_nis.i686** estiver faltando. Para contornar este problema, instale manualmente o pacote que falta usando o comando **yum install nss_nis.i686**.

(BZ#1803161)

nginx não pode carregar certificados de servidor a partir de fichas de segurança de hardware

O servidor web **nginx** suporta o carregamento de chaves privadas TLS a partir de tokens de segurança de hardware diretamente dos módulos PKCS#11. Entretanto, atualmente é impossível carregar certificados de servidor a partir de tokens de segurança de hardware através do URI PKCS#11. Para contornar este problema, armazenar certificados de servidor no sistema de arquivos

(BZ#1668717)

php-fpm faz com que o SELinux AVC seja negado quando o php-opcache é instalado com PHP 7.2

Quando o pacote **php-opcache** é instalado, o Gerenciador de Processos FastCGI (**php-fpm**) faz com que a SELinux AVC seja negada. Para contornar este problema, altere a configuração padrão no arquivo **/etc/php.d/10-opcache.ini** para o seguinte:

```
opcache.huge_code_pages=0
```

Note que este problema afeta apenas o fluxo **php:7.2**, não o fluxo **php:7.3**.

(BZ#1670386)

O nome do pacote mod_wsgi está faltando ao ser instalado como uma dependência

Com uma mudança na instalação **mod_wsgi**, descrita no [BZ#1779705](#), o pacote **python3-mod_wsgi** não fornece mais o nome **mod_wsgi**. Ao instalar o módulo **mod_wsgi**, você deve especificar o nome completo do pacote. Esta mudança causa problemas com as dependências de pacotes de terceiros.

Se você tentar instalar um pacote de terceiros que requeira uma dependência chamada **mod_wsgi**, um erro semelhante ao seguinte é retornado:

```
Error:
Problem: conflicting requests
- nothing provides mod_wsgi needed by package-requires-mod_wsgi.el8.noarch
```

Para contornar este problema, escolha uma das seguintes opções:

- a. Reconstruir o pacote (ou pedir ao fornecedor terceirizado uma nova construção) para exigir o nome completo do pacote **python3-mod_wsgi**.
- b. Criar um meta pacote com o nome do pacote que falta:
 1. Construa seu próprio meta pacote vazio que fornece o nome **mod_wsgi**.
 2. Adicione o **module_hotfixes=True** line ao arquivo de configuração **.repo** do repositório que inclui o meta pacote.
 3. Instalar manualmente o **python3-mod_wsgi**.

(BZ#1829692)

11.9. COMPILADORES E FERRAMENTAS DE DESENVOLVIMENTO

Funções sintéticas geradas pelo GCC confundem SystemTap

A otimização do GCC pode gerar funções sintéticas para cópias parcialmente simplificadas de outras funções. Ferramentas como SystemTap e GDB não podem distinguir estas funções sintéticas das funções reais. Como consequência, o SystemTap coloca sondas em pontos de entrada de funções sintéticas e reais e, assim, registra múltiplos acertos de sondas para uma única chamada de função real.

Para contornar este problema, modifique os scripts SystemTap para detectar a recorrência e evitar a colocação de sondas relacionadas a funções parciais simplificadas.

Este roteiro de exemplo

```
sonda kernel.function({i1}"can_nice").call {i}
```

pode ser modificado desta forma:

```
global in_can_nice%

probe kernel.function("can_nice").call {
  in_can_nice[tid()] ++;
  if (in_can_nice[tid()] > 1) { next }
  /* code for real probe handler */
}

probe kernel.function("can_nice").return {
  in_can_nice[tid()] --;
}
```

Observe que este roteiro de exemplo não considera todos os cenários possíveis, tais como a falta de kprobes ou kretprobes, ou a verdadeira recursividade pretendida.

(BZ#1169184)

11.10. GESTÃO DA IDENTIDADE

A mudança **/etc/nsswitch.conf** requer uma reinicialização manual do sistema

Qualquer alteração no arquivo **/etc/nsswitch.conf**, por exemplo rodando o comando **authselect select profile_id**, requer uma reinicialização do sistema para que todos os processos relevantes usem a versão

atualizada do arquivo **/etc/nsswitch.conf**. Se uma reinicialização do sistema não for possível, reinicie o serviço que une seu sistema ao Active Directory, que é o **System Security Services Daemon** (SSSD) ou **winbind**.

(BZ#1657295)

SSSD retorna a adesão incorreta ao grupo LDAP para usuários locais quando o domínio de arquivos está habilitado

Se o Daemon System Security Services (SSSD) serve usuários dos arquivos locais e o atributo **ldap_rfc2307_fallback_to_local_users** na seção [domínio/LDAP] do arquivo **sssd.conf** é definido como True, então o provedor de arquivos não inclui membros de grupo de outros domínios. Como consequência, se um usuário local é membro de um grupo LDAP, o comando **id local_user** não retorna a filiação do usuário ao grupo LDAP. Para contornar este problema, desabilite o domínio de **arquivos** implícito, adicionando

```
enable_files_domain=False
```

para a seção **[sssd]** no arquivo **/etc/sss/sss.conf**.

Como resultado, **id local_user** retorna a adesão correta ao grupo LDAP para usuários locais.

(BZ#1652562)

O SSSD não lida corretamente com múltiplas regras de correspondência de certificados com a mesma prioridade

Se um determinado certificado corresponde a várias regras de correspondência de certificados com a mesma prioridade, o System Security Services Daemon (SSSD) utiliza apenas uma das regras. Como alternativa, use uma única regra de correspondência de certificado cujo filtro LDAP consiste nos filtros das regras individuais concatenadas com o | (ou) operador. Para exemplos de regras de correspondência de certificados, consulte a página de manual sss-certamp(5).

(BZ#1447945)

Grupos privados não podem ser criados com auto_private_group = híbrido quando múltiplos domínios são definidos

Grupos privados não podem ser criados com a opção **auto_private_group = híbrido** quando múltiplos domínios são definidos e a opção híbrida é usada por qualquer domínio que não seja o primeiro. Se um domínio de arquivos implícito for definido junto com um domínio AD ou LDAP no arquivo **sssd.conf** e não estiver marcado como **MPG_HYBRID**, então o SSSD falha em criar um grupo privado para um usuário que tem uid=gid e o grupo com este gid não existe no AD ou LDAP.

O respondedor **sssd_nss** verifica o valor da opção **auto_private_groups** apenas no primeiro domínio. Como consequência, em configurações onde vários domínios são configurados, o que inclui a configuração padrão no RHEL 8, a opção **auto_private_groups** não tem efeito.

Para contornar este problema, configure **enable_files_domain = falso** na seção **sssd** do **sssd.conf**. Como resultado, se a opção **enable_files_domain** estiver definida como falsa, então o **sssd** não adiciona um domínio com **id_provider=files** no início da lista de domínios ativos e, portanto, este bug não ocorre.

(BZ#1754871)

python-ply não é compatível com FIPS

O módulo YACC do pacote **python-ply** utiliza o algoritmo de hashing MD5 para gerar a impressão digital de uma assinatura YACC. Entretanto, o modo FIPS bloqueia o uso do MD5, que só é permitido em contextos sem segurança. Como consequência, o **python-ply** não é compatível com o FIPS. Em um sistema em modo FIPS, todas as chamadas para **ply.yacc.yacc()** falham com a mensagem de erro:

UnboundLocalError: variável local 'sig' referenciada antes da atribuição

O problema afeta o **python-pycparser** e alguns casos de uso de **python-cffi**. Para contornar este problema, modificar a linha 2966 do arquivo `/usr/lib/python3.6/site-packages/ply/yacc.py`, substituindo **sig = md5()** por **sig = md5(usado para segurança=False)**. Como resultado, o **python-ply** pode ser usado no modo FIPS.

(BZ#1747490)

FreeRADIUS truncata silenciosamente Túnel-Palavras-palavras com mais de 249 caracteres

Se uma senha de túnel tiver mais de 249 caracteres, o serviço FreeRADIUS a truncará silenciosamente. Isto pode levar a incompatibilidades inesperadas de senhas com outros sistemas.

Para contornar o problema, escolha uma senha que tenha 249 caracteres ou menos.

(BZ#1723362)

A instalação da KRA falha se todos os membros da KRA forem réplicas ocultas

O utilitário **ipa-kra-install** falha em um cluster onde a Key Recovery Authority (KRA) já está presente se a primeira instância da KRA for instalada em uma réplica oculta. Conseqüentemente, não é possível adicionar mais instâncias KRA ao cluster.

Para contornar este problema, descubra a réplica oculta que tem o papel de KRA antes de acrescentar novas instâncias de KRA. Você pode escondê-la novamente quando **a instalação do ipa-kra-install** for concluída com sucesso.

(BZ#1816784)

O Servidor de Diretório avverte sobre atributos ausentes no esquema se esses atributos forem utilizados em um filtro de busca

Se você definir o parâmetro **nsslapd-verify-filter-schema** para **alertar-invalidar**, o Servidor de Diretório processa operações de busca com atributos que não estão definidos no esquema e registra um aviso. Com esta configuração, o Servidor de Diretório retorna os atributos solicitados nos resultados da busca, independentemente de os atributos estarem ou não definidos no esquema.

Uma versão futura do Servidor de Diretório mudará a configuração padrão do **esquema nsslapd-verify-filter** para impor verificações mais rígidas. O novo padrão advertirá sobre atributos que estão faltando no esquema, e rejeitará pedidos ou retornará apenas resultados parciais.

(BZ#1790259)

ipa-healthcheck-0.4 não torna obsoletas as versões mais antigas do ipa-healthcheck

A ferramenta **Healthcheck** foi dividida em dois sub-pacotes: **ipa-healthcheck** e **ipa-healthcheck-core**. Entretanto, apenas o sub-pacote **ipa-healthcheck-core** está corretamente configurado para versões obsoletas do **ipa-healthcheck**. Como resultado, a atualização do **Healthcheck** apenas instala o **ipa-healthcheck-core** e o comando **ipa-healthcheck** não funciona após a atualização.

Para contornar este problema, instale o sub-pacote **ipa-healthcheck-0.4** manualmente usando **o yum install ipa-healthcheck-0.4**.

([BZ#1852244](#))

11.11. DESKTOP

Limitações da sessão Wayland

Com o Red Hat Enterprise Linux 8, o ambiente GNOME e o Gerenciador de Exibição GNOME (GDM) usam **Wayland** como o tipo de sessão default ao invés da sessão **X11**, que foi usada com a versão anterior principal da RHEL.

As seguintes características estão atualmente indisponíveis ou não funcionam como esperado em **Wayland**:

- **X11** utilitários de configuração, como o **xrandr**, não funcionam sob **Wayland** devido a sua abordagem diferente de manuseio, resoluções, rotações e layout. Você pode configurar os recursos de exibição usando as configurações do GNOME.
- A gravação em tela e a área de trabalho remota requerem aplicações que suportem a API do portal em **Wayland**. Certas aplicações legadas não suportam a API do portal.
- A acessibilidade do ponteiro não está disponível no site **Wayland**.
- Não há um gerente de prancheta disponível.
- O GNOME Shell em **Wayland** ignora as capturas de teclado emitidas pela maioria dos aplicativos legados **X11**. Você pode habilitar uma aplicação **X11** para emitir garras de teclado usando a tecla **/org/gnome/mutter/wayland/xwayland-grab-access-rules** GSettings. Por padrão, o GNOME Shell no site **Wayland** permite que as seguintes aplicações emitam garras de teclado:
 - **GNOME Boxes**
 - **Vinagre**
 - **Xephyr**
 - **virt-manager**, **virt-viewer**, e **remote-viewer**
 - **vncviewer**
- **Wayland** dentro de máquinas virtuais convidadas (VMs) tem problemas de estabilidade e desempenho. A RHEL volta automaticamente para a sessão **X11** quando está rodando em uma VM.

Se você atualizar para o RHEL 8 a partir de um sistema RHEL 7 onde você usou a sessão **X11** GNOME, seu sistema continua a usar **X11**. O sistema também volta automaticamente para **X11** quando os seguintes drivers gráficos estão em uso:

- O driver proprietário da NVIDIA
- O motorista de **cirrus**
- O motorista de **mga**

- O motorista de **velocidade**

Você pode desativar o uso do site **Wayland** manualmente:

- Para desativar **Wayland** no GDM, defina a opção **WaylandEnable=false** no arquivo **/etc/gdm/custom.conf**.
- Para desativar **Wayland** na sessão GNOME, selecione a opção legada **X11** usando o menu da roda dentada na tela de login após digitar seu nome de login.

Para obter mais detalhes em **Wayland**, consulte <https://wayland.freedesktop.org/>.

(BZ#1797409)

O drag-and-drop não funciona entre a área de trabalho e as aplicações

Devido a um bug no pacote **gnome-shell-extensions**, a funcionalidade de arrastar e soltar não funciona atualmente entre o desktop e as aplicações. O suporte para este recurso será adicionado de volta em um lançamento futuro.

(BZ#1717947)

Não é possível desativar os repositórios flatpak dos Repositórios de Software

Atualmente, não é possível desativar ou remover os repositórios **flatpak** na ferramenta Repositórios de Software no utilitário Software GNOME.

(BZ#1668760)

Geração 2 RHEL 8 máquinas virtuais às vezes não inicializam nos hosts do Hyper-V Server 2016

Ao usar o RHEL 8 como sistema operacional convidado em uma máquina virtual (VM) rodando em um host Microsoft Hyper-V Server 2016, a VM, em alguns casos, falha no boot e retorna ao menu de boot do GRUB. Além disso, o seguinte erro é registrado no registro de eventos do Hyper-V:

O sistema operacional convidado informou que falhou com o seguinte código de erro: 0x1E

Este erro ocorre devido a um erro de firmware UEFI no host Hyper-V. Para contornar este problema, use o Hyper-V Server 2019 como o host.

(BZ#1583445)

A falha do sistema pode resultar na perda da configuração do fadump

Este número é observado em sistemas onde o dump assistido por firmwares (fadump) está habilitado, e a partição de inicialização está localizada em um sistema de arquivo de journaling como o XFS. Uma falha do sistema pode fazer com que o carregador de inicialização carregue um **initrd** mais antigo que não tenha o suporte de captura de dump habilitado. Conseqüentemente, após a recuperação, o sistema não captura o arquivo **vmcore**, o que resulta na perda da configuração fadump.

Trabalhar em torno deste problema:

- Se **/boot** for uma divisória separada, execute o seguinte:
 1. Reinicie o serviço de kdump

2. Execute os seguintes comandos como usuário `root`, ou usando uma conta de usuário com direitos `CAP_SYS_ADMIN`:

```
# fsfreeze -f  
# fsfreeze -u
```

- Se `/boot` não for uma partição separada, reinicialize o sistema.

(BZ#1723501)

11.12. INFRA-ESTRUTURAS GRÁFICAS

Incapaz de executar aplicações gráficas usando o comando `sudo`

Ao tentar executar aplicações gráficas como um usuário com privilégios elevados, a aplicação não consegue abrir com uma mensagem de erro. A falha acontece porque **Xwayland** é restrito pelo arquivo **Xauthority** para usar credenciais de usuário regulares para autenticação.

Para contornar este problema, use o comando **sudo -E** para executar aplicações gráficas como um usuário **root**.

(BZ#1673073)

radeon falha em reiniciar o hardware corretamente

O driver do kernel **radeon** atualmente não reinicia corretamente o hardware no contexto do `kexec`. Em vez disso, o **radeon** cai, o que faz com que o resto do serviço **kdump** falhe.

Para contornar este problema, faça **uma** lista negra em **kdump** adicionando a seguinte linha ao arquivo `/etc/kdump.conf`:

```
dracut_args --omit-drivers "radeon"  
force_rebuild 1
```

Reinicie a máquina e **kdump**. Após iniciar **kdump**, a linha **force_rebuild 1** pode ser removida do arquivo de configuração.

Note que, neste cenário, nenhum gráfico estará disponível durante **kdump**, mas **kdump** funcionará com sucesso.

(BZ#1694705)

Múltiplos displays HDR em uma única topologia MST podem não ligar

Em sistemas que utilizam GPUs NVIDIA Turing com o **novo** driver, o uso de um hub **DisplayPort** (como uma doca para laptop) com vários monitores que suportam HDR conectados a ele pode resultar na falha em ligar todos os monitores, apesar de ter feito isso em versões anteriores da RHEL. Isto é devido ao sistema pensar erroneamente que não há largura de banda suficiente no hub para suportar todos os monitores.

(BZ#1812577)

11.13. O CONSOLE WEB

Usuários sem privilégios podem acessar a página de Assinaturas

Se um não-administrador navegar para a página **Subscriptions** do console web, o console web exibe uma mensagem de erro genérica **O Cockpit teve um erro interno inesperado**.

Para contornar este problema, acesse o console web com um usuário privilegiado e certifique-se de verificar a caixa de seleção **Reuse my password for privileged tasks**

(BZ#1674337)

11.14. VIRTUALIZAÇÃO

Baixo desempenho de display GUI em máquinas virtuais RHEL 8 em um host Windows Server 2019

Ao usar o RHEL 8 como um sistema operacional convidado em modo gráfico em um host Windows Server 2019, o desempenho da tela GUI é baixo, e a conexão a um console de saída do convidado leva atualmente muito mais tempo do que o esperado.

Esta é uma questão conhecida nos hosts do Windows 2019 e está pendente de uma correção pela Microsoft. Para contornar este problema, conecte-se ao convidado usando SSH ou use o Windows Server 2016 como host.

(BZ#1706541)

A exibição de vários monitores de máquinas virtuais que utilizam Wayland não é possível com QXL

Usar o utilitário de **visualização remota** para exibir mais de um monitor de uma máquina virtual (VM) que está usando o servidor de exibição Wayland faz com que a VM fique sem resposta e que a mensagem de status *Waiting for display* seja exibida indefinidamente.

Para contornar este problema, use **virtio-gpu** em vez de **qxl** como dispositivo GPU para VMs que utilizam Wayland.

(BZ#1642887)

os comandos de **virsh iface-*** não funcionam de forma consistente

Atualmente, comandos **virsh iface-***, tais como **virsh iface-start** e **virsh iface-destruição**, frequentemente falham devido a dependências de configuração. Portanto, recomenda-se não usar comandos **virsh iface-*** para configurar e gerenciar as conexões de rede do host. Ao invés disso, use o programa NetworkManager e suas aplicações de gerenciamento relacionadas.

(BZ#1664592)

As máquinas virtuais RHEL 8 às vezes não podem inicializar em máquinas Witherspoon

As máquinas virtuais RHEL 8 (VMs) que utilizam o tipo de máquina **pseries-rhel7.6.0-sxxm** em alguns casos não inicializam nos hosts *Power9 S922LC for HPC* (também conhecidos como Witherspoon) que utilizam a CPU DD2.2 ou DD2.3.

A tentativa de iniciar tal VM, em vez disso, gera a seguinte mensagem de erro:

```
qemu-kvm: Nível de capacidade do ramo indireto seguro não suportado pelo kvm
```

Para contornar este problema, configure a configuração da máquina virtual em XML da seguinte maneira:

```
<domain type='qemu' xmlns:qemu='http://libvirt.org/schemas/domain/qemu/1.0'>
  <qemu:commandline>
    <qemu:arg value='-machine'/>
    <qemu:arg value='cap-ibs=workaround'/>
  </qemu:commandline>
```

(BZ#1732726, BZ#1751054)

As máquinas virtuais IBM POWER não funcionam corretamente com os nós NUMA vazios

Atualmente, quando uma máquina virtual IBM POWER (VM) rodando em um host RHEL 8 é configurada com um nó NUMA que usa memória zero (**memória='0'**) e zero CPUs, a VM não pode iniciar. Portanto, a Red Hat recomenda fortemente não usar VMs POWER IBM com tais nós NUMA vazios no RHEL 8.

(BZ#1651474)

A topologia de CPU SMT não é detectada por VMs quando se usa o modo host passthrough no AMD EPYC

Quando uma máquina virtual (VM) inicia com o modo de passagem da CPU em um host AMD EPYC, a bandeira de recurso **TOPOEXT** CPU não está presente. Conseqüentemente, a VM não é capaz de detectar uma topologia de CPU virtual com múltiplas roscas por núcleo. Para contornar este problema, inicialize a VM com o modelo de CPU EPYC em vez de passthrough do host.

(BZ#1740002)

Os identificadores de disco na RHEL 8.2 VMs podem mudar na reinicialização da VM.

Ao utilizar uma máquina virtual (VM) com RHEL 8.2 como sistema operacional convidado em um hipervisor Hyper-V, os identificadores do dispositivo para os discos virtuais da VM em alguns casos mudam quando a VM é reinicializada. Por exemplo, um disco originalmente identificado como **/dev/sda** pode se tornar **/dev/sdb**. Como conseqüência, a VM pode falhar o boot, e scripts que referenciam os discos da VM podem parar de funcionar.

Para evitar este problema, a Red Hat recomenda fortemente a definição de nomes persistentes para os discos na VM. Para informações detalhadas, consulte a documentação do Microsoft Azure: <https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-device-names-problems>.

(BZ#1777283)

As máquinas virtuais às vezes falham ao utilizar muitos discos virtio-blk

A adição de um grande número de dispositivos virtio-blk a uma máquina virtual (VM) pode esgotar o número de vetores de interrupção disponíveis na plataforma. Se isso ocorrer, o sistema operacional convidado da VM não inicializa e exibe uma **fila de entrada de dados com dracut-initqueue[392]: Advertência: Não foi possível inicializar o** erro.

(BZ#1719687)

Anexar dispositivos LUN a máquinas virtuais usando o virtio-blk não funciona

O tipo de máquina q35 não suporta dispositivos de virtio 1.0 de transição e, portanto, a RHEL 8 não suporta características que foram depreciadas no virtio 1.0. Em particular, não é possível em um host RHEL 8 enviar comandos SCSI de dispositivos virtio-blk. Como conseqüência, a conexão de um disco físico como um dispositivo LUN a uma máquina virtual falha ao usar o controlador virtio-blk.

Observe que os discos físicos ainda podem ser passados para o sistema operacional convidado, mas devem ser configurados com a opção **dispositivo='disco'** em vez de **dispositivo='lun'**.

(BZ#1777138)

A migração de um convidado POWER9 de um hospedeiro RHEL 7-ALT para o RHEL 8 falha

Atualmente, a migração de uma máquina virtual POWER9 de um sistema host RHEL 7-ALT para o RHEL 8 torna-se insensível com um status "Migration status: active".

Para contornar este problema, desabilite as Transparent Huge Pages (THP) no host RHEL 7-ALT, o que permite que a migração seja concluída com sucesso.

(BZ#1741436)

11.15. APOIO

aferramenta de apoio aos adesivos não funciona com a política de criptografia do FUTURO

Como uma chave criptográfica utilizada por um certificado no API do Portal do Cliente não atende aos requisitos da política de criptografia do **FUTURO** em todo o sistema, o utilitário de **suporte de adesivos** não funciona com este nível de política no momento.

Para contornar este problema, use a política de criptografia **DEFAULT** enquanto se conecta ao API do Portal do Cliente.

(BZ#1802026)

11.16. CONTÊINERES

Não se espera que a UDICA trabalhe com o fluxo estável 1.0

A UDICA, a ferramenta para gerar políticas SELinux para contêineres, não deve trabalhar com contêineres que são executados via podman 1.0.x no fluxo do módulo **container-tools:1.0**.

(JIRA:RHELPLAN-25571)

Notas sobre o apoio FIPS com Podman

O Federal Information Processing Standard (FIPS) exige a utilização de módulos certificados. Anteriormente, Podman instalava corretamente os módulos certificados em contêineres, habilitando as bandeiras adequadas na partida. Entretanto, neste lançamento, a Podman não configura corretamente os ajudantes de aplicação adicionais normalmente fornecidos pelo sistema na forma da política criptográfica do sistema FIPS. Embora a configuração da política criptográfica de todo o sistema não seja exigida pelos módulos certificados, ela melhora a capacidade das aplicações de utilizar os módulos criptográficos de forma compatível. Para contornar este problema, troque seu recipiente para executar o comando **update-crypto-policies --set FIPS** antes que qualquer outro código de aplicação seja executado.

(BZ#1804193)

CAPÍTULO 12. INTERNACIONALIZAÇÃO

12.1. RED HAT ENTERPRISE LINUX 8 IDIOMAS INTERNACIONAIS

O Red Hat Enterprise Linux 8 suporta a instalação de múltiplos idiomas e a mudança de idiomas com base em suas exigências.

- Línguas do leste asiático - japonês, coreano, chinês simplificado e chinês tradicional.
- Línguas européias - inglês, alemão, espanhol, francês, italiano, português e russo.

A tabela a seguir lista as fontes e os métodos de entrada fornecidos para vários idiomas principais.

Idioma	Fonte padrão (Font Package)	Métodos de entrada
Inglês	dejavu-sans-fonts	
Francês	dejavu-sans-fonts	
Alemão	dejavu-sans-fonts	
Italiano	dejavu-sans-fonts	
Russo	dejavu-sans-fonts	
Espanhol	dejavu-sans-fonts	
Português	dejavu-sans-fonts	
Chinês simplificado	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
Chinês Tradicional	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
Japonês	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkkc
Coreano	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-hangul, libhangu

12.2. MUDANÇAS NOTÁVEIS NA INTERNACIONALIZAÇÃO DA RHEL 8

A RHEL 8 introduz as seguintes mudanças na internacionalização em comparação com a RHEL 7:

- Foi adicionado o suporte para o padrão da indústria de computação **Unicode 11**.
- A internacionalização é distribuída em múltiplos pacotes, o que permite instalações com menor espaço físico. Para mais informações, consulte [Utilizando lancheiras](#).

- As atualizações do pacote **glibc** para múltiplos locais estão agora sincronizadas com o Common Locale Data Repository (CLDR).

APÊNDICE A. LISTA DE BILHETES POR COMPONENTE

As identificações Bugzilla e JIRA estão listadas neste documento para referência. Os bugs do Bugzilla que são acessíveis ao público incluem um link para o bilhete.

Componente	Ingressos
389-ds-base	BZ#1715406 , BZ#1748016 , BZ#1790259 , BZ#1748994 , BZ#1739718
NetworkManager	BZ#1626348
anaconda	BZ#1747382 , BZ#1637472 , BZ#1748756 , BZ#1649359 , BZ#1715303 , BZ#1696609 , BZ#1672405 , BZ#1687747 , BZ#1745064 , BZ#1659400 , BZ#1821192 , BZ#1822880 , BZ#1823578 , BZ#1748281 , BZ#1746391
auditoria	BZ#1757986
authselect	BZ#1657295
bind	BZ#1564443 , BZ#1664863 , BZ#1704328
binutils	BZ#177777002 , BZ#1618748
buildah-container	BZ#1627898
clevis	BZ#1766526 , BZ#1564559 , BZ#1436780 , BZ#1784524
cloud-init	BZ#1641190 , BZ#1666961
cockpit-appstream	BZ#1676506
cockpit	BZ#1678465 , BZ#1754163 , BZ#1666722
módulo de ferramentas-container-rhel8	BZ#1784267
corosync-qdevice	BZ#1784200
createrepo_c	BZ#1743186
crypto-policies	BZ#1690565 , BZ#1660839
dispositivo-mapper-multipath	BZ#1797660
dhcp	BZ#1729211

Componente	Ingressos
distribuição	BZ#1657927
dnf	BZ#1676891, BZ#1754609
dnsmasq	BZ#1700916
edk2	BZ#1748180
elfutils	BZ#1744992
fapolicyd	BZ#1759895
agentes de vedação	BZ#1775847
firewalld	BZ#1737045, BZ#1740670, BZ#1733066
freeradius	BZ#1723362
gcc-toolset-9	BZ#1774118
gcc	BZ#1726641, BZ#1698607, BZ#1747157
gdb	BZ#1768593
gdm	BZ#1749960
glibc	BZ#1410154, BZ#1764214, BZ#1749439, BZ#1764235, BZ#1746928, BZ#1777241, BZ#1361965, BZ#1747502, BZ#1764218, BZ#1764238, BZ#1746933, BZ#1747453
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1724302
gnome-software	BZ#1668760
gnutls	BZ#1628553, BZ#1677754
go-toolset	BZ#1747150
grafana-pcp	BZ#1685315
grafana	BZ#1725278

Componente	Ingressos
graphviz	BZ#1704875
grub2	BZ#1583445, BZ#1723501
httpd-2.4-módulo	BZ#1747923
httpd	BZ#1633224
inicial-setup	BZ#1676439
ipa	BZ#1665051 , BZ#1816784 , BZ#1719767 , BZ#1777564 , BZ#1664719 , BZ#1664718
ipcalc	BZ#1638834
java-11-openjdk	BZ#1746875
kernel-rt	BZ#1680161
kernel	BZ#1744397, BZ#1698297, BZ#1687094, BZ#1720227, BZ#1846345, BZ#1635295, BZ#1793389, BZ#1706541, BZ#1666538, BZ#1602962, BZ#1649647, BZ#1153521, BZ#1694705, BZ#1348508, BZ#1748451, BZ#1708456, BZ#1654962, BZ#1609288, BZ#1777283, BZ#1791664, BZ#1792125, BZ#1792691, BZ#1812666, BZ#1812577, BZ#1757933, BZ#1763661, BZ#1780432, BZ#1401552, BZ#1716002, BZ#1593711, BZ#1620349, BZ#1724969, BZ#1714330, BZ#1714486, BZ#1660368, BZ#1524687, BZ#1274406, BZ#1650518, BZ#1636572, BZ#1727369, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1503672, BZ#1570255, BZ#1696451, BZ#1665295, BZ#1658840, BZ#1660627, BZ#1569610, BZ#1730502
kexec-tools	BZ#1750278, BZ#1690729
kmod-kvdo	BZ#1737639 , BZ#1657301
krb5	BZ#1754690
libbpf	BZ#1759154
libdnf	BZ#1697472

Componente	Ingressos
libgnome-keyring	BZ#1607766
libndp	BZ#1697595
libpfm	BZ#1731019
libreswan	BZ#1777474
libselenium-python-2,8-módulo	BZ#1666328
libvirt	BZ#1749672 , BZ#1664592, BZ#1528684
llvm-toolset	BZ#1747139
lorax	BZ#1754711
ltrace	BZ#1655368
lvm2	BZ#1600174, BZ#1496229, BZ#1768536
fazer	BZ#1774790
maven	BZ#1783926
mod_wsgi	BZ#1829692 , BZ#1779705
murmurar	BZ#1737553
nfs-utils	BZ#1719983 , BZ#1592011
nftables	BZ#1778883 , BZ#1643192
nginx	BZ#1668717
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1724250 , BZ#1817533 , BZ#1645153
numactl	BZ#1730738
opencv	BZ#1694647

Componente	Ingressos
openscap	BZ#163636431 , BZ#1618489 , BZ#1646197 , BZ#1803116 , BZ#1795563 , BZ#1824152 , BZ#1642373
openssh	BZ#1744108
openssl-pkcs11	BZ#1705505 , BZ#1664807 , BZ#1745082
openssl	BZ#1685470 , BZ#1749068
oscap-anaconda-addon	BZ#1665082 , BZ#1674001 , BZ#1691305 , BZ#1787156 , BZ#1816199
marcapasso	BZ#1712584 , BZ#1700104
pam	BZ#1252859 , BZ#1537242
pcp	BZ#1723598
pcs	BZ#1631519 , BZ#1631514 , BZ#1676431 , BZ#1442116 , BZ#1619620
perl-LDAP	BZ#1663063
php-7.2-módulo	BZ#1670386
php-pecl-xdebug	BZ#1769857
pki-core	BZ#1698084 , BZ#1303254
podman	BZ#1804193 , BZ#1645280
policoreutils	BZ#1563742 , BZ#1417455
postfix	BZ#1723950 , BZ#1745321
powertop	BZ#1716721
pykickstart	BZ#1637872
python-ply	BZ#1747490
python38-3,8-módulo	BZ#1747329

Componente	Ingressos
qemu-kvm	BZ#1651474 , BZ#1740002 , BZ#1719687 , BZ#1651994 , BZ#1741346
traseiro	BZ#1729501
redhat-release	BZ#1817591
redhat-support-tool	BZ#1802026
rhel-system-roles-sap	BZ#1660832
rng-tools	BZ#1692435
rpm	BZ#1688849
rsyslog	JIRA:RHELPLAN-10431 , BZ#1659383 , BZ#1679512 , BZ#1740683 , BZ#1676559 , BZ#1692073 , BZ#1692072
conjunto ferrugem	BZ#1776847
s390utils	BZ#1750326
samba	BZ#1754409 , JIRA:RHELPLAN-13195
scap-security-guide	BZ#1755447 , BZ#1754919 , BZ#1750755 , BZ#1755194
scap-workbench	BZ#1640715
selinux-policy	BZ#1641631 , BZ#1746398 , BZ#1826788 , BZ#1727887 , BZ#1726166 , BZ#1726246
setools	BZ#1731519
setroubleshoot-plugins	BZ#1649842
configuração	BZ#1730396 , BZ#1663556
skopeo-container	BZ#1627900
skopeo	BZ#1810053
sscg	BZ#1717880

Componente	Ingressos
sssd	BZ#1669407 , BZ#1652562 , BZ#1447945 , BZ#1754871
gerenciador de assinaturas	BZ#1674337
sudo	BZ#1786990 , BZ#1733961
systemd	BZ#1686892 , BZ#1640802
systemtap	BZ#1744989
tpm2-ferramentas	BZ#1725714
sintonizado	BZ#1738250
udica	BZ#1763210 , BZ#1732704
vdo	BZ#1713749
virt-manager	BZ#1677019
wayland	BZ#1673073
whois	BZ#1734183
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1698565
zlib	BZ#1659433 , BZ#1666798
outros	BZ#1640697 , BZ#1659609 , BZ#1687900 , BZ#1697896 , BZ#1797409 , BZ#1790635 , BZ#1823398 , BZ#1745507 , BZ#1732726 , BZ#1757877 , JIRA:RHELPLAN-25571 , BZ#1777138 , JIRA:RHELPLAN-27987 , BZ#1797671 , BZ#1780124 , JIRA:RHELPLAN-2507 , JIRA:RHELPLAN-37713 , JIRA:RHELPLAN-3777777 , BZ#1841170 , JIRA:RHELPLAN-13995 , BZ#1785248 , BZ#1755347 , BZ#1784455 , BZ#1784456 , BZ#1789401 , JIRA:RHELPLAN-41384 , BZ#1690207 , JIRA:RHELPLAN-1212 , BZ#1559616 , BZ#1812552 , JIRA:RHELPLAN-14047 , BZ#1769727 , JIRA:RHELPLAN-27394 , BZ#1642765 , JIRA:RHELPLAN-10304 , BZ#1646541 , BZ#1647725 , BZ#1686057 , BZ#1748980 , BZ#1827628

APÊNDICE B. HISTÓRICO DE REVISÃO

0.1-8

Qua Fev 10 2021, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentada uma questão conhecida (Virtualização).

0.1-7

Thu Jan 28 2021, Lucie Maňásková(lmanasko@redhat.com)

- Atualizado o capítulo Antevistas Tecnológicas.

0.1-6

Qui Dez 10 2020, Lenka Špačková(lspackova@redhat.com)

- Acrescentou informações sobre o manuseio de AD GPOs em SSSD a Novas características (Gerenciamento de Identidade).

0.1-5

Ter 01 dez. 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou uma correção de erros para emissão com fapolicyd (Segurança).
- Acrescentou um problema conhecido (Instalador).

0.1-4

Ter 24 de novembro de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Atualizada a seção Novos recursos (Networking).

0.1-3

Sexta-feira, 30 de outubro de 2020, Lenka Špačková(lspackova@redhat.com)

- Descrição atualizada dos fluxos de aplicação na seção Repositórios.

0.1-2

Seg 05 de outubro de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou uma correção de erros (Networking).

0.1-1

Ter 29 de setembro de 2020, Lenka Špačková(lspackova@redhat.com)

- Atualização do caminho de atualização no local com o lançamento do RHEL 7.9.

0.1-0

Qui 27 Ago 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou uma correção de erros (Kernel).

0.0-9

Seg 10 de agosto de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou um assunto conhecido (Gerenciamento de Identidade).

0.0-8

Ter 21 Jul 2020, Lucie Maňásková(lmanasko@redhat.com)

- Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 8.2.1.

0.0-7

Thu Jul 16 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou uma Pré-visualização Tecnológica (Networking).
- Atualizada a seção Novos recursos.

0.0-6

Thu Jun 25 2020, Jaroslav Klech(jklech@redhat.com)

- Granulou o capítulo de parâmetros do núcleo.
- Acrescentei várias melhorias ao capítulo de controladores de dispositivos.

0.0-5

Sex 19 de junho de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou novas questões conhecidas.
- Várias atualizações em outras notas de lançamento.

0.0-4

Thu Jun 04 Jun 2020, Lucie Maňásková(lmanasko@redhat.com)

- Atualizada a seção Novos recursos.
- Acrescentou um problema conhecido (Containers).

0.0-3

Quarta-feira 20 de maio de 2020, Lenka Špačková(lspackova@redhat.com)

- Acrescentou um problema conhecido (linguagens de programação dinâmica, servidores web e de banco de dados).
- Acrescentou uma correção de erros (Compiladores e ferramentas de desenvolvimento).
- Várias atualizações em outras notas de lançamento.

0.0-2

Ter 28 de abril de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 8.2.

0.0-1

Seg 09 Mar 2020, Jaroslav Klech(jklech@redhat.com)

- Proporcionou mudanças importantes nos parâmetros do núcleo externo e nos novos capítulos de drivers.

0.0-0

Ter 21 de janeiro de 2020, Lucie Maňásková(Imanasko@redhat.com)

- Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 8.2 Beta.