Red Hat Enterprise Linux 8

8.3 Notas de Lançamento

Notas de Lançamento do Red Hat Enterprise Linux 8.3

Last Updated: 2021-02-22

Red Hat Enterprise Linux 8 8.3 Notas de Lançamento

Notas de Lançamento do Red Hat Enterprise Linux 8.3

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 © 2021 | You need to change the HOLDER entity in the en-US/8.3_Release_Notes.ent file | 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 8.3 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
RHEL para Edge 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 7
Gestão da Identidade 7
O console web 7
Virtualização 7
Área de trabalho e gráficos 7
Atualização no local e conversão de SO 7
.NET 5 está agora disponível no RHEL 8 como uma prévia de tecnologia 8
O OpenJDK 11 já está disponível 9
Recursos adicionais 9
Laboratórios do Portal do Cliente Red Hat 9

CAPÍTULO 2. ARQUITETURAS 11

CAPÍTULO 3. DISTRIBUIÇÃO DO CONTEÚDO NO RHEL 8 12
3.1. INSTALAÇÃO 12
3.2. REPOSITÓRIOS 12
3.3. FLUXOS DE APLICAÇÃO 13

CAPÍTULO 4. LANÇAMENTO RHEL 8.3.1 14
4.1. NOVAS CARACTERÍSTICAS 14

CAPÍTULO 5. MUDANÇAS IMPORTANTES NOS PARÂMETROS DO KERNEL EXTERNO 16
Novos parâmetros do kernel 16
Parâmetros de kernel atualizados 17
Novos parâmetros /proc/sys/fs 20

CAPÍTULO 6. LANÇAMENTO RHEL 8.3.0 22
6.1. NOVAS CARACTERÍSTICAS 22
6.1.1. Instalador e criação de imagem 22
6.1.2. RHEL para Edge 24
6.1.3. Gestão de software 24
6.1.4. Conchas e ferramentas de linha de comando 25
6.1.5. Serviços de infra-estrutura 26
6.1.6. Segurança 29
6.1.7. Trabalho em rede 38
6.1.8. Kernel 40
6.1.9. Sistemas de arquivo e armazenamento 44
6.1.10. Alta disponibilidade e clusters 46
6.1.11. Linguagens de programação dinâmica, servidores web e de banco de dados 48
6.1.12. Compiladores e ferramentas de desenvolvimento 53
6.1.13. Gestão da Identidade 59
6.1.14. Desktop 66
6.1.15. Infra-estruturas gráficas 67
6.1.16. O console web 68
6.1.17. Funções do Sistema Red Hat Enterprise Linux 69

6.1.18. Virtualização 70
6.1.19. RHEL em ambientes de nuvens 76
6.1.20. Contêineres 76
6.1.21. Novos motoristas 77
Drivers de rede 77
Drivers gráficos e drivers diversos 77
6.1.22. Drivers atualizados 79
Atualizações de driver de rede 79
Atualizações do driver de armazenamento 79
Atualizações gráficas e de drivers diversos 79
6.2. CORREÇÃO DE ERROS 79
6.2.1. Instalador e criação de imagem 79
6.2.2. Gestão de software 81
6.2.3. Conchas e ferramentas de linha de comando 81
6.2.4. Segurança 82
6.2.5. Trabalho em rede 84
6.2.6. Kernel 85
6.2.7. Alta disponibilidade e clusters 87
6.2.8. Linguagens de programação dinâmica, servidores web e de banco de dados 87
6.2.9. Compiladores e ferramentas de desenvolvimento 88
6.2.10. Gestão da Identidade 91
6.2.11. Infra-estruturas gráficas 93
6.2.12. Virtualização 93
6.2.13. Contêineres 94
6.3. ANTEVISÕES TECNOLÓGICAS 94
6.3.1. Trabalho em rede 94
6.3.2. Kernel 96
6.3.3. Sistemas de arquivo e armazenamento 97
6.3.4. Alta disponibilidade e clusters 99
6.3.5. Gestão da Identidade 100
6.3.6. Desktop 101
6.3.7. Infra-estruturas gráficas 102
6.3.8. Funções do Sistema Red Hat Enterprise Linux 102
6.3.9. Virtualização 103
6.3.10. Contêineres 104
6.4. FUNCIONALIDADE DEPRECIADA 104
6.4.1. Instalador e criação de imagem 105
6.4.2. Gestão de software 106
6.4.3. Serviços de infra-estrutura 106
6.4.4. Segurança 106
6.4.5. Trabalho em rede 107
6.4.6. Kernel 108
6.4.7. Sistemas de arquivo e armazenamento 108
6.4.8. Gestão da Identidade 109
6.4.9. Desktop 110
6.4.10. Infra-estruturas gráficas 110
6.4.11. O console web 111
6.4.12. Funções do Sistema Red Hat Enterprise Linux 111
6.4.13. Virtualização 111
6.4.14. Contêineres 112
6.4.15. Pacotes depreciados 112
6.5. PROBLEMAS CONHECIDOS 112
6.5.1. Instalador e criação de imagem 113

6.5.2. Gestão de assinaturas 116
6.5.3. Serviços de infra-estrutura 116
6.5.4. Segurança 117
6.5.5. Trabalho em rede 122
6.5.6. Kernel 124
6.5.7. Sistemas de arquivo e armazenamento 128
6.5.8. Linguagens de programação dinâmica, servidores web e de banco de dados 130
6.5.9. Gestão da Identidade 130
6.5.10. Desktop 131
6.5.11. Infra-estruturas gráficas 132
6.5.12. O console web 133
6.5.13. Funções do Sistema Red Hat Enterprise Linux 133
6.5.14. Virtualização 133
6.5.15. RHEL em ambientes de nuvens 135
6.5.16. Apoio 136
6.5.17. Contêineres 136
6.6. INTERNACIONALIZAÇÃO 136
6.6.1. Red Hat Enterprise Linux 8 idiomas internacionais 136
6.6.2. Mudanças notáveis na internacionalização da RHEL 8 137

APÊNDICE A. LISTA DE BILHETES POR COMPONENTE 138

APÊNDICE B. HISTÓRICO DE REVISÃO 146

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 8.3, você pode configurar uma senha root e criar uma conta de usuário antes de iniciar a instalação. Anteriormente, você configurava uma senha de root e criava uma conta de usuário após iniciar o processo de instalação. Você também pode criar imagens personalizadas com base em um backend muito mais confiável e também empurrar imagens para nuvens através do console web RHEL.

RHEL para Edge

RHEL 8.3 apresenta **RHEL for Edge** para a instalação remota da RHEL em servidores Edge. A RHEL for Edge é uma imagem rpm-ostree que você pode compor usando o Image Builder. Você pode instalar a imagem usando um arquivo Kickstart e depois gerenciar a imagem para incluir atualizações de imagem e fazer com que a imagem volte a um estado funcional anterior.

A seguir, os principais destaques da RHEL for Edge:

- Atualizações atômicas, onde o estado de cada atualização é conhecido e nenhuma mudança é vista até que você reinicie o dispositivo.
- Controles de saúde personalizados e rollbacks inteligentes para garantir a resiliência.
- Fluxos de trabalho focados em contêineres, onde é possível separar as atualizações do SO principal das atualizações da aplicação, e testar e implantar diferentes versões de aplicações.
- Cargas úteis OTA otimizadas para ambientes de baixa largura de banda.

Para mais informações, veja Seção 6.1.2, “RHEL para Edge” .

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.

Segurança

A RHEL 8.3 fornece funções Ansible para implantações automatizadas de soluções de Decriptação Baseada em Políticas (PBD) usando **Clevis** e **Tang**, e esta versão do pacote **rhel-system-roles** também contém uma função Ansible para o registro RHEL através de **Rsyslog**.

Os pacotes de **guia scap-security-guide** foram rebaseados para a versão 0.1.50, e **OpenSCAP** foi rebaseado para a versão 1.3.3. Estas atualizações proporcionam melhorias substanciais, incluindo um perfil alinhado com o CIS RHEL 7 Benchmark v2.2.0 e um perfil alinhado com a Health Insurance Portability and Accountability Act (HIPAA) que é exigido pelas organizações de saúde norte-americanas.

Com esta atualização, você pode agora gerar funções de remediação baseadas em resultados a partir de perfis personalizados usando a ferramenta **SCAP Workbench**.

A estrutura **USBGuard** agora fornece sua própria política SELinux, notifica os usuários desktop na GUI, e a versão 0.7.8 contém muitas outras melhorias e correções de bugs.

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

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

- **nginx 1.18**
- **Node.js 14**

- **Perl 5.30**
- **PHP 7.4**
- **Ruby 2.7**

Os seguintes componentes foram atualizados no RHEL 8.3:

- **Git** para a versão 2.27
- **Squid** para a versão 4.11

Veja Seção 6.1.11, "Linguagens de programação dinâmica, servidores web e de banco de dados" para mais informações.

Conjuntos de ferramentas de compilação

Os seguintes conjuntos de ferramentas de compilação foram atualizados no RHEL 8.3:

- **GCC Toolset 10**
- **LLVM Toolset 10.0.1**
- **Rust Toolset 1.45.2**
- **Go Toolset 1.14.7**

Veja Seção 6.1.12, "Compiladores e ferramentas de desenvolvimento" para mais informações.

Gestão da Identidade

O conjunto de cifras Rivest Cipher 4 (RC4), o tipo de criptografia padrão para usuários, serviços e trusts entre domínios Active Directory (AD) em uma floresta AD, foi depreciado no RHEL 8. Por razões de compatibilidade, esta atualização introduz uma nova subpolítica criptográfica **AD-SUPPORT** para permitir o suporte ao tipo de criptografia RC4 depreciado. A nova sub-política permite o uso de RC4 com soluções de integração de Gerenciamento de Identidade RHEL (IdM) e SSSD Active Directory.

Veja Seção 6.1.13, "Gestão da Identidade" para mais informações.

O console web

O console web oferece uma opção para alternar entre acesso administrativo e acesso limitado de dentro de uma sessão do usuário.

Virtualização

Máquinas virtuais (VMs) hospedadas no hardware IBM Z podem agora usar o recurso IBM Secure Execution. Isto torna as VMs resistentes a ataques se o host for comprometido, e também evita que hosts não confiáveis obtenham informações da VM. Além disso, os dispositivos DASD podem agora ser atribuídos às VMs no IBM Z.

Área de trabalho e gráficos

Agora você pode usar o desktop GNOME em sistemas IBM Z.

O subsistema gráfico do kernel **Direct Rendering Manager** (DRM) foi rebaseado para a versão 5.6 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.

Veja Seção 6.1.14, "Desktop" e Seção 6.1.15, "Infra-estruturas gráficas" para mais detalhes.

Atualização no local e conversão de SO

In-place upgrade from RHEL 7 to RHEL 8

Os caminhos de atualização suportados no local são atualmente:

- Da RHEL 7.8 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: IBM POWER 9 (little endian) e IBM Z (Estrutura A)
- De RHEL 7.7 a RHEL 8.2 em sistemas com SAP HANA.

Para garantir que seu sistema permaneça compatível após a atualização para o RHEL 8.2, atualize para a última versão do RHEL 8.3 ou ative os repositórios do RHEL 8.2 Extended Update Support (EUS). Em sistemas com SAP HANA, ative os repositórios RHEL 8.2 Update Services for SAP Solutions (E4S).

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:

- O**salto** agora suporta a entrada do usuário ao gerar perguntas verdadeiro/falso para determinar como proceder com a atualização.
- Agora você pode atualizar vários hosts simultaneamente usando a interface web Satellite UI.
- A atualização no local agora é suportada para instâncias sob demanda na AWS e Microsoft Azure, usando a Infra-estrutura de Atualização da Red Hat (RHUI).
- Com o lançamento da assessoria RHBA-2021:0569, você pode criar scripts personalizados para o relatório de pré-atualização do **Leapp**. Consulte Automatizando seu fluxo de trabalho do relatório de pré-atualização do Red Hat Enterprise Linux para obter detalhes.

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 .

Conversion from a different Linux distribution to RHEL

Se você estiver usando o CentOS 8 ou Oracle Linux 8, você pode converter seu sistema operacional para RHEL 8 usando o utilitário **Convert2RHEL**. Para mais informações, consulte https://red.ht/migrate.

Se você estiver usando uma versão anterior do CentOS ou Oracle Linux, ou seja, as versões 6 ou 7, você pode converter seu sistema operacional para RHEL e, em seguida, realizar uma atualização no local para RHEL 8.

.NET 5 está agora disponível no RHEL 8 como uma prévia de tecnologia

O .NET 5 está agora disponível como uma prévia tecnológica no Red Hat Enterprise Linux 8 e na plataforma OpenShift Container. O .NET 5 inclui novas versões em idiomas: C# 9 e F# 5.0. Foram feitas melhorias significativas de desempenho nas bibliotecas de base, GC e JIT. .NET 5 tem **aplicações de arquivo único**, o que permite distribuir aplicações .NET como um único executável, com todas as dependências incluídas. Imagens UBI8 para .NET 5 estão disponíveis no registro de contêineres da Red Hat e podem ser usadas com o OpenShift.

Para usar .NET 5, instale o pacote **dotnet-sdk-5.0**:

```
$ sudo dnf install -y dotnet-sdk-5.0
```

Para mais informações, consulte a documentação .NET 5.

O OpenJDK 11 já está disponível

A nova versão do Open Java Development Kit (OpenJDK) já está disponível. Para mais informações sobre os recursos introduzidos neste lançamento e as mudanças nas funcionalidades existentes, consulte os recursos do OpenJDK.

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
- Auxiliar de Atualização do Red Hat Enterprise Linux
- 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 8.3 é distribuído com o kernel versão 4.18.0-240, 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 freqüência 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 8.3.1

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 8.3.1 são descritos abaixo.

4.1. NOVAS CARACTERÍSTICAS

Pacotes Flatpak para várias aplicações desktop

Flatpak é um sistema para executar aplicações gráficas como containers. Usando Flatpak, você pode instalar e atualizar uma aplicação independentemente do sistema operacional do host.

Esta atualização fornece imagens de recipientes Flatpak das seguintes aplicações no catálogo de recipientes Red Hat Container:

Nome da aplicação	Identificação do recipiente Flatpak
Firefox	org.mozilla.firefox
GIMP	org.gimp.GIMP
Inkscape	org.inkscape.Inkscape
Thunderbird	org.mozilla.Thunderbird

Para instalar recipientes Flatpak disponíveis no Catálogo de Recipientes Red Hat, use o seguinte procedimento:

1. Certifique-se de que a última versão do cliente Flatpak esteja instalada em seu sistema:

```
# atualização do yum flatpak
```

2. Habilitar o repositório RHEL Flatpak:

```
# flatpak remoto-add rhel https://flatpaks.redhat.io/rhel.flatpakrepo
```

3. Forneça as credenciais para sua conta RHEL:

```
# podman login registry.redhat.io
```

   Por padrão, Podman salva as credenciais somente até que o usuário faça o logout.

4. Opcional: Guarde suas credenciais permanentemente:

```
$ cp $XDG_RUNTIME_DIR/containers/auth.json \
    $HOME/.config/flatpak/oci-auth.json
```

5. Instale a imagem do contêiner Flatpak:

```
$ flatpak instalar rhel container-id
```

(JIRA:RHELPLAN-30958)

Rust Toolset rebaseado para a versão 1.47.0

O Rust Toolset foi atualizado para a versão 1.47.0. As mudanças notáveis incluem:

- As funções avaliadas em tempo de compilação **const fn** foram melhoradas e agora podem usar características de controle de fluxo, por exemplo, **se**, **enquanto**, e **combinar**.
- A nova anotação **#[track_caller]** pode agora ser colocada em funções. Os pânicos das funções anotadas relatam a pessoa que telefona como a fonte.
- A Biblioteca Padrão da Ferrugem agora implementa genericamente características para arrays de qualquer comprimento. Anteriormente, muitas das implementações de traços para matrizes eram preenchidas apenas para comprimentos entre 0 e 32.

Para instruções detalhadas sobre o uso, consulte Utilização do conjunto de ferramentas enferrujadas .

(BZ#1883839)

O papel do Sistema de Logging agora suporta filtro baseado em propriedade em suas saídas

Com esta atualização, filtros baseados em propriedades foram adicionados à saída de arquivos, à saída de arquivos para a frente e à saída de arquivos remotos da função do sistema de registro. O recurso é fornecido pela sub-rotina **rsyslog** subjacente, e é configurável através da Função do Sistema de Logging RHEL. Como resultado, os usuários podem se beneficiar da capacidade de filtrar as mensagens de log pelas propriedades, tais como nome da máquina, etiqueta, e a própria mensagem é útil para gerenciar logs.

(BZ#1889492)

O papel do Sistema de Logging RHEL agora suporta o comportamento do rsyslog

Com este aprimoramento, **o rsyslog** recebe a mensagem da Virtualização da Red Hat e encaminha a mensagem para a **pesquisa elástica**.

(BZ#1889893)

A imagem do recipiente ubi8/pause já está disponível

Podman agora usa o **ubi8/pause** em vez da imagem do recipiente **k8s.gcr.io/pause** para segurar as informações do espaço de nomes da rede da cápsula.

(BZ#1690785)

CAPÍTULO 5. MUDANÇAS IMPORTANTES NOS PARÂMETROS DO KERNEL EXTERNO

Este capítulo fornece aos administradores de sistemas um resumo das mudanças significativas no kernel enviado com o Red Hat Enterprise Linux 8.3. Estas mudanças podem incluir, por exemplo, entradas **proc** adicionadas ou atualizadas, valores default **sysctl** e **sysfs**, parâmetros de inicialização, opções de configuração do kernel ou quaisquer mudanças perceptíveis de comportamento.

Novos parâmetros do kernel

acpi_no_watchdog = [HW,ACPI,WDT]

Este parâmetro permite ignorar a Interface Avançada de Configuração e Alimentação (ACPI) baseada na interface de vigilância (WDAT) e deixar o motorista nativo controlar o dispositivo de vigilância.

dfltcc = [HW,S390]

Este parâmetro configura o suporte de hardware **zlib** para as arquiteturas IBM Z.
Formato: { on | on | off | def_only | inf_only | always }

As opções são:

- **on** (padrão) - suporte de hardware IBM **Zlib** para compressão no nível 1 e descompressão
- **off** - Sem suporte de hardware IBM **Zlib**
- **def_only** - Suporte de hardware IBM **Zlib** somente para o algoritmo **deflate** (compressão no nível 1)
- **inf_only** - Suporte de hardware IBM **Zlib** somente para o algoritmo **inflacionado** (descompressão)
- **sempre** - Semelhante ao **anterior**, mas ignora o nível de compressão selecionado e usa sempre o suporte de hardware (usado para depuração)

irqchip.gicv3_pseudo_nmi = [ARM64]

Este parâmetro permite o suporte de pseudo interrupções não-máscaras (NMIs) no núcleo.
Para utilizar este parâmetro é necessário construir o kernel com o item de configuração **CONFIG_ARM64_PSEUDO_NMI**.

panic_on_taint =

Máscara de bits para chamar condicionalmente o **pânico()** em **add_taint()**
Formato

Uma máscara de bit hexadecimal que representa um conjunto de bandeiras **TAINT** que causará pânico no kernel quando a chamada ao sistema **add_taint()** for invocada com qualquer uma das bandeiras deste conjunto. A chave opcional **nousertaint** evita falhas forçadas pelo espaço do usuário ao escrever no arquivo **/proc/sys/kernel/tainted** qualquer flagset que combine com a máscara de bit em **panic_on_taint**.

Para obter mais informações, consulte a documentação a montante.

prot_virt = [S390]

Formato

Este parâmetro permite a hospedagem de máquinas virtuais protegidas que estão isoladas do hipervisor se o suporte de hardware estiver presente.

rcutree.use_softirq = [KNL]

Este parâmetro permite a eliminação do processamento do **softirq** da TREERCU.
Se você definir este parâmetro como zero, ele move todo o processamento **RCU_SOFTIRQ** para kthreads rcuc per-CPU. Se você definir **rcutree.use_softirq** para um valor diferente de zero (padrão), **RCU_SOFTIRQ** é usado por padrão. Especifique **rcutree.use_softirq=0** para usar rcuc kthreads.

split_lock_detect = [X86]

Este parâmetro permite a detecção de bloqueio dividido. Quando ativado, e se houver suporte de hardware, instruções atômicas que acessam dados através dos limites da linha de cache resultarão em uma exceção de verificação de alinhamento.
As opções são:

- **desligado** - não habilitado
- **aviso** - o kernel emitirá avisos de taxa limitada sobre as aplicações que acionam a Exceção de Verificação de Alinhamento (#AC). Este modo é o padrão nas CPUs que suportam a detecção de bloqueio dividido.
- **fatal** - o kernel enviará o sinal de erro Buss (SIGBUS) para aplicações que acionem a exceção #AC.
  Se a exceção #AC for atingida enquanto não for executada no modo usuário, o kernel emitirá um erro oops tanto no modo de **advertência** quanto no modo **fatal**.

srbds = [X86,INTEL]

Este parâmetro controla a atenuação da amostragem de dados de registro especial (SRBDS). Certas CPUs são vulneráveis a um exploit semelhante ao MDS (Microarchitectural Data Sampling), que pode vazar bits do gerador de números aleatórios.

Por padrão, o microcódigo atenua este problema. Entretanto, a correção do microcódigo pode fazer com que as instruções **RDRAND** e **RDSEED** fiquem muito mais lentas. Entre outros efeitos, isto resultará na redução da produção do dispositivo fonte de número aleatório do kernel **do urandom**.

Para desativar a mitigação do microcódigo, defina a seguinte opção:

- **off** - Desabilitar a mitigação e remover o impacto do desempenho para o **RDRAND** e **RDSEED**

svm = [PPC]

Formato: { on | off | y | n | 1 | 0 }
Este parâmetro controla o uso do Mecanismo de Execução Protegida em sistemas pSeries.

nopv = [X86,XEN,KVM,HYPER_V,VMWARE]

Este parâmetro desabilita as otimizações PV que forçam o convidado a funcionar como convidado genérico sem drivers PV.
Atualmente são apoiados os convidados XEN HVM, KVM, HYPER_V e VMWARE.

Parâmetros de kernel atualizados

hugepagesz = [HW]

Este parâmetro especifica um enorme tamanho de página. Use este parâmetro em conjunto com o parâmetro **hugepages** para pré-alocar um número de páginas enormes do tamanho especificado. Especifique os parâmetros **hugepagesz** e **hugepages** em pares, como por exemplo:

```
hugepagesz=2M hugepages=512
```

O parâmetro **hugepagesz** só pode ser especificado uma vez na linha de comando para um tamanho de página enorme específico. Os tamanhos de página enormes válidos dependem da arquitetura.

hugepages = [HW]

Este parâmetro especifica o número de páginas enormes a serem pré-alocadas. Este parâmetro normalmente segue o parâmetro válido **hugepagesz** ou **default_hugepagesz**.
Entretanto, se **hugepages** é o primeiro ou o único parâmetro de linha de comando HugeTLB, ele especifica implicitamente o número de páginas enormes do tamanho padrão a serem alocadas. Se o número de páginas enormes do tamanho padrão for implicitamente especificado, ele não pode ser sobrescrito pelo par de parâmetros **hugepagesz hugepages** para o tamanho padrão.

Por exemplo, em uma arquitetura com 2M de tamanho de página padrão enorme:

```
hugepages=256 hugepagesz=2M hugepages=512
```

As configurações do exemplo acima resultam na alocação de 256 2M páginas enormes e uma mensagem de aviso de que o parâmetro **hugepages=512** foi ignorado. Se as **hugepages** forem precedidas por **hugepagesz** inválidas, as **hugepages** serão ignoradas.

default_hugepagesz = [HW]

Este parâmetro especifica o tamanho padrão de página enorme. Você pode especificar o **padrão_hugepagesz** apenas uma vez na linha de comando. Opcionalmente, você pode seguir o parâmetro **hugepagesz padrão** com o parâmetro **hugepagesz** para pré-alocar um número específico de páginas enormes com o tamanho padrão. Além disso, você pode especificar implicitamente o número de páginas enormes de tamanho padrão para pré-alocar.
Por exemplo, em uma arquitetura com 2M de tamanho de página padrão enorme:

```
hugepages=256
default_hugepagesz=2M hugepages=256
hugepages=256 default_hugepagesz=2M
```

As configurações do exemplo acima resultam na alocação de 256 2M de páginas enormes. O tamanho padrão válido de página enorme depende da arquitetura.

efi = [EFI]

Formato: "old_map", "nochunk", "noruntime", "debug", "nosoftreserve" }
As opções são:

- **old_map** [X86-64] - Mudar para o antigo mapeamento de serviços de tempo de execução EFI baseado em ioremap. 32 bits ainda usa este por padrão
- **nochunk** - Desabilitar a leitura de arquivos em "pedaços" no toco de inicialização do EFI, já que a leitura de pedaços pode causar problemas com algumas implementações de firmware
- **noruntime** - Desativar o suporte aos serviços de tempo de execução da EFI
- **debug** - Habilitar saída de depuração diversa

- **nosoftreserve** - O atributo **EFI_MEMORY_SP** (Specific Purpose) às vezes faz com que o kernel reserve a faixa de memória para um driver de mapeamento de memória a reivindicar. Especifique **efi=nosoftreserve** para desativar esta reserva e tratar a memória por seu tipo de base (por exemplo **EFI_CONVENTIONAL_MEMORY** / "System RAM").

intel_iommu = [DMAR]

Remapping de Acesso Direto à Memória Intel IOMMU (DMAR).
As opções adicionais são:

- **noboun**ce (Default off) - Desabilita o buffer de ressalto para dispositivos não confiáveis, como os dispositivos Thunderbolt. Isto tratará os dispositivos não confiáveis como os dispositivos de confiança. Portanto, este ajuste pode expor riscos de segurança de ataques de acesso direto à memória (DMA).

mem = nn[KMG] [KNL,BOOT] [KNL,BOOT

Este parâmetro força o uso de uma quantidade específica de memória.
A quantidade de memória a ser utilizada nos casos a seguir:

1. Para teste.
2. Quando o núcleo não é capaz de ver toda a memória do sistema.
3. A memória que fica após o limite do **memorial** é excluída do hipervisor, sendo então atribuída aos convidados da KVM.
   [X86] Trabalho como limite de endereço máximo. Use junto com o parâmetro **memmap** para evitar colisões físicas do espaço de endereços. Sem o **memmap**, os dispositivos de interconexão de componentes periféricos (PCI) poderiam ser colocados em endereços pertencentes à RAM não utilizada.

   Observe que esta configuração só tem efeito durante o tempo de inicialização, já que no caso 3 acima, a memória pode precisar ser adicionada quente após a inicialização se a memória do sistema de hipervisor não for suficiente.

pci = [PCI]

Várias opções de subsistema de Interconexão de Componentes Periféricos (PCI).
Algumas opções aqui presentes funcionam num dispositivo específico ou num conjunto de dispositivos (**<pci_dev>**). Estes são especificados num dos seguintes formatos:

```
[<domain>:]<bus>:<dev>.<func>[/<dev>.<func>]*
pci:<vendor>:<device>[:<subvendor>:<subdevice>]
```

Note que o primeiro formato especifica um barramento PCI/dispositivo/endereço de função que pode mudar se novo hardware for inserido, se o firmware da placa-mãe mudar, ou devido a mudanças causadas por outros parâmetros do kernel. Se o domínio for deixado indeterminado, é considerado zero. Opcionalmente, um caminho para um dispositivo através de múltiplos endereços de dispositivos/funções pode ser especificado após o endereço base (isto é mais robusto contra problemas de renumeração). O segundo formato seleciona dispositivos usando IDs do espaço de configuração que podem corresponder a múltiplos dispositivos no sistema.

As opções são:

- **hpmmiosize** - A quantidade fixa de espaço de ônibus que é reservada para a janela de E/S (MMIO) da ponte hotplug. O tamanho padrão é de 2 megabytes.

- **hpmmioprefsize** - A quantidade fixa de espaço de ônibus que é reservada para a janela MMIO_PREF da ponte hotplug. O tamanho padrão é de 2 megabytes.

pcie_ports = [PCIE]

Manuseio de serviços de porta PCIe (Peripheral Component Interconnect Express).
As opções são:

- **nativo** - Use serviços PCIe nativos (PME, AER, DPC, PCIe hotplug) mesmo que a plataforma não dê permissão ao sistema operacional para usá-los. Este cenário pode causar conflitos se a plataforma também tentar utilizar estes serviços.
- **dpc-native** - Use o serviço PCIe nativo somente para DPC. Esta configuração pode causar conflitos se o firmware usar AER ou DPC.
- **compatriota** - Desabilitar serviços PCIe nativos (PME, AER, DPC, PCIe hotplug).

rcu_nocbs = [KNL]

O argumento é uma lista de CPU. A seqüência "tudo" pode ser usada para especificar cada CPU do sistema.

usbcore.authorized_default = [USB]

A autorização padrão do dispositivo USB.
As opções são:

- -**1** (Default) - Autorizado, exceto para USB sem fio
- **0** - Não autorizado
- **1** - Autorizado
- **2** - Autorizado se o dispositivo estiver conectado à porta interna

usbcore.old_scheme_first = [USB]

Este parâmetro permite começar com o antigo esquema de inicialização do dispositivo. Esta configuração se aplica somente a dispositivos de baixa e alta velocidade (padrão 0 = desligado).

usbcore.quirks = [USB]

Uma lista de entradas quirk para aumentar a lista de entradas quirk do núcleo USB embutido. As entradas da lista são separadas por vírgulas. Cada entrada tem o formulário **VendorID:ProductID:Flags**, por exemplo **quirks=0781:5580:bk,0a5c:5834:gij**. O **IDs** são números hexadecimais de 4 dígitos e **Flags** é um conjunto de letras. Cada letra mudará o quirk incorporado; definindo-o se estiver claro e limpando-o se estiver definido.
As bandeiras adicionadas:

- **o** - **USB_QUIRK_HUB_SLOW_RESET**, o hub precisa de um atraso extra após o reset de sua porta

Novos parâmetros /proc/sys/fs

protected_fifos

Este parâmetro é baseado nas restrições do software Openwall e fornece proteção, permitindo evitar escritas não intencionais para um FIFO controlado por atacantes, onde um programa destinado a criar um arquivo regular.
As opções são:

- **0** - Escrever para FIFOs é irrestrito.
- **1** - Não permite que a bandeira **O_CREAT** abra em FIFOs que não possuímos em diretórios pegajosos escrevíveis no mundo, a menos que sejam de propriedade do proprietário do diretório.
- **2** - Aplica-se a diretórios pegajosos e graváveis em grupo.

protected_regular

Este parâmetro é semelhante ao parâmetro **protegido_fifos**, porém evita escrever em um arquivo regular controlado por um atacante, onde um programa pretende criar um.
As opções são:

- **0** - Escrever para arquivos regulares é irrestrito.
- **1** - Não permite a abertura da bandeira **O_CREAT** em arquivos regulares que não possuímos em diretórios pegajosos graváveis no mundo, a menos que sejam de propriedade do proprietário do diretório.
- **2** - Aplica-se a diretórios pegajosos e graváveis em grupo.

CAPÍTULO 6. LANÇAMENTO RHEL 8.3.0

6.1. NOVAS CARACTERÍSTICAS

Esta parte descreve as novas características e principais melhorias introduzidas no Red Hat Enterprise Linux 8.3.

6.1.1. Instalador e criação de imagem

Anaconda rebaseado para a versão 33.16

Com este lançamento, o Anaconda foi rebaseado para a versão 33.16. Esta versão oferece as seguintes melhorias notáveis em relação à versão anterior.

- O Programa de Instalação agora exibe endereços IPv6 estáticos em várias linhas e não redimensiona mais as janelas.
- O Programa de Instalação agora exibe os tamanhos do setor de dispositivos NVDIMM suportados.
- O nome do host agora está configurado corretamente em um sistema instalado com configuração estática IPv6.
- Agora você pode usar caracteres não-ASCII em frases-passe de criptografia de disco.
- O Programa de Instalação exibe uma recomendação apropriada para criar um novo sistema de arquivo em /boot, /tmp, e todos os pontos de montagem /var e /usr exceto /usr/local e /var/wwww.
- O Programa de Instalação agora verifica corretamente o layout do teclado e não muda o status da tela Layout do Teclado quando as teclas do teclado (ALT SHIFT) são usadas para alternar entre diferentes layouts e idiomas.
- O modo de salvamento não falha mais nos sistemas com partições RAID1 existentes.
- A mudança da versão LUKS do recipiente está agora disponível na tela de **particionamento manual**.
- O Programa de Instalação termina com sucesso a instalação sem o pacote **btrfs-progs**.
- O Programa de Instalação agora usa a versão padrão LUKS2 para um recipiente criptografado.
- O Programa de Instalação não trava mais quando um arquivo Kickstart coloca volumes físicos (PVs) de um grupo de volume lógico (VG) em uma lista de **risco ignorada**.
- Introduz um novo caminho de montagem **/mnt/sysroot** para a raiz do sistema. Este caminho é usado para montar / do sistema alvo. Normalmente, a raiz física e a raiz do sistema são as mesmas, portanto **/mnt/sysroot** é anexado ao mesmo sistema de arquivo que **/mnt/sysimage**. As únicas exceções são os sistemas rpm-ostree, onde a raiz do sistema muda com base na implantação. Então, o **/mnt/sysroot** é anexado a um subdiretório de **/mnt/sysimage**. Recomenda-se o uso do **/mnt/sysroot** para o chroot.

(BZ#1691319, BZ#1679893, BZ#1684045, BZ#1688478, BZ#1700450, BZ#1720145, BZ#1723888, BZ#1754977, BZ#1755996, BZ#1784360, BZ#1796310, BZ#1871680)

Mudanças na GUI no Programa de Instalação RHEL

O Programa de Instalação RHEL agora inclui as seguintes configurações de usuário na janela Resumo da Instalação:

- Senha de raiz
- Criação do usuário

Com esta mudança, você pode agora configurar uma senha root e criar uma conta de usuário antes de iniciar a instalação. Anteriormente, você configurava uma senha de root e criava uma conta de usuário após iniciar o processo de instalação.

Uma senha root é usada para entrar na conta do administrador (também conhecida como superusuário ou root) que é usada para tarefas de administração do sistema. O nome do usuário é usado para fazer o login a partir de uma linha de comando; se você instalar um ambiente gráfico, então seu gerenciador de login gráfico usa o nome completo. Para mais detalhes, veja *Performing a standard RHEL installation* documento.

(JIRA:RHELPLAN-40469)

O Image Builder backend **osbuild-composer** substitui o **lorax-composer**

O backend **osbuild-composer** substitui o **lorax-composer**. O novo serviço fornece APIs REST para a construção de imagens. Como resultado, os usuários podem se beneficiar de um backend mais confiável e de imagens de saída mais previsíveis.

(BZ#1836211)

Image Builder **osbuild-composer** suporta um conjunto de tipos de imagens

Com a substituição do backend **osbuild-composer**, o seguinte conjunto de tipos de imagens suportadas no **osbuild-composer** desta vez:

- Arquivo TAR (.tar)
- QEMU QCOW2 (.qcow2)
- VMware Virtual Machine Disk (.vmdk)
- Amazon Machine Image (.ami)
- Azure Disk Image (.vhd)
- OpenStack Image (.qcow2)

As seguintes saídas não são suportadas desta vez:

- sistema ext4-filesystem
- disco particionado
- Nuvem de Alibaba
- Google GCE

(JIRA:RHELPLAN-42617)

Image Builder agora apóia o empurrar para as nuvens através da GUI

Com esta melhoria, ao criar imagens, os usuários podem escolher a opção de empurrar para as nuvens de serviço **Azure** e **AWS** através do GUI **Image Builder**. Como resultado, os usuários podem se beneficiar de uploads e instantâneos mais fáceis.

(JIRA:RHELPLAN-30878)

6.1.2. RHEL para Edge

Apresentando as imagens RHEL for Edge

Com este lançamento, você pode agora criar imagens RHEL personalizadas para servidores Edge.

Você pode usar o Image Builder para criar imagens RHEL for Edge e depois usar o instalador RHEL para implantá-las em sistemas AMD e Intel de 64 bits. O Image Builder gera uma imagem RHEL for Edge como **rel-edge-commit** em um arquivo **.tar**.

Uma imagem RHEL for Edge é uma imagem **rpm-ostree** que inclui pacotes de sistema para instalação remota da RHEL nos servidores Edge.

Os pacotes do sistema incluem:

- Pacote de OS base
- Podman como o motor do contêiner

Você pode personalizar a imagem para configurar o conteúdo do SO de acordo com suas necessidades, e pode implantá-los em máquinas físicas e virtuais.

Com uma imagem RHEL for Edge, você pode conseguir o seguinte:

- Atualizações atômicas, onde o estado de cada atualização é conhecido e nenhuma mudança é vista até que você reinicie o dispositivo.
- Verificações sanitárias personalizadas usando Greenboot e rollbacks inteligentes para resiliência em caso de atualizações falhadas.
- Fluxos de trabalho focados em contêineres, onde é possível separar as atualizações do SO principal das atualizações da aplicação, e testar e implantar diferentes versões de aplicações.
- Cargas úteis OTA otimizadas para ambientes de baixa largura de banda.
- Verificações sanitárias personalizadas usando o Greenboot para garantir a resiliência.

Para mais informações sobre composição, instalação e gerenciamento das imagens RHEL for Edge, consulte Composição, instalação e gerenciamento das imagens RHEL for Edge .

(JIRA:RHELPLAN-56676)

6.1.3. Gestão de software

O valor padrão para a **melhor** opção de configuração dnf foi alterado de **Verdadeiro** para **Falso**

Com esta atualização, o valor para a **melhor** opção de configuração dnf foi definido para **True** no arquivo de configuração padrão para manter o comportamento dnf original. Como resultado, para os usuários que utilizam o arquivo de configuração padrão, o comportamento permanece inalterado.

Se você fornecer seus próprios arquivos de configuração, certifique-se de que a opção **best=True** esteja presente para manter o comportamento original.

(BZ#1832869)

Nova opção --norepopath para o comando dnf reposync já está disponível

Anteriormente, o comando **reposync** criou um subdiretório sob o diretório **--download-path** para cada repositório baixado, por padrão. Com esta atualização, a opção **--norepopath** foi introduzida, e o **reposync** não cria o subdiretório. Como resultado, o repositório é baixado diretamente para o diretório especificado por **--download-path**. Esta opção também está presente no **YUM v3**.

(BZ#1842285)

Habilidade de ativar e desativar os plugins libdnf

Anteriormente, a verificação da assinatura era codificada em código rígido na versão RHEL dos plug-ins **libdnf**. Com esta atualização, o utilitário **microdnf** pode ativar e desativar os plug-ins **libdnf**, e a verificação de assinatura pode agora ser desativada da mesma forma que no DNF. Para desativar a verificação de assinatura, use o comando **--disableplugin=subscription-manager**. Para desabilitar todos os plug-ins, use o comando **--noplugins**.

(BZ#1781126)

6.1.4. Conchas e ferramentas de linha de comando

Atualizações doReaR

RHEL 8.3 introduz uma série de atualizações na utilidade Relax-and-Recover**(ReaR**). As mudanças notáveis incluem:

- Foi adicionado suporte para o gerenciamento de dados Rubrik Cloud Data Management (CDM) de terceiros como software de backup externo. Para utilizá-lo, defina a opção **BACKUP** no arquivo de configuração para **CDM**.
- Criação de uma imagem de resgate com um arquivo maior que 4 GB no IBM POWER, pouca arquitetura endian foi habilitada.
- O layout do disco criado pela **ReaR** não inclui mais entradas para os dispositivos Rancher 2 Longhorn iSCSI e sistemas de arquivo.

(BZ#1743303)

smartmontools rebaseado para a versão 7.1

O pacote **smartmontools** foi atualizado para a versão 7.1, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Adições de HDD, SSD e USB ao banco de dados da unidade.
- Novas opções **-j** e **--json** para habilitar o modo de saída JSON.
- Solução para a resposta incompleta das subpáginas de **Log** de algumas SSDs SAS.
- Melhor manuseio do comando **READ CAPACITY**.
- Várias melhorias para a decodificação das páginas de registro.

(BZ#1671154)

opencryptoki rebaseado para a versão 3.14.0

Os pacotes **opencryptoki** foram atualizados para a versão 3.14.0, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Melhorias no serviço criptográfico EP11:
  - Suporte de dilítio
  - Suporte ao algoritmo de assinatura digital Edwards-curve (EdDSA)
  - Suporte de Rivest-Shamir-Adleman com almofada de criptografia assimétrica ideal (RSA-OAEP) com hash não-SHA1 e função de geração de máscara (MGF)
- Processo aprimorado e travamento da rosca
- Melhora no bloqueio de **árvores** e objetos
- Suporte para o novo hardware IBM Z z15
- Suporte de múltiplas instâncias token para módulo de plataforma confiável (TPM), arquitetura criptográfica IBM (ICA) e instalação de serviço criptográfico integrado (ICSF)
- Adicionada uma nova ferramenta **p11sak**, que lista as chaves token em um repositório de token **openCryptoki**
- Adicionado um utilitário para migrar um repositório de fichas para criptografia compatível com FIPS
- Ferramenta fixa **pkcsep11_migrate**
- Pequenas correções do software do ICSF

(BZ#1780293)

gpgme rebaseado para a versão 1.13.1.

Os pacotes **gpgme** foram atualizados para a versão upstream 1.13.1. Mudanças notáveis incluem:

- Novas bandeiras de contexto **sem cache de chaves** (tem um efeito quando usado com GnuPG 2.2.7 ou posterior), **request-origin** (tem um efeito quando usado com GnuPG 2.2.6 ou posterior), **auto-localização de chaves**, e **modelo de confiança** foram introduzidos.
- A nova ferramenta **gpgme-json** como servidor nativo de mensagens para navegadores web foi adicionada. A partir de agora, a criptografia e decodificação de chaves públicas é suportada.
- Foi introduzida uma nova API de criptografia para suportar a especificação direta de chaves, incluindo a opção de recipientes ocultos e a retirada de chaves de um arquivo. Isto também permite o uso de uma subchave.

(BZ#1829822)

6.1.5. Serviços de infra-estrutura

powertop rebaseado para a versão 2.12

Os pacotes **powertop** foram atualizados para a versão 2.12. Mudanças notáveis em relação à versão 2.11, anteriormente disponível, incluem:

- Uso do Device Interface Power Management (DIPM) para link SATA PM.
- Suporte aos sistemas móveis e desktop Intel Comet Lake, ao servidor Skylake e à arquitetura Tremont baseada em Atom (Jasper Lake).

(BZ#1783110)

sintonizado rebaseado para a versão 2.14.0

Os pacotes **ajustados** foram atualizados para a versão upstream 2.14.0. Melhorias notáveis incluem:

- Foi introduzido o perfil de **otimização-console de série**.
- Foi adicionado suporte para um perfil pós-carregado.
- Foi adicionado o plugin do **irqbalance** para o manuseio das configurações do **irqbalance**.
- Foi adicionado o ajuste específico de arquitetura para as plataformas Marvell ThunderX e AMD.
- O plug-in do programador foi estendido para suportar **cgroups-v1** para ajuste de afinidade de CPU.

(BZ#1792264)

tcpdump rebaseado para a versão 4.9.3

O utilitário **tcpdump** foi atualizado para a versão 4.9.3 para corrigir as Vulnerabilidades e Exposições Comuns (CVE).

(BZ#1804063)

libpcap rebaseada para a versão 1.9.1

Os pacotes **da libpcap** foram atualizados para a versão 1.9.1 para corrigir as Vulnerabilidades e Exposições Comuns (CVE).

(BZ#1806422)

iperf3 agora suporta a opção sctp no lado do cliente

Com esta melhoria, o usuário pode usar o Stream Control Transmission Protocol (SCTP) em vez do Transmission Control Protocol (TCP) no lado do cliente para testar o rendimento da rede.

As seguintes opções para o **iperf3** estão agora disponíveis no lado do cliente dos testes:

- **--sctp**
- **--xbind**
- **--nstreams**

Para obter mais informações, consulte **Opções Específicas do Cliente** na página de manual **iperf3**.

(BZ#1665142)

iperf3 agora suporta SSL

Com esta melhoria, o usuário pode usar a autenticação RSA entre o cliente e o servidor para restringir as conexões ao servidor apenas a clientes legítimos.

As seguintes opções para o **iperf3** estão agora disponíveis no lado do servidor:

- **--rsa-private-key-path**
- **--authorized-users-path**

As seguintes opções para o **iperf3** estão agora disponíveis no lado do cliente da comunicação:

- **--nome do usuário**
- **--rsa-public-key-path**

(BZ#1700497)

ligante rebaseado a 9.11.20

O pacote **bind** foi atualizado para a versão 9.11.20, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Aumento da confiabilidade em sistemas com muitos núcleos de CPU, através da fixação de várias condições de corrida.
- Relatório detalhado de erros: **Dig** e outras ferramentas podem agora imprimir a opção Extended DNS Error (EDE), se ela estiver presente.
- Os IDs das mensagens nas transferências do Protocolo de Transferência de Zona DNS de entrada (AXFR) são verificados e registrados, quando são inconsistentes.

(BZ#1818785)

Um novo perfil TuneD de otimização-console serial para reduzir E/S para consoles seriais, baixando o valor da impressão

Com esta atualização, está disponível um novo perfil TuneD de **otimização-console serial**. Em alguns cenários, os drivers do kernel podem enviar grandes quantidades de operações de E/S para o console serial. Tal comportamento pode causar uma falta de resposta temporária enquanto a E/S é escrita no console serial. O perfil do **console serial otimizado** reduz esta E/S ao baixar o valor de **impressão** do padrão de **7 4 1 7**para **4 4 1 7**. Os usuários com um console serial que desejarem fazer esta mudança em seu sistema podem instrumentar seu sistema da seguinte forma:

```
# perfil tuned-adm profile throughput performance optimize-console de série
```

Como resultado, os usuários terão um valor de **impressão** mais baixo que persiste durante uma reinicialização, o que reduz a probabilidade de que o sistema fique pendurado.

Este perfil TuneD reduz a quantidade de E/S escritas no console serial ao remover informações de depuração. Se você precisar coletar estas informações de depuração, você deve garantir que este perfil não esteja habilitado e que o valor de sua **impressão** esteja definido para **7 4 1 7**. Para verificar o valor da execução da **impressão**:

```
# cat /proc/sys/kernel/printk
```

(BZ#1840689)

Novos perfis TuneD adicionados para as plataformas baseadas em AMD

No RHEL 8.3, o perfil de **desempenho de produção** TuneD foi atualizado para incluir o ajuste para as plataformas baseadas em AMD. Não há necessidade de alterar nenhum parâmetro manualmente e a sintonia é aplicada automaticamente no sistema **AMD**. Os sistemas **AMD Epyc Naples** e **Roma** alteram os seguintes parâmetros no perfil padrão de **desempenho de produção**:

sched_migration_cost_ns=5000000 e **kernel.numa_balancing=0**

Com esta melhoria, o desempenho do sistema é melhorado em ~5%.

(BZ#1746957)

relembrado para a versão 1.5.22

Os pacotes **memcached** foram atualizados para a versão 1.5.22. As mudanças notáveis em relação à versão anterior incluem:

- O TLS foi ativado.
- A opção **-o inline_ascii_response** foi removida.
- A opção **-Y [authfile]** foi adicionada junto com o modo de autenticação para o protocolo ASCII.
- **memcached** pode agora recuperar seu cache entre as reinicializações.
- Novos meta comandos experimentais foram adicionados.
- Várias melhorias de desempenho.

(BZ#1809536)

6.1.6. Segurança

Cyrus O SASL agora suporta a ligação de canais com os plug-ins SASL/GSSAPI e SASL/GSS-SPNEGO

Esta atualização adiciona suporte para a fixação de canais com os plug-ins **SASL/GSSAPI** e **SASL/GSS-SPNEGO**. Como resultado, quando usado nas bibliotecas **openldap**, este recurso permite que **Cyrus SASL** mantenha compatibilidade e acesso ao Microsoft Active Directory e aos sistemas Microsoft Windows que estão introduzindo a vinculação obrigatória de canais para conexões LDAP.

(BZ#1817054)

Libreswan rebaseado para 3,32

Com esta atualização, Libreswan foi rebaseada para a versão 3.32, que inclui várias novas características e correções de bugs. As características notáveis incluem:

- Libreswan não requer mais a certificação separada FIPS 140-2.
- Libreswan agora implementa as recomendações criptográficas do RFC 8247, e muda a preferência de SHA-1 e RSA-PKCS v1.5 para SHA-2 e RSA-PSS.
- Libreswan suporta interfaces ipsecXX virtuais XFRMi que simplificam a escrita de regras de firewall.

- A recuperação de nós que se chocaram e reinicializaram em uma rede de criptografia de malha completa é melhorada.

(BZ#1820206)

A biblioteca libssh foi rebaseada para a versão 0.9.4

A biblioteca **libssh**, que implementa o protocolo SSH, foi atualizada para a versão 0.9.4.

Esta atualização inclui correções e melhorias de bugs, inclusive:

- Adicionado suporte para as chaves **Ed25519** em arquivos PEM.
- Adicionado suporte para o algoritmo de troca de chaves **diffie-hellman-group14-sha256**.
- Adicionado suporte ao **usuário local** na palavra-chave **Match** no arquivo de configuração do cliente **libssh**.
- Os critérios de**correspondência** de argumentos de palavras-chave agora são sensíveis a maiúsculas e minúsculas (note que as palavras-chave não são sensíveis a maiúsculas e minúsculas, mas os argumentos de palavras-chave são sensíveis a maiúsculas e minúsculas)
- CVE-2019-14889 e CVE-2020-1730 fixos.
- Adicionado suporte para a criação recorrente de diretórios ausentes encontrados na cadeia de caminho fornecida para o arquivo conhecido do anfitrião.
- Adicionado suporte para chaves **OpenSSH** em arquivos PEM com comentários e espaços brancos principais.
- Removido a inclusão da configuração do servidor **OpenSSH** da configuração do servidor **libssh**.

(BZ#1804797)

gnutls rebaseados para 3.6.14

Os pacotes de **gnutls** foram rebaseados para a versão upstream 3.6.14. Esta versão fornece muitas correções e melhorias de bugs, mais notadamente:

- **gnutls** agora rejeita certificados com campos de **tempo** que contenham caracteres inválidos ou formatação.
- **gnutls** agora verifica os certificados CA de confiança para tamanhos mínimos de chaves.
- Ao exibir uma chave privada criptografada, o utilitário **certtool** não inclui mais sua descrição em texto simples.
- Os servidores que utilizam **gnutls** agora anunciam o suporte de grampeamento OCSP.
- Os clientes que utilizam **gnutls** agora enviam grampos OCSP somente mediante solicitação.

(BZ#1789392)

gnutls FIPS DH verifica agora em conformidade com NIST SP 800-56A rev. 3

Esta atualização dos pacotes de **gnutls** fornece verificações exigidas pela Publicação Especial NIST 800-56A Revisão 3, seções 5.7.1.1 e 5.7.1.2, etapa 2. A mudança é necessária para futuras certificações FIPS 140-2. Como resultado, **os gnutls** agora aceitam apenas parâmetros 2048-bit ou maiores da RFC 7919 e RFC 3526 durante a troca de chaves Diffie-Hellman quando operando no modo FIPS.

(BZ#1849079)

gnutls agora realiza validações de acordo com NIST SP 800-56A rev 3

Esta atualização dos pacotes **gnutls** acrescenta as verificações exigidas pela Publicação Especial NIST 800-56A Revisão 3, seções 5.6.2.2.2.2 e 5.6.2.1.3, etapa 2. A adição prepara **os gnutls** para futuras certificações FIPS 140-2. Como resultado, **os gnutls** realizam etapas adicionais de validação para chaves públicas geradas e recebidas durante a troca de chaves Diffie-Hellman quando operando no modo FIPS.

(BZ#1855803)

update-crypto-policies e fips-mode-setup mudado para crypto-policies-scripts

Os scripts **update-crypto-policies** e **fips-mode-setup**, que anteriormente estavam incluídos no pacote **crypto-policies**, são agora movidos para um subpacote separado RPM **crypto-policies-scripts**. O pacote é instalado automaticamente através do pacote Recomenda a dependência de instalações regulares. Isto permite que a imagem **ubi8/ubi-minimal** evite a inclusão do intérprete da linguagem Python e assim reduz o tamanho da imagem.

(BZ#1832743)

OpenSC rebaseado para a versão 0.20.0

O pacote **opensc** foi rebaseado para a versão 0.20.0 que trata de múltiplos bugs e problemas de segurança. Mudanças notáveis incluem:

- Com esta atualização, **CVE-2019-6502**, **CVE-2019-15946**, **CVE-2019-15945**, **CVE-2019-19480**, **CVE-2019-19481** e **CVE-2019-19479** as questões de segurança são resolvidas.
- O módulo OpenSC agora suporta as funções **C_WrapKey** e **C_UnwrapKey**.
- Agora você pode usar a facilidade para detectar a inserção e remoção de leitores de cartões, como esperado.
- O utilitário **pkcs11** agora suporta o atributo **CKA_ALLOWED_MECHANISMS**.
- Esta atualização permite a detecção padrão dos cartões **OsEID**.
- A Carta OpenPGP v3 agora suporta **Elliptic Curve Cryptography** (ECC).
- O PKCS#11 URI agora truncata o nome do leitor com elipse.

(BZ#1810660)

stunnel rebaseado para a versão 5.56

Com esta atualização, o invólucro de criptografia **do stunnel** foi rebaseado para a versão 5.56 a montante, que inclui várias novas características e correções de bugs. As características notáveis incluem:

- Novas opções de **ticketKeySecret** e **ticketMacSecret** que controlam a confidencialidade e a proteção da integridade dos bilhetes de sessão emitidos. Estas opções permitem retomar sessões em outros nós em um cluster.
- Nova opção de **curvas** para controlar a lista de curvas elípticas no OpenSSL 1.1.0 e posteriores.
- Nova opção de **ciphersuites** para controlar a lista de ciphersuites TLS 1.3 permitidos.

- Adicionados **sslVersion**, **sslVersionMin** e **sslVersionMax** para OpenSSL 1.1.0 e posteriores.

(BZ#1808365)

libkcapi rebaseada para a versão 1.2.0

O pacote **libkcapi** foi rebaseado para a versão upstream 1.2.0, que inclui pequenas mudanças.

(BZ#1683123)

setools rebaseados para 4.3.0

O pacote **setools**, que é uma coleção de ferramentas projetadas para facilitar a análise política da SELinux, foi atualizado para a versão 4.3.0.

Esta atualização inclui correções e melhorias de bugs, inclusive:

- Método **sediff** revisado para regras de Type Enforcement (TE), que reduz significativamente os problemas de memória e tempo de execução.
- Acrescentou suporte de contexto **infiniband** ao **seinfo**, **sediff**, e **apol**.
- Adicionada configuração **apol** para a localização da ferramenta Qt assistente utilizada para exibir a documentação on-line.
- Problemas fixos com **sediff**:
  - Cabeçalho de propriedades exibindo quando não solicitado.
  - Comparação de nomes de arquivos de **tipo_transição**.
- Permissão fixa para o **envio de** informações **para a** direção do fluxo de informações.
- Acrescentou métodos à classe **TypeAttribute** para torná-la uma coleção Python completa.
- **Genfscon** agora procura classes, em vez de usar valores fixos que foram descartados da **libsepol**.

O pacote de **setools** requer os seguintes pacotes:

- **setools-console**
- **setools-console-analises**
- **setools-gui**

(BZ#1820079)

Os arquivos e diretórios CephFS individuais podem agora ter etiquetas SELinux

O Sistema de Arquivos Ceph (CephFS) permitiu recentemente o armazenamento de etiquetas SELinux nos atributos estendidos dos arquivos. Anteriormente, todos os arquivos em um volume CephFS eram etiquetados com um único **sistema de** etiquetas **comum_u:object_r:cephfs_t:s0**. Com esta melhoria, é possível mudar as etiquetas para arquivos individuais, e o SELinux define as etiquetas dos arquivos recém-criados com base nas regras de transição. Note que arquivos anteriormente não rotulados ainda têm a etiqueta **system_u:object_r:cephfs_t:s0** até serem explicitamente modificados.

(BZ#1823764)

OpenSCAP rebaseado para a versão 1.3.3

Os pacotes **openscap** foram atualizados para a versão upstream 1.3.3, que fornece muitas correções e melhorias em relação à versão anterior, mais notadamente:

- Adicionado o script **autotailor** que lhe permite gerar arquivos sob medida usando uma interface de linha de comando (CLI).
- Adicionada a parte de fuso horário à Lista de Verificação de Configuração Extensível Formato de Descrição de Testes (XCCDF) Carimbos de início e fim de tempo
- Acrescentou a sonda independente **do conteúdo do yamlfile** como um rascunho de implementação.
- Introduziu a **urna:xccdf:fix:script:kubernetes** fix tipo em XCCDF.
- Capacidade adicional de gerar a correção **machineconfig**.
- A ferramenta **oscap-podman** pode agora detectar alvos ambíguos de escaneamento ambíguos.
- A sonda **rpmverifyfile** pode agora verificar os arquivos do diretório **/bin**.
- Corrigidas falhas quando regexes complicados são executados na sonda de **conteúdo de arquivo de texto58**.
- As características de avaliação do relatório XCCDF são agora consistentes com as entidades OVAL da sonda **system_info**.
- Correspondência fixa do padrão de caminho de arquivo no modo off-line na sonda de **conteúdo de arquivo de texto58**.
- Fixada a repetição infinita na sonda de **dependência do sistema**.

(BZ#1829761)

O Guia de Segurança SCAP agora fornece um perfil alinhado com o CIS RHEL 8 Benchmark v1.0.0

Com esta atualização, os pacotes **scap-security-guide** fornecem um perfil alinhado com o CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0. O perfil permite que você endureça a configuração do sistema usando as diretrizes do Center for Internet Security (CIS). Como resultado, você pode configurar e automatizar a conformidade de seus sistemas RHEL 8 com o CIS usando o CIS Ansible Playbook e o perfil CIS SCAP.

Note que a regra **rpm_verify_permissions** no perfil do CIS não funciona corretamente.

(BZ#1760734)

guia de segurança da scap agora fornece um perfil que implementa o HIPAA

Esta atualização dos pacotes de **guia de segurança do seguro** de saúde acrescenta o perfil da Health Insurance Portability and Accountability Act (HIPAA) ao conteúdo de conformidade de segurança RHEL 8. Este perfil implementa as recomendações descritas no website da Regra de Privacidade da HIPAA.

A Norma de Segurança HIPAA estabelece as normas nacionais dos EUA para proteger as informações eletrônicas de saúde pessoal dos indivíduos que são criadas, recebidas, usadas ou mantidas por uma entidade coberta. A Regra de Segurança requer salvaguardas administrativas, físicas e técnicas

apropriadas para garantir a confidencialidade, integridade e segurança das informações de saúde protegidas eletronicamente.

(BZ#1832760)

guia de segurança de scap-guia rebaixado para 0,1,50

Os pacotes **scap-security-guide**, que contêm o mais recente conjunto de políticas de segurança para sistemas Linux, foram atualizados para a versão 0.1.50.

Esta atualização inclui correções e melhorias de bugs, mais notadamente:

- O conteúdo possível foi melhorado: numerosas regras contêm remediações possíveis pela primeira vez e outras regras foram atualizadas para resolver problemas de correção.
- Correções e melhorias no conteúdo do **scap-security-guide** para varredura dos sistemas RHEL7, inclusive:
  - Os pacotes de **guias de segurança scap** agora fornecem um perfil alinhado com a marca de referência CIS RHEL 7 v2.2.0. Observe que a regra **rpm_verify_permissions** no perfil CIS não funciona corretamente; veja **rpm_verify_permissions** fails in the CIS profile known issue.
  - Os perfis do Guia de Segurança SCAP agora desabilitam e mascaram corretamente os serviços que não devem ser iniciados.
  - As **regras de auditoria dos comandos privilegiados** nos pacotes de **guia de segurança de scap** agora funcionam corretamente para comandos privilegiados.
  - A remediação da regra **dconf_gnome_login_banner_text** nos pacotes **scap-security-guide** não falha mais incorretamente.

(BZ#1815007)

SCAP Workbench pode agora gerar remediações baseadas em resultados a partir de perfis personalizados

Com esta atualização, você pode agora gerar funções de remediação baseadas em resultados a partir de perfis personalizados usando a ferramenta **SCAP Workbench**.

(BZ#1640715)

Nova função possível fornece implantações automatizadas dos clientes Clevis

Esta atualização do pacote **rhel-system-roles** introduz o papel do sistema **nbde_client** RHEL. Esta função possível permite que você implante vários clientes Clevis de forma automatizada.

(BZ#1716040)

Novo papel possível agora pode criar um servidor Tang

Com esta melhoria, você pode implantar e gerenciar um servidor Tang como parte de uma solução automatizada de criptografia de disco com o novo papel do sistema **nbde_server**. O **nbde_server** Ansible role, que está incluído no pacote **rhel-system-roles**, suporta as seguintes características:

- Chaves Tang rotativas
- Implantação e backup de chaves Tang

Para mais informações, consulte as chaves de servidor Tang rotativo .

(BZ#1716039)

clevis rebaseada para a versão 13

Os pacotes **clevis** foram rebaseados para a versão 13, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- **clevis luks unlock** pode ser usado no dispositivo com um arquivo chave no modo não-interativo.
- **clevis encripta tpm2** analisa o campo **pcr_ids** se a entrada for dada como uma matriz JSON.
- A página man **clevis-luks-unbind(1**) não se refere mais apenas ao LUKS v1.
- **clevis luks bind** não escreve mais para um slot inativo, se a senha dada estiver incorreta.
- **clevis luks bind** agora funciona enquanto o sistema utiliza o local não-inglês.
- Suporte adicional para **tpm2-tools** 4.x.

(BZ#1818780)

clevis luks edit permite editar uma configuração de pino específica

Esta atualização dos pacotes **clevis** introduz o novo sub-comando **clevis luks edit** que permite editar uma configuração de pino específica. Por exemplo, agora você pode alterar o endereço URL de um servidor Tang e o parâmetro **pcr_ids** em uma configuração TPM2. Você também pode adicionar e remover novos pinos **sss** e alterar o limiar de um pino **sss**.

(BZ#1436735)

clevis luks bind -y agora permite encadernação automatizada

Com este aprimoramento, Clevis suporta a encadernação automatizada com o parâmetro **-y**. Agora você pode usar a opção **-y** com o comando **clevis luks bind**, que responde automaticamente às solicitações subseqüentes com *yes*. Por exemplo, ao usar um pino Tang, você não é mais obrigado a confiar manualmente nas teclas Tang.

(BZ#1819767)

fapolicyd rebaseado para a versão 1.0

Os pacotes **fapolicyd** foram rebaseados para a versão 1.0, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- O problema de sincronização de múltiplos fios foi resolvido.
- Desempenho aprimorado com redução do tamanho do banco de dados e do tempo de carregamento.
- Uma nova opção de confiança para o pacote **fapolicyd** no arquivo **fapolicyd.conf** foi adicionada para personalizar o back end de confiança. Você pode adicionar todos os arquivos, binários e scripts confiáveis ao novo arquivo **/etc/fapolicyd/fapolicyd.trust**.
- Você pode gerenciar o arquivo **fapolicyd.trust** usando o CLI.
- Você pode limpar ou descarregar o banco de dados usando o CLI.

- O pacote **fapolicyd** substitui o banco de dados mágico para uma melhor decodificação dos scripts. O CLI imprime o tipo MIME do arquivo semelhante ao comando de arquivo de acordo com a substituição.
- O arquivo **/etc/fapolicyd/fapolicyd.rules** suporta um grupo de valores como valores de atributo.
- O daemon **fapolicyd** tem uma opção **syslog_format** para definir o formato dos eventos de **auditoria/silog**.

(BZ#1817413)

fapolicyd agora fornece sua própria política SELinux em fapolicyd-selinux

Com este aprimoramento, a estrutura **fapolicyd** agora fornece sua própria política de segurança SELinux. O daemon está confinado sob o domínio **fapolicyd_t** e a política é instalada através do subpacote **fapolicyd-selinux**.

(BZ#1714529)

USBGuard rebaseado para a versão 0.7.8

Os pacotes **usbguard** foram rebaseados para a versão 0.7.8, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- O parâmetro **HidePII=true|false** no arquivo **/etc/usbguard/usbguard-daemon.conf** pode agora ocultar informações pessoalmente identificáveis das entradas de auditoria.
- O arquivo **AuthorizedDefault=keep|none|all|internal** parameter in the **/etc/usbguard/usbguard-daemon.conf** pode predefinir o estado de autorização dos dispositivos controladores.
- Com o novo atributo de regra **tipo com-conexão**, os usuários podem agora distinguir o tipo de conexão do dispositivo.
- Os usuários podem agora anexar regras temporárias com a opção **-t**. As regras temporárias permanecem na memória apenas até que o daemon reinicie.
- **as regras da lista usbguard** podem agora filtrar regras de acordo com determinadas propriedades.
- **usbguard gerar-política** pode agora gerar uma política para dispositivos específicos.
- O comando **usbguard allow|block|reject** pode agora lidar com as cadeias de regras, e um alvo é aplicado em cada dispositivo que corresponda à cadeia de regras especificada.
- Novos subpacotes **usbguard-notifier** e **usbguard-selinux** estão incluídos.

(BZ#1738590)

OUSBGuard oferece muitas melhorias para usuários corporativos de desktop

Esta adição ao projeto USBGuard contém melhorias e correções de bugs para melhorar a usabilidade para usuários corporativos de desktop. As mudanças importantes incluem:

- Para manter o arquivo de regras **/etc/usbguard/rules.conf** limpo, os usuários podem definir vários arquivos de configuração dentro do diretório **RuleFolder=/etc/usbguard/rules.d/**. Por padrão, o *RuleFolder* é especificado no arquivo **/etc/usbguard/usbguard/rules.conf**.

- A ferramenta **usbguard-notifier** agora fornece notificações GUI. A ferramenta notifica o usuário sempre que um dispositivo é conectado ou desconectado e se o dispositivo é permitido, bloqueado ou rejeitado por qualquer usuário.
- Agora você pode incluir comentários nos arquivos de configuração, porque as linhas **usbguard-daemon** não mais parses começando com **#**.

(BZ#1667395)

USBGuard agora fornece sua própria política SELinux em usbguard-selinux

Com este aprimoramento, a estrutura **USBGuard** agora fornece sua própria política de segurança SELinux. O daemon está confinado sob o domínio **usbguard_t** e a política é instalada através do subpacote **usbguard-selinux**.

(BZ#1683567)

alibcap agora suporta capacidades ambientais

Com esta atualização, os usuários são capazes de conceder capacidades ambientais no login e evitar a necessidade de ter acesso às raízes para os processos adequadamente configurados.

(BZ#1487388)

A biblioteca da libseccomp foi rebaseada para a versão 2.4.3

A biblioteca **da libseccomp**, que fornece uma interface para o mecanismo de filtragem de chamadas do sistema **seccomp**, foi atualizada para a versão 2.4.3.

Esta atualização fornece numerosas correções e melhorias de bugs. As mudanças notáveis incluem:

- Atualizou a tabela de **chamada de sistema** para o Linux v5.4-rc4.
- Não mais definindo valores **__NR_x** para chamadas de sistema que não existem.
- **__SNR_x** é agora utilizado internamente.
- Adicionado **definir** para **__SNR_ppoll**.
- Corrigido um problema de multiplexação com chamadas de sistema s390/s390x shm*.
- Removida a bandeira **estática** da compilação das ferramentas da **libseccomp**.
- Suporte adicional para chamadas de sistema relacionadas ao **io-uring**.
- Corrigido o problema do nome do módulo Python introduzido na versão v2.4.0; o módulo é nomeado **seccomp** como era anteriormente.
- Corrigido um vazamento potencial de memória identificado pelo **tilintar** da ferramenta **scmp_bpf_sim**.

(BZ#1770693)

o móduloomamqp1 agora é suportado

Com esta atualização, o protocolo **AMQP 1.** 0 suporta o envio de mensagens para um destino no ônibus. Anteriormente, o Openstack usava o protocolo **AMQP1** como padrão de comunicação, e este protocolo agora pode registrar mensagens em mensagens AMQP. Esta atualização introduz o sub-

pacote **rsyslog-omamqp1** para entregar o modo de saída **omamqp1**, que registra mensagens e as envia para o destino no ônibus.

(BZ#1713427)

OpenSCAP comprime conteúdo remoto

Com esta atualização, OpenSCAP utiliza a compressão **gzip** para transferir conteúdo remoto. O tipo mais comum de conteúdo remoto é a alimentação CVE baseada em texto, que aumenta de tamanho com o tempo e normalmente tem que ser baixada para cada varredura. A compressão **gzip** reduz a largura de banda para 10% da largura de banda necessária para o conteúdo não comprimido. Como resultado, isto reduz os requisitos de largura de banda em toda a cadeia entre o sistema escaneado e o servidor que hospeda o conteúdo remoto.

(BZ#1855708)

O Guia de Segurança SCAP agora fornece um perfil alinhado com o NIST-800-171

Com esta atualização, os pacotes de **guia de segurança da scap** proporcionam um perfil alinhado com a norma NIST-800-171. O perfil permite endurecer a configuração do sistema de acordo com os requisitos de segurança para proteção de Informações Não Classificadas Controladas (CUI) em sistemas de informação não-federais. Como resultado, é mais fácil configurar os sistemas para serem alinhados com a norma NIST-800-171.

(BZ#1762962)

6.1.7. Trabalho em rede

Os módulos de rastreamento de conexão IPv4 e IPv6 foram fundidos no módulo nf_conntrack

Este aprimoramento funde os módulos de rastreamento de conexão **nf_conntrack_ipv4** e **nf_conntrack_ipv6** Netfilter no módulo do kernel do **nf_conntrack**. Devido a esta mudança, a lista negra dos módulos específicos da família de endereços não funciona mais no RHEL 8.3, e você pode colocar na lista negra apenas o módulo **nf_conntrack** para desativar o suporte de rastreamento de conexão tanto para os protocolos IPv4 como IPv6.

(BZ#1822085)

firewalld rebaseado para a versão 0.8.2

Os pacotes **firewalld** foram atualizados para a versão 0.8.2, que fornece uma série de correções de bugs em relação à versão anterior. Para detalhes, veja as Notas de Lançamento do firewalld 0.8.2 .

(BZ#1809636)

NetworkManager rebaseado para a versão 1.26.0

Os pacotes **NetworkManager** foram atualizados para a versão upstream 1.26.0, que fornece uma série de melhorias e correções de bugs em relação à versão anterior:

- O NetworkManager restabelece a auto-negociação, velocidade e ajuste duplex para seu valor original ao desativar um dispositivo.
- Os perfis Wi-Fi conectam-se agora automaticamente se todas as tentativas de ativação anteriores falharem. Isto significa que uma falha inicial na conexão automática à rede não mais bloqueia o automatismo. Um efeito colateral é que os perfis Wi-Fi existentes que antes estavam bloqueados agora se conectam automaticamente.

- As páginas de homem **nm-settings-nmcli(5**) e **nm-settings-dbus(5**) foram adicionadas.
- Foi adicionado suporte para uma série de parâmetros de ponte.
- Foi adicionado suporte para as interfaces de encaminhamento e encaminhamento virtual (VRF). Para mais detalhes, consulte Reutilização permanente do mesmo endereço IP em interfaces diferentes.
- Foi adicionado suporte ao modo de criptografia sem fio Opportunistic Wireless Encryption mode (OWE) para redes Wi-Fi.
- O NetworkManager agora suporta prefixos de 31 bits em links IPv4 ponto-a-ponto de acordo com a RFC 3021.
- O utilitário **nmcli** agora suporta a remoção de configurações usando a **modificação da conexão nmcli**
- O NetworkManager não cria e ativa mais dispositivos escravos se faltar um dispositivo mestre.

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

- NetworkManager 1.26.0
- NetworkManager 1.24.0

(BZ#1814746)

O XDP é condicionalmente suportado

A Red Hat suporta o recurso eXpress Data Path (XDP) somente se todas as condições a seguir se aplicarem:

- Você carrega o programa XDP em uma arquitetura AMD ou Intel de 64 bits
- Você usa a biblioteca **libxdp** para carregar o programa no kernel
- O programa XDP usa um dos seguintes códigos de retorno: **XDP_ABORTED**, **XDP_DROP**, ou **XDP_PASS**
- O programa XDP não utiliza a descarga de hardware XDP

Para detalhes sobre os recursos XDP não suportados, veja Visão geral dos recursos XDP que estão disponíveis como Technology Preview

(BZ#1889736)

xdp-tools é totalmente suportado

O pacote **xdp-tools**, que contém utilitários de suporte de espaço do usuário para o recurso eXpress Data Path (XDP) do kernel, é agora suportado nas arquiteturas AMD e Intel 64-bit. Isto inclui a biblioteca **libxdp**, o utilitário **xdp-loader** para carregar programas XDP, o programa de exemplo **xdp-filter** para filtragem de pacotes e o utilitário **xdpdump** para capturar pacotes de uma interface de rede com o XDP habilitado.

(BZ#1820670)

O utilitário dracut por padrão agora usa o NetworkManager no disco RAM inicial

Anteriormente, o utilitário **dracut** estava usando um script shell para gerenciar a rede no disco RAM inicial, **initrd**. Em certos casos, isto poderia causar problemas. Por exemplo, o NetworkManager envia outro pedido DHCP, mesmo que o script no disco RAM já tenha solicitado um endereço IP, o que poderia resultar em um timeout.

Com esta atualização, o **dracut** por padrão agora usa o NetworkManager no disco RAM inicial e evita que o sistema se depare com problemas. Caso você queira voltar à implementação anterior e recriar as imagens do disco RAM, use os seguintes comandos:

```
# echo 'add_dracutmodules+=" network-legacy "' > /etc/dracut.conf.d/enable-network-legacy.conf

# dracut -vf --regenerate-all
```

(BZ#1626348)

A configuração da rede na linha de comando do kernel foi consolidada sob o parâmetro ip

Os parâmetros **ipv6**, **netmask**, **gateway** e **hostname** para definir a configuração da rede na linha de comando do kernel foram consolidados sob o parâmetro **ip**. O parâmetro **ip** aceita formatos diferentes, tais como os seguintes:

```
ip=__IP_address__:__peer__:__gateway_IP_address__:__net_mask__:__host_name__:__interface_name__:__configuration_method__
```

Para mais detalhes sobre os campos individuais e outros formatos que este parâmetro aceita, veja a descrição do parâmetro **ip** na página de manual **dracut.cmdline(7)**.

Os parâmetros **ipv6**, **netmask**, **gateway** e **hostname** não estão mais disponíveis no RHEL 8.

(BZ#1905138)

6.1.8. Kernel

Versão do Kernel em RHEL 8.3

O Red Hat Enterprise Linux 8.3 é distribuído com o kernel versão 4.18.0-240.

(BZ#1839151)

Filtro de Pacote Extendido Berkeley para RHEL 8.3

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 depois 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 8.3, os seguintes componentes **eBPF** são suportados:

- O pacote de ferramentas **BPF Compiler Collection (BCC)**, que fornece ferramentas para análise de E/S, redes 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.
- O recurso **eXpress Data Path (XDP)**, que fornece acesso aos pacotes recebidos antes que a pilha do kernel em rede os processe, é suportado sob condições específicas. Para mais detalhes, consulte a seção Rede das Notas de Relase.
- O pacote **libbpf**, que é crucial para aplicações relacionadas ao bpf como **bpftrace** e desenvolvimento **bpf**/**xdp**. Para mais detalhes, consulte a nota de lançamento dedicada à libbpf, totalmente suportada.
- O pacote **xdp-tools**, que contém utilitários de suporte de espaço do usuário para o recurso **XDP**, é agora suportado nas arquiteturas AMD e Intel 64-bit. Para obter mais detalhes, consulte a seção Rede das Notas de Lançamento.

Observe que 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 **bpftrace** tracing
- O soquete **AF_XDP** para conectar o caminho **eXpress Data Path (XDP)** ao espaço do usuário

Para mais informações sobre os componentes da Technology Previews, consulte Technology Previews.

(BZ#1780124)

Cornelis Networks Omni-Path Architecture (OPA) Host Software

O software hospedeiro Omni-Path Architecture (OPA) é totalmente suportado no Red Hat Enterprise Linux 8.3. 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 agrupado.

Para instruções sobre a instalação da arquitetura Omni-Path, consulte o arquivo Notas de versão do software Intel® Omni-Path Fabric.

(BZ#1893174)

TSX agora está desativado por padrão

A partir do RHEL 8.3, o kernel agora tem a tecnologia **Intel® Transactional Synchronization Extensions (TSX)** desativada por padrão para melhorar a segurança do sistema operacional. A mudança se aplica às CPUs que suportam a desativação **TSX**, incluindo os Processadores Escaláveis Intel® Xeon® de segunda geração (anteriormente conhecidos como Cascade Lake com chipsets Intel® C620 Series).

Para usuários cujas aplicações não utilizam **TSX**, a mudança remove a penalidade de desempenho padrão do **TSX Asynchronous Abort (TAA)** mitigações sobre os Processadores Escaláveis Intel® Xeon® de 2ª Geração.

A mudança também alinha o comportamento do kernel RHEL com o upstream, onde **TSX** foi desativado por padrão desde o Linux 5.4.

Para ativar **TSX**, adicione o parâmetro **tsx=on** à linha de comando do kernel.

(BZ#1828642)

RHEL 8.3 agora suporta o recurso de rastreamento do proprietário da página

Com esta atualização, você pode usar o recurso de rastreamento do proprietário da página para observar a utilização da memória do kernel no nível de alocação de página.

Para habilitar o rastreador de páginas, execute as seguintes etapas :

```
# grubby --args="page_owner=on" --update-kernel=0
# reboot
```

Como resultado, o rastreador do proprietário da página rastreará o consumo de memória do kernel, o que ajuda a depurar vazamentos de memória do kernel e a detectar os drivers que utilizam muita memória.

(BZ#1825414)

EDAC para AMD EPYC™ A série de processadores 7003 é agora suportada

Este aprimoramento fornece suporte a dispositivos de detecção e correção de erros (EDAC) para processadores da série AMD EPYC™ 7003. Anteriormente, erros de memória corrigidos (EC) e não corrigidos (UEs) não eram relatados nos sistemas baseados nos processadores da série AMD EPYC™ 7003. Com esta atualização, tais erros agora serão relatados usando EDAC.

(BZ#1735611)

Flamegraph é agora suportado com a ferramenta **perf**

Com esta atualização, a ferramenta de linha de comando **perf** suporta flamegraphs para criar uma representação gráfica do desempenho do sistema. Os dados do **perf** são agrupados em amostras com pilhas de retrocessos similares. Como resultado, estes dados são convertidos em uma representação visual para permitir uma identificação mais fácil de áreas de código computacionalmente intensivo. Para gerar um flamegraph usando a ferramenta **perf**, execute os seguintes comandos:

```
$ perf script record flamegraph -F 99 -g -- stress --cpu 1 --vm-bytes 128M --timeout 10s
stress: info: [4461] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
stress: info: [4461] successful run completed in 10s
[ perf record: Woken up 1 times to write data ]
[ perf record: Captured and wrote 0.060 MB perf.data (970 samples) ]
$ perf script report flamegraph
dumping data to flamegraph.html
```

Nota : Para gerar flamegrafos, instale o **js-d3-flame-graph** rpm.

(BZ#1281843)

/**dev**/**random** e /**dev**/**urandom** são agora condicionalmente alimentados pelo Kernel Crypto API DRBG

No modo FIPS, os geradores /**dev**/**random** e /**dev**/**urandom** pseudorandom number são alimentados pelo Kernel Crypto API Deterministic Random Bit Generator (DRBG). As aplicações em modo FIPS utilizam os dispositivos mencionados como fonte de ruído compatível com FIPS, portanto os dispositivos têm que empregar algoritmos aprovados por FIPS. Para atingir este objetivo, os ganchos necessários foram adicionados ao driver /**dev**/**random**. Como resultado, os ganchos são habilitados no modo FIPS e fazem com que /**dev**/**random** e /**dev**/**urandom** para se conectar ao Kernel Crypto API DRBG.

(BZ#1785660)

libbpf totalmente apoiada

O pacote **libbpf**, crucial para aplicações relacionadas ao bpf como **bpftrace** e desenvolvimento **bpf/xdp**, é agora totalmente suportado.

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 utilitárioIshw agora fornece informações adicionais da CPU

Com este aprimoramento, o utilitário Listar Hardware (*lshw*) exibe mais informações sobre a CPU. O campo **versão da** CPU agora fornece a família, modelo e detalhes passo a passo dos processadores do sistema em formato numérico como **versão**

(BZ#1794049)

kernel-rt árvore de origem foi atualizada para a árvore RHEL 8.3

As fontes do **kernel-rt** foram atualizadas para usar a mais recente árvore de fontes do kernel do Red Hat Enterprise Linux. O conjunto de correções em tempo real também foi atualizado para a última versão upstream, v5.6.14-rt7. Ambas as atualizações fornecem uma série de correções e melhorias de bugs.

(BZ#1818138, BZ#1818142)

tpm2-ferramentas rebaseadas para a versão 4.1.1

O pacote **tpm2-tools** foi atualizado para a versão 4.1.1, que fornece uma série de adições, atualizações e remoções de comandos. Para mais detalhes, veja o pacote Updates to tpm2-tools na solução RHEL8.3.

(BZ#1789682)

O adaptador de rede Mellanox ConnectX-6 Dx é agora totalmente suportado

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. Este recurso, anteriormente disponível como uma previsão tecnológica, agora é totalmente suportado no RHEL 8.3.

(BZ#1782831)

drivermlxsw rebaseado para a versão 5.7

O **driver mlxsw** é atualizado para a versão upstream 5.7 e inclui as seguintes novas características:

- O recurso de ocupação de buffer compartilhado, que fornece dados de ocupação de buffer.
- O recurso de queda de pacotes, que permite monitorar a **camada 2**, **camada 3**, **túneis** e queda da **lista de controle de acesso**.
- Apoio de policias de armadilhas de pacotes.
- Suporte à configuração de prioridade de porta padrão usando o agente Link Layer Discovery Protocol (LLDP).
- Seleção de Transmissão Aprimorada (ETS) e Filtro Token Bucket (TBF) disciplina de fila de apoio à descarga.

- O modo de enfileiramento **em** fila vermelha está habilitado para evitar quedas prematuras de pacotes.
- O recurso de prioridade de ação de edição de **skbedit** da classe de tráfego SKB permite a troca de metadados de pacotes e complementa com o TOS (**Pedit** Traffic Class Offloading).

(BZ#1821646)

6.1.9. Sistemas de arquivo e armazenamento

A LVM pode agora gerenciar volumes VDO

O LVM agora suporta o segmento Virtual Data Optimizer (VDO) tipo. Como resultado, agora você pode usar utilitários LVM para criar e gerenciar volumes VDO como volumes lógicos LVM nativos.

A VDO fornece recursos de desduplicação em bloco em linha, compressão e provisionamento fino.

Para mais informações, consulte Deduplicando e comprimindo volumes lógicos sobre a RHEL .

(BZ#1598199)

A pilha SCSI agora funciona melhor com adaptadores de alto desempenho

O desempenho da pilha SCSI foi melhorado. Como resultado, a próxima geração de adaptadores de ônibus host de alto desempenho (HBAs) são agora capazes de IOPS (I/Os por segundo) mais altos na RHEL.

(BZ#1761928)

O driver do megaraid_sas foi atualizado para a versão mais recente

O driver do **megaraid_sas** foi atualizado para a versão 07.713.01.00-rc1. Esta atualização fornece várias correções de erros e melhorias relacionadas à melhoria do desempenho, melhor estabilidade dos adaptadores MegaRAID suportados, e um conjunto de recursos mais rico.

(BZ#1791041)

Stratis agora lista o nome do pool em erro

Quando você tenta criar um pool Stratis em um dispositivo de bloco que já está em uso por um pool Stratis existente, o utilitário **Stratis** relata agora o nome do pool existente. Anteriormente, o utilitário listava apenas a etiqueta UUID do pool.

(BZ#1734496)

FPIN ELS suporte de notificação de quadros

O driver **lpfc** Fibre Channel (FC) agora suporta as Notificações de Impacto de Desempenho de Tecido (FPINs) relativas à integridade do link, que ajudam a identificar problemas no nível do link e permitem que o switch escolha um caminho mais confiável.

(BZ#1796565)

Novos comandos para depurar metadados LVM on-disk

O utilitário **pvck**, que está disponível no pacote **lvm2**, agora fornece comandos de baixo nível para depurar ou resgatar metadados LVM on-disk em volumes físicos:

- Para extrair metadados, use o comando **pvck --dump**.

- Para reparar metadados, use o comando **pvck --repair**.

Para mais informações, consulte a página de manual **pvck(8)**.

(BZ#1541165)

LVM RAID suporta integridade DM para evitar perda de dados devido a dados corrompidos em um dispositivo

Agora é possível adicionar a integridade do Device Mapper (DM) a uma configuração RAID LVM para evitar a perda de dados. A camada de integridade detecta a corrupção de dados em um dispositivo e alerta a camada RAID para corrigir os dados corrompidos através do RAID LVM.

Enquanto o RAID evita a perda de dados devido a falha do dispositivo, adicionar integridade a uma matriz RAID LVM evita a perda de dados devido a dados corrompidos em um dispositivo. Você pode adicionar a camada de integridade ao criar um novo RAID LVM, ou você pode adicioná-lo a um RAID LVM que já existe.

(JIRA:RHELPLAN-39320)

Armazenamento Resiliente (GFS2) apoiado em nuvens públicas AWS, Azure e Aliyun

O armazenamento resiliente (GFS2) é agora suportado em três grandes nuvens públicas, Amazon (AWS), Microsoft (Azure) e Alibaba (Aliyun) com a introdução do suporte de dispositivos de blocos compartilhados nessas plataformas. Como resultado, o GFS2 é agora um verdadeiro sistema híbrido de arquivos de cluster de nuvens com opções para uso tanto nas instalações quanto na nuvem pública. Para informações sobre a configuração de armazenamento em bloco compartilhado no Microsoft Azure e no AWS, veja Implementação do Red Hat Enterprise Linux 8 em plataformas de nuvem pública . Para informações sobre a configuração do armazenamento em bloco compartilhado no Alibaba Cloud, veja Configurando o Armazenamento em Bloco Compartilhado para um Cluster de Alta Disponibilidade da Red Hat no Alibaba Cloud.

(BZ#1900019)

O espaço do usuário agora suporta o mais recente daemon nfsdcld

O userspace agora suporta o último daemon **nfsdcld**, que é o único método de rastreamento de clientes com consciência de nome. Este aprimoramento garante a recuperação do cliente a partir do daemon **knfsd** de contêineres aberto ou bloqueado, sem qualquer corrupção de dados.

(BZ#1817756)

nconnect agora suporta múltiplas conexões simultâneas

Com este aperfeiçoamento, você pode usar a funcionalidade **nconnect** para criar várias conexões simultâneas a um servidor NFS, permitindo uma capacidade de balanceamento de carga diferente. Habilite a funcionalidade **nconnect** com a opção de montagem **nconnect=X** NFS, onde *X* é o número de conexões simultâneas a serem usadas. O limite de corrente é 16.

(BZ#1683394, BZ#1761352)

daemonnfsdcld para rastreamento de informações de clientes é agora suportado

Com este aprimoramento, o daemon **nfsdcld** é agora o método padrão no rastreamento de informações por cliente em um armazenamento estável. Como resultado, o NFS v4 executado em containers permite que os clientes recuperem as aberturas ou bloqueios após um reinício do servidor.

(BZ#1817752)

6.1.10. Alta disponibilidade e clusters

marca-passo rebaseado para a versão 2.0.4

O gerenciador de recursos de cluster Pacemaker foi atualizado para a versão 2.0.4, que fornece uma série de correções de bugs.

(BZ#1828488)

Nova propriedade de aglomerado de prioridade de atraso

O Pacemaker agora suporta a nova propriedade de cluster de **prioridade-depósito**, que permite configurar um cluster de dois nós para que, em uma situação de cérebro dividido, o nó com menos recursos funcionando seja o nó que é cercado.

A propriedade da **delimitação de prioridade** pode ser definida para uma duração de tempo. O valor padrão para esta propriedade é 0 (desabilitado). Se esta propriedade for definida para um valor diferente de zero, e o meta-atributo de **prioridade** for configurado para pelo menos um recurso, então em uma situação de cérebro dividido, o nó com a maior prioridade combinada de todos os recursos que correm sobre ele terá mais probabilidade de sobreviver.

Por exemplo, se você definir **pcs resource default priority=1** e **pcs property set priority-fencing-delay=15s** e nenhuma outra prioridade for definida, então o nó que estiver rodando mais recursos terá mais probabilidade de sobreviver porque o outro nó esperará 15 segundos antes de iniciar a esgrima. Se um determinado recurso é mais importante que o resto, você pode dar-lhe uma prioridade maior.

O nó que executa o papel principal de um clone promocional receberá um ponto extra se uma prioridade tiver sido configurada para aquele clone.

Qualquer atraso definido com o **atraso de cerca de prioridade** será adicionado a qualquer atraso da **pcmk_delay_base** e **pcmk_delay_max** propriedades do dispositivo de cerca. Este comportamento permite algum atraso quando ambos os nós têm prioridade igual, ou ambos os nós precisam ser cercados por algum outro motivo além da perda do nó (por exemplo, **on-fail=fencing** é definido para uma operação de monitoramento de recursos). Se usado em combinação, recomenda-se definir a propriedade **priority-fencing-delay** para um valor significativamente maior do que o atraso máximo de **pcmk_delay_base** e **pcmk_delay_max**, para ter certeza de que o nó priorizado é preferido (o dobro do valor seria completamente seguro).

(BZ#1784601)

Novos comandos para gerenciar múltiplos conjuntos de padrões de recursos e operações

Agora é possível criar, listar, alterar e excluir vários conjuntos de padrões de recursos e operações. Ao criar um conjunto de valores padrão, você pode especificar uma regra que contenha expressões de **recursos** e **operações**. Isto permite, por exemplo, configurar um valor padrão de recurso para todos os recursos de um determinado tipo. Os comandos que listam os valores padrão existentes agora incluem múltiplos conjuntos de valores padrão em sua saída.

- O **recurso pcs [op] conjunto de padrões de criação de** comando cria um novo conjunto de valores padrão. Ao especificar regras com este comando, somente expressões de **recurso** e **op**, incluindo **e**, **ou** e parênteses, são permitidas.
- O **recurso pcs [op] default set delete | remove** comando remove conjuntos de valores padrão.
- O comando de **atualização do conjunto de recursos pcs [op] padrão** muda os valores padrão em um conjunto.

(BZ#1817547)

Suporte para recursos de agrupamento de etiquetas

Agora é possível etiquetar recursos de cluster em um cluster Pacemaker com o comando **pcs tag**. Este recurso permite administrar um conjunto específico de recursos com um único comando. Você também pode usar o comando **pcs tag** para remover ou modificar uma tag de recurso e para exibir a configuração da tag.

Os comandos **pcs resource enable**, **pcs resource disable**, **pcs resource manage**, e **pcs resource unmanage** aceitam as tags IDs como argumentos.

(BZ#1684676)

Pacemaker agora apóia a recuperação através da desmobilização de um recurso promovido, em vez de pará-lo completamente

Agora é possível configurar um recurso promocional em um cluster Pacemaker para que quando uma ação de promoção ou monitoramento falhar para aquele recurso, ou a partição na qual o recurso está rodando perder quorum, o recurso será rebaixado mas não será totalmente interrompido.

Esta característica pode ser útil quando você prefere que o recurso continue disponível no modo não-promocionado. Por exemplo, se a partição de um banco de dados mestre perder quorum, você pode preferir que o recurso do banco de dados perca o papel de **mestre**, mas permaneça vivo no modo somente leitura para que aplicações que só precisam ler possam continuar a funcionar apesar do quorum perdido. Este recurso também pode ser útil quando uma desmobilização bem sucedida é suficiente para a recuperação e muito mais rápida do que um reinício completo.

Para apoiar esta característica:

- O meta-atributo da operação **em falta** agora aceita um valor **demoto** quando usado com ações de **promoção**, como no exemplo a seguir:

```
pcs resource op add my-rsc promote on-fail=\i>"demote\i
```

- O meta-atributo da operação **em falta** agora aceita um valor **demoto** quando usado com ações de **monitoramento** com **intervalo** definido para um valor diferente de zero e **papel** definido para **Mestre**, como no exemplo a seguir:

```
pcs resource op add my-rsc monitor interval===\"10s=\" on-fail===\"demote===\"Master==\"
```

- A propriedade de agrupamento **sem políticas de quorum** aceita agora um valor **demoto**. Quando definida, se uma partição de cluster perder quorum, quaisquer recursos promovidos serão despromovidos mas deixados em funcionamento e todos os outros recursos serão parados.

A especificação de um metaatributo **demoto** para uma operação não afeta como a promoção de um recurso é determinada. Se o nó afetado ainda tiver a maior pontuação de promoção, ele será selecionado para ser promovido novamente.

(BZ#1837747, BZ#1843079)

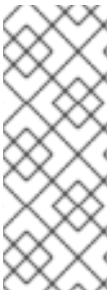
Novo parâmetro de configuração SBD_SYNC_RESOURCE_STARTUP SBD para melhorar a sincronização com Pacemaker

Para melhor controlar a sincronização entre SBD e Pacemaker, o arquivo **/etc/sysconfig/sbd** agora suporta o parâmetro **SBD_SYNC_RESOURCE_STARTUP**. Quando Pacemaker e pacotes SBD da

RHEL 8.3 ou posterior são instalados e SBD é configurado com **SBD_SYNC_RESOURCE_STARTUP=true**, a SBD entra em contato com o daemon Pacemaker para obter informações sobre o estado do daemon.

Nesta configuração, o daemon Pacemaker aguardará até ser contatado pela SBD, tanto antes de iniciar seus subdomínios quanto antes da saída final. Como resultado, o Pacemaker não executará recursos se a SBD não puder se comunicar ativamente com ele, e o Pacemaker não sairá até que ele tenha relatado um encerramento gracioso à SBD. Isto evita a situação improvável que pode ocorrer durante um desligamento gracioso quando a SBD não detecta o breve momento em que nenhum recurso está funcionando antes que o Pacemaker finalmente se desligue, o que desencadearia uma reinicialização desnecessária. A detecção de um desligamento gracioso usando um aperto de mão definido também funciona no modo de manutenção. O método anterior de detectar um desligamento gracioso com base na ausência de recursos em funcionamento tinha que ser desativado no modo de manutenção, uma vez que os recursos em funcionamento não seriam tocados no desligamento.

Além disso, a habilitação deste recurso evita o risco de uma situação de "split-brain" em um cluster quando SBD e Pacemaker começam ambos com sucesso, mas a SBD não consegue contatar o pacemaker. Isto poderia acontecer, por exemplo, devido às políticas da SELinux. Nesta situação, o marca-passo assumiria que a SBD está funcionando quando não está. Com este novo recurso habilitado, o Pacemaker não completará a inicialização até que a SBD entre em contato com ele. Outra vantagem deste novo recurso é que, quando ativado, a SBD entrará em contato com o Pacemaker repetidamente, usando um batimento cardíaco, e é capaz de entrar em pânico no nó se o Pacemaker parar de responder a qualquer momento.



NOTA

Se você editou seu arquivo /etc/sysconfig/sbd ou configurou a SBD através do PCS, então uma atualização RPM não irá puxar o novo parâmetro **SBD_SYNC_RESOURCE_STARTUP**. Nestes casos, para implementar este recurso você deve adicioná-lo manualmente a partir do arquivo **/etc/sysconfig/sbd.rpmnew** ou seguir o procedimento descrito na seção **Configuração via ambiente** da página de manual **sbd**(8).

(BZ#1718324, BZ#1743726)

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

Um novo fluxo de módulos: rubi:2.7

RHEL 8.3 introduz o Ruby 2.7.1 em um novo fluxo de módulo **Ruby:2.7**. Esta versão oferece uma série de melhorias de desempenho, correções de bugs e segurança e novas funcionalidades sobre o Ruby 2.6 distribuído com o RHEL 8.1.

As melhorias notáveis incluem:

- Foi introduzido um novo Coletor de Lixo Compactável (GC). Este GC pode desfragmentar um espaço de memória fragmentado.
- Ruby ainda Outro Compilador-Compilador (Racc) agora fornece uma interface de linha de comando para o Gerador de Parser de um-para-a-direita - LALR(1).
- O ambiente de leitura e avaliação de impressão (REPL) do Ruby Shell interativo**(irb**), agora suporta edição de várias linhas.
- A correspondência de padrões, freqüentemente utilizada em linguagens de programação funcional, foi introduzida como uma característica experimental.

- O parâmetro numerado como parâmetro de bloco padrão foi introduzido como uma característica experimental.

As seguintes melhorias de desempenho foram implementadas:

- A estratégia de cache de fibra foi alterada para acelerar a criação de fibra.
- O desempenho do método **CGI.escapeHTML** foi melhorado.
- O desempenho da classe **Monitor** e do módulo **MonitorMixin** foi melhorado.

Além disso, a conversão automática de argumentos de palavras-chave e argumentos posicionais foi depreciada. Na Ruby 3.0, os argumentos posicionais e os argumentos de palavras-chave serão separados. Para mais informações, consulte a documentação a montante .

Para suprimir avisos contra características experimentais, use a opção **-W:no-experimental** command line. Para desativar um aviso de depreciação, use a opção **-W:no-deprecated** da linha de comando ou adicione **Warning[:deprecated] = falso** ao seu código.

Para instalar o fluxo do módulo **rubi:2.7**, use:

```
#módulo yum instalar rubi:2.7
```

Se você quiser atualizar a partir do fluxo **rubi:2.6**, veja Mudando para um fluxo posterior .

(BZ#1817135)

Um novo fluxo de módulos: nodejs:14

Um novo fluxo de módulos, **nodejs:14**, está agora disponível. O **Node.js 14**, incluído no RHEL 8.3, oferece inúmeras novas características e correções de bugs e segurança sobre o **Node.js 12** distribuído no RHEL 8.1.

As mudanças notáveis incluem:

- O motor V8 foi atualizado para a versão 8.3.
- Foi implementada uma nova Interface de Sistema WebAssembly experimental (WASI).
- Um novo Async Local Storage API experimental foi introduzido.
- O recurso de relatório de diagnóstico agora é estável.
- Os APIs dos fluxos foram endurecidos.
- As advertências dos módulos experimentais foram removidas.

Com o lançamento da assessoria RHEA-2020:5101, a RHEL 8 fornece o **Node.js 14.15.0**, que é a versão mais recente do Suporte de Longo Prazo (LTS) com maior estabilidade.

Para instalar o fluxo de módulos **nodejs:14**, use:

```
# yum module install nodejs:14
```

Se você quiser atualizar a partir do fluxo **nodejs:12**, veja Mudando para um fluxo posterior .

(BZ#1815402, BZ#1891809)

git rebaseado para a versão 2.27

Os pacotes de **git** foram atualizados para a versão upstream 2.27. Mudanças notáveis em relação à versão 2.18, anteriormente disponível, incluem:

- O comando **git checkout** foi dividido em dois comandos separados:
  - **interruptor de git** para gerenciar filiais
  - **git restore** para gerenciar mudanças dentro da árvore de diretórios
- O comportamento do comando **git rebaseado** agora é baseado no fluxo de trabalho de **fusão** por padrão em vez do **patch** anterior **aplicar o** fluxo de trabalho. Para preservar o comportamento anterior, defina a variável de configuração **rebase.backend** a **ser aplicada**.
- O comando **git difftool** pode agora ser usado também fora de um repositório.
- Quatro novas variáveis de configuração, **{autor,committer}.{nome,e-mail}**, foram introduzidas para substituir o **usuário.{nome,e-mail}** em casos mais específicos.
- Várias novas opções foram adicionadas que permitem aos usuários configurar SSL para comunicação com proxies.
- O manuseio de commits com mensagens de registro em codificação de caracteres não-UTF-8 foi melhorado nas utilidades de **exportação rápida** e **importação rápida de git**.
- A extensão **lfs** foi adicionada como um novo pacote **git-lfs**. Git Large File Storage (LFS) substitui arquivos grandes por ponteiros de texto dentro do **Git** e armazena o conteúdo do arquivo em um servidor remoto.

(BZ#1825114, BZ#1783391)

Mudanças em Python

RHEL 8.3 introduz as seguintes mudanças no fluxo do módulo **python38:3.8**:

- O intérprete **Python** foi atualizado para a versão 3.8.3, que fornece várias correções de erros.
- O pacote **python38-pip** foi atualizado para a versão 19.3.1, e o **pip** agora suporta a instalação de rodas **manylinux2014**.

O desempenho do intérprete **Python 3.6**, fornecido pelos pacotes **python3**, foi significativamente melhorado.

As imagens dos recipientes **ubi8/python-27**, **ubi8/python-36** e **ubi8/python-38** agora suportam a instalação do utilitário **pipenv** a partir de um índice de pacotes personalizados ou de um espelho PyPI, se fornecido pelo cliente. Anteriormente, **o pipenv** só podia ser baixado a partir do repositório PyPI upstream, e se o repositório upstream não estivesse disponível, a instalação falhava.

(BZ#1847416, BZ#1724996, BZ#1827623, BZ#1841001)

Um novo fluxo de módulos: php:7.4

RHEL 8.3 apresenta o **PHP 7.4**, que fornece uma série de correções e melhorias sobre a versão 7.3.

Este lançamento introduz uma nova extensão experimental, Interface de Função Estrangeira (FFI), que permite chamar funções nativas, acessar variáveis nativas e criar e acessar estruturas de dados definidas em bibliotecas C. A extensão FFI está disponível no pacote **php-ffi**.

As seguintes extensões foram removidas:

- A extensão **wddx**, removida da embalagem **php-xml**
- A extensão da **recodificação**, removida do pacote **php-recode**.

Para instalar o fluxo do módulo **php:7.4**, use:

```
#módulo yum instalar php:7.4
```

Se você quiser atualizar do fluxo **php:7.3**, veja Mudando para um fluxo posterior .

Para detalhes sobre o uso do PHP no RHEL 8, veja Utilizando a linguagem PHP scripting.

(BZ#1797661)

Um novo fluxo de módulos: nginx:1.18

O servidor web e proxy **nginx 1.18**, que fornece uma série de correções de bugs, correções de segurança, novas características e melhorias em relação à versão 1.16, está agora disponível. As mudanças notáveis incluem:

- Melhorias na taxa de solicitação HTTP e limitação de conexão foram implementadas. Por exemplo, as diretrizes **limit_rate** e **limit_rate_after** agora suportam variáveis, incluindo novas variáveis **$limit_req_status** e **$limit_conn_status**. Além disso, foi adicionado o modo dry-run para as diretrizes **limit_conn_dry_run** e **limit_req_req_dry_run**.
- Uma nova diretiva **auth_delay** foi adicionada, o que permite o processamento atrasado de pedidos não autorizados.
- As seguintes diretrizes agora suportam variáveis: **grpc_pass**, **proxy_upload_rate**, e **proxy_download_rate**.
- Variáveis adicionais de protocolo PROXY foram adicionadas, nomeadamente **$proxy_protocol_server_addr** e **$proxy_protocol_server_port**.

Para instalar o fluxo **nginx:1.18**, use:

```
# yum instalar módulo nginx:1.18
```

Se você quiser atualizar do fluxo **nginx:1.16**, veja Mudando para um fluxo posterior .

(BZ#1826632)

Um novo fluxo de módulos: perl:5.30

A RHEL 8.3 apresenta o **Perl 5.30**, que fornece uma série de correções e melhorias em relação ao **Perl 5.26** lançado anteriormente. A nova versão também deprecia ou remove certas características do idioma. As mudanças notáveis com impacto significativo incluem:

- A **matemática::BigInt::CalcEmu**, **arybase**, e **B::Debug** módulos foram removidos
- Os descritores de arquivo são agora abertos com uma bandeira **close on-exec**
- Não é mais permitido abrir o mesmo símbolo que um arquivo e como um cabo de diretório
- Os atributos de sub-rotina agora devem preceder as assinaturas de sub-rotina

- Os atributos **:locked** e **:uniq** foram removidos
- Listas de variáveis sem vírgulas em formatos não são mais permitidas
- Não é mais permitido um operador de documentos aqui **<<**
- Certos usos, antes depreciados, de uma pulseira esquerda sem forma**({**) em padrões de expressão regular não são mais permitidos
- A sub-rotina **AUTOLOAD()** não pode mais ser herdada para funções não-método
- O pragma de **ordenação** não permite mais especificar um algoritmo de **ordenação**
- A sub-rotina **B::OP::terse()** foi substituída pela sub-rotina **B::Concise::b_terse()**
- A função **File::Glob::glob()** foi substituída pela função **File::Glob::bsd_glob()**
- A função **dump(**) agora deve ser invocada totalmente qualificada como **CORE::dump()**
- O operador yada-yada (**...**) é uma declaração agora, não pode ser usada como uma expressão
- A atribuição de um valor não zero à variável **$[** retorna agora um erro fatal
- As variáveis **$*** e **$#** não são mais permitidas
- Não é mais permitido declarar variáveis usando a função **my(**) em um ramo de falsa condição
- Usando as funções **sysread(**) e **syswrite()** nas alças **:utf8** agora retorna um erro fatal
- A função **pack()** não retorna mais o formato malformado UTF-8
- Pontos de código unicode com valor maior que **IV_MAX** não são mais permitidos
- O Unicode 12.1 é agora suportado

Para atualizar de um fluxo de módulo **perl** anterior, veja Mudando para um fluxo posterior .

Perl 5.30 também está disponível como uma imagem de recipiente s2i-enabled **ubi8/perl-530**.

(BZ#1713592, BZ#1732828)

Um novo fluxo de módulos: perl-libwww-perl:6.34

O RHEL 8.3 introduz um novo pacote de módulos **perl-libwww-perl:6.34**, que fornece o pacote **perl-libwww-perl** para todas as versões do **Perl** disponível no RHEL 8. O pacote não modular **perl-libwww-perl**, disponível desde o RHEL 8.0, que não pode ser usado com outros fluxos **Perl** além do 5.26, foi obsoleto pelo novo fluxo padrão **perl-libwwww-perl:6.34**.

(BZ#1781177)

Um novo fluxo de módulos: perl-IO-Socket-SSL:2.066

Um novo fluxo de módulos **perl-IO-Socket-SSL:2.066** está agora disponível. Este módulo fornece os pacotes **perl-IO-Socket-SSL** e **perl-Net-SSLeay** e é compatível com todos os fluxos **Perl** disponíveis no RHEL 8.

(BZ#1824222)

O fluxo do módulo squid:4 rebaseado para a versão 4.11

O servidor proxy **Squid**, fornecido pelo fluxo do módulo **squid:4**, foi atualizado da versão 4.4 para a versão 4.11. Este lançamento fornece vários bugs e correções de segurança, e várias melhorias, tais como novas opções de configuração.

(BZ#1829467)

Mudanças no fluxo do módulo httpd:2.4

RHEL 8.3 introduz as seguintes mudanças notáveis no Servidor HTTP Apache, disponível através do fluxo do módulo **httpd:2.4**:

- O módulo **mod_http2** rebaseado para a versão 1.15.7
- Mudanças de configuração nas diretrizes **H2Upgrade** e **H2Push**
- Uma nova diretiva de configuração do **H2Padding** para controlar o estofamento dos quadros de carga útil do HTTP/2
- Numerosas correções de erros.

(BZ#1814236)

Apoio para o registro em diário da diretiva CustomLog em httpd

Agora é possível emitir logs de acesso (transferência) para o **journald** a partir do Servidor HTTP Apache usando uma nova opção para a diretiva **CustomLog**.

A sintaxe suportada é a seguinte:

```
CustomLog journald:formato prioritário|nickname
```

onde *priority* é qualquer cadeia de prioridade até o **debug** como usado na diretiva**LogLevel**.

Por exemplo, para fazer o log to **journald** usando o formato de log **combinado**, use:

```
CustomLog journald:info combinado
```

Observe que, ao utilizar esta opção, o desempenho do servidor pode ser menor do que ao efetuar logon diretamente em arquivos planos.

(BZ#1209162)

6.1.12. Compiladores e ferramentas de desenvolvimento

Novo conjunto de ferramentas GCC 10

O GCC Toolset 10 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**.

O compilador GCC foi atualizado para a versão 10.2.1, que fornece muitas correções e melhorias de bugs que estão disponíveis no GCC upstream.

As seguintes ferramentas e versões são fornecidas pelo GCC Toolset 10:

Ferramenta	Versão
GCC	10.2.1
GDB	9.2
Valgrind	3.16.0
SystemTap	4.3
Dyninst	10.1.0
binutils	2.35
elfutils	0.180
dwz	0.12
fazer	4.2.1
strace	5.7
ltrace	0.7.91
annobin	9.29

Para instalar o GCC Toolset 10, execute o seguinte comando como raiz:

```
# yum instalar gcc-toolset-10
```

Para executar uma ferramenta do GCC Toolset 10:

```
$ scl habilita gcc-toolset-10 tool
```

Para executar uma sessão shell onde as versões de ferramentas do GCC Toolset 10 substituem as versões do sistema dessas ferramentas:

```
$ scl habilita gcc-toolset-10 bash
```

Para mais informações, consulte Utilizando o GCC Toolset.

Os componentes do GCC Toolset 10 estão disponíveis nas duas imagens do contêiner:

- **rhel8/gcc-toolset-10-toolchain**, que inclui o compilador GCC, o depurador GDB, e a ferramenta de automação **make**.
- **rhel8/gcc-toolset-10-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/
```

Observe que agora somente as imagens dos recipientes do GCC Toolset 10 são suportadas. As imagens de contêineres das versões anteriores do GCC Toolset são depreciadas.

Para detalhes sobre as imagens dos contêineres, veja Utilizando as imagens dos contêineres do GCC Toolset.

(BZ#1842656)

Rust Toolset rebaseado para a versão 1.45.2

O Rust Toolset foi atualizado para a versão 1.45.2. As mudanças notáveis incluem:

- A **árvore de carga** de subcomandos para visualizar as dependências está agora incluída na **carga**.
- A fundição de valores de ponto flutuante a inteiros produz agora um molde de fixação. Anteriormente, quando um valor de ponto flutuante truncado estava fora do intervalo para o tipo inteiro alvo, o resultado era um comportamento indefinido do compilador. Valores de ponto flutuante não finitos levavam também a um comportamento indefinido. Com este aprimoramento, os valores finitos são fixados no intervalo mínimo ou máximo do número inteiro. Valores infinitos positivos e negativos são, por padrão, fixados ao número inteiro máximo e mínimo respectivamente, valores Not-a-Number(NaN) a zero.
- As macros de procedimentos funcionais em expressões, padrões e declarações são agora estendidas e estabilizadas.

Para instruções detalhadas sobre o uso, consulte Utilização do conjunto de ferramentas enferrujadas .

(BZ#1820593)

LLVM Toolset rebaseado para a versão 10.0.1

O conjunto de ferramentas LLVM foi atualizado para a versão 10.0.1. Com esta atualização, os pacotes **de clang-libs** não incluem mais bibliotecas de componentes individuais. Como resultado, não é mais possível vincular aplicações contra elas. Para vincular aplicações contra as bibliotecas de **clang**, use o pacote **libclang-cpp.so**.

Para mais informações, consulte Utilizando o conjunto de ferramentas LLVM .

(BZ#1820587)

Go Toolset rebaseado para a versão 1.14.7

O Go Toolset foi atualizado para a versão 1.14.7 As mudanças notáveis incluem:

- O sistema de módulos Go é agora totalmente suportado.
- O SSL versão 3.0 (SSLv3) não é mais suportado. Entre as melhorias notáveis do Delve debugger estão
- O novo **examinemem de** comando (ou **x**) para examinar a memória bruta
- O novo **display de** comando para impressão dos valores de uma expressão durante cada parada do programa

- A nova bandeira **--tty** para o fornecimento de um Teletypewriter (TTY) para o programa de depuração
- O novo suporte de coredump para Arm64
- A nova capacidade de imprimir etiquetas de gorotina
- O lançamento do servidor do Debug Adapter Protocol (DAP)
- A saída melhorada dos comandos **dlv trace** and **trace** REPL (read-eval-print-loop)

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#1820596)

SystemTap rebaseado para a versão 4.3

A ferramenta de instrumentação SystemTap foi atualizada para a versão 4.3, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- As sondas de espaço do usuário podem ser direcionadas pelo **buildid** hexadecimal a partir do **readelf -n**. Esta alternativa a um nome de caminho permite que os binários correspondentes sejam sondados sob qualquer nome, e assim permite que um único script seja direcionado a uma gama de versões diferentes. Esta característica funciona bem em conjunto com o servidor elfutils **debuginfod**.
- As funções de script podem usar variáveis de **texto de** sonda **$** para acessar variáveis no local sondado, o que permite que os scripts SystemTap utilizem lógica comum para trabalhar com uma variedade de sondas.
- As melhorias do programa **stapbpf**, incluindo declarações de tentativa de captura e sondas de erro, foram feitas para permitir uma tolerância de erro adequada nos scripts executados no backend do BPF.

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

(BZ#1804319)

Valgrind rebaseado para a versão 3.16.0

A ferramenta de análise de código executável Valgrind foi atualizada para a versão 3.16.0, que fornece uma série de correções e melhorias de bugs em relação à versão anterior:

- Agora é possível mudar dinamicamente o valor de muitas opções de linha de comando enquanto seu programa está sendo executado sob a Valgrind: através do **vgdb**, através de um **gdb** conectado ao Valgrind gdbserver, ou através de solicitações de clientes do programa. Para obter uma lista de opções dinamicamente modificáveis, execute o comando **valgrind --help-dyn-options**.
- Para as ferramentas Cachegrind(**cg_annotate**) e Callgrind(**callgrind_annotate**), as opções **--auto** e **--show-percs** agora são padrão para **sim**.
- A ferramenta Memcheck produz menos erros falsos positivos em código otimizado. Em particular, o Memcheck agora lida melhor com o caso quando o compilador transformou um código **A**

- A pilha experimental e a ferramenta Global Array Checking(**exp-sgcheck**) foi removida. Uma alternativa para detectar a pilha e os overruns da matriz global é usar a ferramenta AddressSanitizer (ASAN) do GCC, que requer que você reconstrua seu código com a opção **-fsanitize=address**.

(BZ#1804324)

elfutils rebobinado para a versão 0.180

O pacote **elfutils** foi atualizado para a versão 0.180, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Melhor suporte para informações de depuração para código construído com o GCC LTO (link time optimization). Os utilitários **eu-readelf** e **libdw** agora podem ler e manipular seções **.gnu.debuglto_**, e resolver corretamente nomes de arquivos para funções que são definidas em CUs (compilar unidades).

- A utilidade **eu-nm** agora identifica explicitamente os objetos fracos como **V** e os símbolos comuns como **C**.

- O servidor **de debuginfod** agora pode indexar arquivos **.deb** e tem uma extensão genérica para adicionar outros formatos de arquivo de pacotes usando a opção **-Z EXT[=CMD]**. Por exemplo **-Z '.tar.zst=zstdcat'** indica que arquivos terminados com a extensão **.tar.zst** devem ser desempacotados usando o utilitário **zstdcat**.

- A ferramenta **debuginfo-cliente** tem várias novas funções de ajuda, tais como **debuginfod_set_user_data**, **debuginfod_get_user_data**, **debuginfod_get_url** e **debuginfod_add_http_header**. Ele também suporta **arquivos:**// URLs agora.

(BZ#1804321)

GDB agora suporta registro e replay de processos na IBM z15

Com este aperfeiçoamento, o GNU Debugger (GDB) agora suporta registro e replay de processos com a maioria das novas instruções do processador IBM z15 (anteriormente conhecido como arch13). Observe que as seguintes instruções não são atualmente suportadas: SORTL (listas de classificação), DFLTCC (chamada de conversão deflacionada), KDSA (autenticação de assinatura digital computada).

(BZ#1659535)

Os eventos de monitoramento de desempenho Marvell ThunderX2 foram atualizados em papi

Com este aprimoramento, vários eventos de desempenho específicos do ThunderX2, incluindo eventos sem núcleo, foram atualizados. Como resultado, os desenvolvedores podem investigar melhor o desempenho do sistema nos sistemas Marvell ThunderX2.

(BZ#1726070)

A biblioteca de matemática glibc está agora otimizada para IBM Z

Com este aperfeiçoamento, as funções de matemática **libm** foram otimizadas para melhorar o desempenho das máquinas IBM Z. As mudanças notáveis incluem:

- manuseio melhorado do modo de arredondamento para evitar conjuntos de registros e extratos supérfluos de controle de ponto flutuante

- exploração da conversão entre o z196 inteiro e a bóia

(BZ#1780204)

Um diretório temporário adicional específico da libffi está disponível agora

Anteriormente em sistemas endurecidos, os diretórios temporários de todo o sistema podem não ter tido permissões adequadas para uso com a biblioteca **libffi**.

Com este aperfeiçoamento, os administradores do sistema podem agora definir a variável de ambiente **LIBFFI_TMPDIR** para apontar para um diretório temporário específico da libffi com permissões de montagem de **escrita** e **execução** ou selinux.

(BZ#1723951)

Melhor desempenho de strstr() e strcasestr()

Com esta atualização, o desempenho das funções **strstr(**) e **strcasestr()** foi melhorado em várias arquiteturas suportadas. Como resultado, os usuários agora se beneficiam de um desempenho significativamente melhor de todas as aplicações usando rotinas de manipulação de strstr() e memória.

(BZ#1821531)

glibc agora lida corretamente com o carregamento de um arquivo de locale truncado

Se o arquivo de locais do sistema tiver sido previamente truncado, seja devido a uma queda de energia durante a atualização ou uma falha de disco, um processo poderia terminar inesperadamente ao carregar o arquivo. Esta melhoria acrescenta verificações adicionais de consistência ao carregamento do arquivo de locale. Como resultado, os processos agora são capazes de detectar o truncamento do arquivo e cair de volta aos locales instalados não arquivados ou ao locale POSIX padrão.

(BZ#1784525)

A GDB agora suporta debuginfod

Com esta melhoria, o GNU Debugger (GDB) pode agora baixar pacotes de informações de depuração a partir de servidores centralizados sob demanda usando a biblioteca cliente elfutils **debuginfod**.

(BZ#1838777)

pcp rebaseado para a versão 5.1.1-3

O pacote **pcp** foi atualizado para a versão 5.1.1-3. Mudanças notáveis incluem:

- Unidades de serviço atualizadas e melhor integração e confiabilidade **do sistema** para todos os serviços de PCP. Melhor rotação de registros de arquivo e compressão mais oportuna. Correções de bugs de descoberta arquivados no protocolo **pmproxy**.
- Melhorias no **pcp-atop**, **pcp-dstat**, **pmrep**, e ferramentas de monitoramento relacionadas, juntamente com relatórios de etiquetas métricas nas ferramentas de **pmrep** e exportação.
- Melhoria da **bpftrace**, **OpenMetrics**, MMV, o agente do kernel Linux e outros agentes de coleta. Novos coletores métricos para os servidores **Open vSwitch** e **RabbitMQ**.
- Novo serviço **pmfind systemd de** descoberta de anfitriões, que substitui o daemon **pmmgr** autônomo.

(BZ#1792971)

grafana rebaseada para a versão 6.7.3

O pacote **grafana** foi atualizado para a versão 6.7.3. Mudanças notáveis incluem:

- Suporte genérico de mapeamento de papéis **OAuth**
- Um novo painel de troncos
- Exibição de texto com várias linhas no painel da mesa
- Uma nova moeda e unidades de energia

(BZ#1807323)

grafana-pcp rebaseado para a versão 2.0.2

O pacote **grafana-pcp** foi atualizado para a versão 2.0.2. Mudanças notáveis incluem:

- Suporta os mapas multidimensionais do **eBPF** a serem grafados no flamegraph.
- Remove um cache de auto-completamento no editor de consultas, para que as métricas de PCP possam aparecer dinamicamente.

(BZ#1807099)

Uma nova imagem do contêiner rhel8/pcp

A imagem do contêiner **rhel8/pcp** está agora disponível no Red Hat Container Registry. A imagem contém o conjunto de ferramentas Performance Co-Pilot (PCP), que inclui o pacote **pcp-zeroconf** pré-instalado e o PMDA da **OpenMetrics**.

(BZ#1497296)

Uma nova imagem do recipiente rhel8/grafana

A imagem do recipiente **rhel8/grafana** está agora disponível no Red Hat Container Registry. Grafana é um utilitário de código aberto com painel de métricas e editor gráfico para a ferramenta de monitoramento **Graphite**, **Elasticsearch**, **OpenTSDB**, **Prometheus**, **InfluxDB** e **PCP**.

(BZ#1823834)

6.1.13. Gestão da Identidade

O utilitário de backup IdM agora verifica as réplicas de funções necessárias

O utilitário **ipa-backup** agora verifica se todos os serviços usados no cluster IdM, tais como Autoridade Certificadora (CA), Sistema de Nomes de Domínio (DNS) e Agente de Recuperação de Chaves (KRA) estão instalados na réplica onde você está executando o backup. Se a réplica não tiver todos estes serviços instalados, o utilitário **ipa-backup** sai com um aviso, pois os backups realizados naquele host não seriam suficientes para uma restauração completa do cluster.

Por exemplo, se sua implantação de IdM usa uma Autoridade Certificadora (CA) integrada, uma execução de backup em uma réplica não-CA não capturará os dados da CA. A Red Hat recomenda verificar se a réplica onde você realiza um **ipa-backup** tem todos os serviços de IdM utilizados no cluster instalados.

Para mais informações, consulte Preparação para perda de dados com backups IdM .

(BZ#1810154)

Nova ferramenta de notificação de expiração de senha

Notificação de Senha Expirando (EPN), fornecida pelo pacote **ipa-client-epn**, é uma ferramenta independente que você pode usar para construir uma lista de usuários de Gerenciamento de Identidade (IdM) cujas senhas estão expirando em breve.

Os administradores da IdM podem usar EPN para:

- Exibir uma lista de usuários afetados no formato JSON, que é calculada em tempo de execução
- Calcule quantos e-mails serão enviados para um determinado dia ou intervalo de datas
- Enviar notificações de expiração de senha por e-mail aos usuários

A Red Hat recomenda lançar o EPN uma vez por dia de um cliente IdM ou uma réplica com o timer **do sistema ipa-epn.timer** incluído.

(BZ#913799)

JSS agora fornece um SSLContext compatível com FIPS

Anteriormente, Tomcat utilizava a diretiva SSLEngine da classe SSLContext da Java Cryptography Architecture (JCA). A implementação padrão do SunJSSE não está em conformidade com o Federal Information Processing Standard (FIPS), portanto o PKI agora fornece uma implementação em conformidade com o FIPS via JSS.

(BZ#1821851)

Verificar a saúde geral de sua infra-estrutura de chave pública está agora disponível

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#1770322)

Apoio ao PSS da RSA

Com este aprimoramento, PKI agora suporta o algoritmo de assinatura RSA PSS (Probabilistic Signature Scheme).

Para ativar este recurso, defina a seguinte linha no arquivo **pkispawn** script para um determinado subsistema: **pki_use_pss_rsa_signing_algorithm=True**

Como resultado, todos os algoritmos de assinatura padrão existentes para este subsistema (especificados em seu arquivo de configuração **CS.cfg**) usarão a versão PSS correspondente. Por exemplo, **SHA256withRSA** torna-se **SHA256withRSA/PSS**

(BZ#1824948)

O Directory Server exporta a chave privada e o certificado para um espaço de nome privado quando o serviço é iniciado

O servidor de diretório usa bibliotecas OpenLDAP para conexões de saída, tais como acordos de replicação. Como essas bibliotecas não podem acessar diretamente o banco de dados de serviços de segurança de rede (NSS), o Servidor de Diretório extrai a chave privada e os certificados do banco de dados NSS em instâncias com suporte à criptografia TLS para permitir que as bibliotecas OpenLDAP estabeleçam conexões criptografadas. Anteriormente, o Servidor de Diretório extraía a chave privada e os certificados para o diretório definido no parâmetro **nsslapd-certdir** na entrada **cn=config** (padrão: **/etc/dirsrv/slapd-**

(BZ#1638875)

O Servidor de Diretório pode agora passar uma instância para o modo somente leitura se o limite de monitoramento de disco for atingido

Esta atualização adiciona o parâmetro **nsslapd-disk-monitoring-read-on-threshold apenas** à entrada **cn=config**. Se você ativar esta configuração, o Servidor de Diretório muda todos os bancos de dados para somente leitura se o monitoramento em disco estiver ativado e o espaço livre em disco for inferior ao valor configurado no **nsslapd-disk-monitoring-threshold**. Com o **nsslapd-disk-monitoring-somente-leitura-leitura-e-limite** configurado em **on**, os bancos de dados não podem ser modificados até que o Servidor de Diretório desligue a instância com sucesso. Isto pode impedir a corrupção dos dados.

(BZ#1728943)

samba rebaseado para a versão 4.12.3

Os pacotes *samba* foram atualizados para a versão 4.12.3, que fornece uma série de correções e melhorias em relação à versão anterior:

- As funções de criptografia incorporadas foram substituídas pelas funções GnuTLS. Isto melhora significativamente o desempenho do bloco de mensagens do servidor versão 3 (SMB3) e a velocidade de cópia.
- O suporte mínimo de tempo de execução é agora Python 3.5.
- O parâmetro de **tamanho do cache de gravação** foi removido porque o conceito anterior de cache de gravação poderia reduzir o desempenho em sistemas com limitações de memória.
- O suporte para autenticação de conexões usando bilhetes Kerberos com tipos de criptografia DES foi removido.
- O módulo **vfs_netatalk** sistema de arquivo virtual (VFS) foi removido.
- O parâmetro **dos anúncios ldap ssl** é marcado como depreciado e será removido em uma futura versão Samba. Para informações sobre como, alternativamente, codificar o tráfego LDAP e outros detalhes, consulte a solução samba: remoção da opção smb.conf "ldap ssl ads ".
- Por padrão, o Samba no RHEL 8.3 não suporta mais o conjunto de cifras RC4 depreciado. Se você executar Samba como membro de domínio em um AD que ainda requer autenticação RC4 para Kerberos, use o comando **update-crypto-policies --set DEFAULT:AD-SUPPORT** para habilitar o suporte ao tipo de criptografia RC4.

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

(BZ#1817557)

cockpit-session-recording rebaseado para a versão 4

O módulo de **gravação de sessão do cockpit** foi rebaseado para a versão 4. Esta versão prevê as seguintes mudanças notáveis em relação à versão anterior:

- Identificação dos pais atualizada no arquivo **metainfo**.
- Manifesto de pacote atualizado.
- **Rpmmacro** fixo para resolver o caminho correto no CentOS7.
- Manuseio de dados de diário codificados por byte-array.
- Código movido das funções do ciclo de vida de reações depreciadas.

(BZ#1826516)

krb5 rebaseado para a versão 1.18.2

Os pacotes **krb5** foram atualizados para a versão upstream 1.18.2. Correções e melhorias notáveis incluem:

- Os tipos de criptografia de um e três DES foram removidos.
- O rascunho 9 PKINIT foi removido, pois não é necessário para nenhuma das versões suportadas do Active Directory.
- Os plug-ins do mecanismo NegoEx agora são suportados.
- A canonicalização do nome do hospedeiro fallback é agora suportada**(dns_canonicalize_hostname = fallback**).

(BZ#1802334)

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 de **configuração** permite definir parâmetros de configuração global dentro do IdM.
- O módulo **dnsconfig** permite modificar a configuração global do DNS.
- O módulo **dnsforwardzone** permite adicionar e remover encaminhadores DNS da IdM.
- O **dnsrecord** permite o gerenciamento dos registros DNS. Ao contrário do **ipa_dnsrecord** a montante, ele permite o gerenciamento de vários registros em uma única execução, e suporta mais tipos de registros.
- O módulo **dnszone** permite a configuração de zonas no servidor DNS.
- O módulo de **serviço** permite garantir a presença e ausência de serviços.

- O módulo de **abóbada** permite garantir a presença e ausência de abóbadas e dos membros das abóbadas.

Observe que os módulos **ipagroup** e **ipahostgroup** foram ampliados para incluir os gerentes de membros do usuário e do grupo anfitrião, respectivamente. Um gerente de grupo de membros é um usuário ou um grupo que pode adicionar membros a um grupo ou remover membros de um grupo. Para mais informações, consulte as seções **Variáveis** dos respectivos arquivos **/usr/share/doc/doc/ansible-freeipa/README-***.

(JIRA:RHELPLAN-49954)

IdM agora apóia um novo papel do sistema Ansible para gerenciamento de certificados

O Gerenciamento de Identidade (IdM) apóia uma nova função do sistema Ansible para automatizar tarefas de gerenciamento de certificados. O novo papel inclui os seguintes benefícios:

- O papel ajuda a automatizar a emissão e renovação de certificados.
- O papel pode ser configurado para que a autoridade certificadora **ipa** emita seus certificados. Desta forma, você pode usar sua infraestrutura IdM existente para gerenciar a cadeia de confiança dos certificados.
- A função permite especificar os comandos a serem executados antes e após a emissão de um certificado, por exemplo, a parada e o início dos serviços.

(JIRA:RHELPLAN-50002)

A Gestão da Identidade agora apóia o FIPS

Com este aperfeiçoamento, agora é possível utilizar tipos de criptografia que são aprovados pelo Federal Information Processing Standard (FIPS) com os mecanismos de autenticação no Gerenciamento de Identidade (IdM). Observe que uma confiança cruzada entre o IdM e o Active Directory não é compatível com o FIPS.

Os clientes que requerem FIPS mas não requerem um AD trust podem agora instalar o IdM no modo FIPS.

(JIRA:RHELPLAN-43531)

OpenDNSSEC em idm:DL1 rebaseado para a versão 2.1

O componente OpenDNSSEC do fluxo do módulo **idm:DL1** foi atualizado para a série 2.1, que é a versão atual de longo prazo de suporte upstream. O OpenDNSSEC é um projeto de código aberto que impulsiona a adoção de Extensões de Segurança de Sistema de Nomes de Domínio (DNSSEC) para aumentar ainda mais a segurança na Internet. OpenDNSSEC 2.1 fornece uma série de correções e melhorias de bugs em relação à versão anterior. Para mais informações, leia as notas de lançamento a montante: https://www.opendnssec.org/archive/releases/

(JIRA:RHELPLAN-48838)

IdM agora suporta o desvalorizado conjunto de cifras RC4 com uma nova subpolítica criptográfica de todo o sistema

Esta atualização introduz a nova subpolítica criptográfica **AD-SUPPORT** que permite o conjunto de cifras Rivest Cipher 4 (RC4) em Gerenciamento de Identidade (IdM).

Como administrador no contexto dos trusts cross-forest do IdM-Active Directory (AD), você pode ativar a nova subpolítica **AD-SUPPORT** quando o AD não estiver configurado para usar o Advanced Encryption Standard (AES). Mais especificamente, a Red Hat recomenda ativar a nova subpolítica se

uma das seguintes condições se aplicar:

- As contas de usuário ou serviço no AD possuem chaves de criptografia RC4 e não possuem chaves de criptografia AES.
- Os links de confiança entre domínios individuais do Active Directory possuem chaves de criptografia RC4 e não possuem chaves de criptografia AES.

Para ativar a subpolítica **AD-SUPPORT** além da política de criptografia **DEFAULT**, entre:

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

Alternativamente, para atualizar os trusts entre domínios AD em uma floresta AD para que eles suportem tipos fortes de criptografia AES, veja o seguinte artigo da Microsoft: AD DS: Segurança: Erro de tipo "Unsupported etype" ao acessar um recurso em um domínio confiável.

(BZ#1851139)

Ajuste aos novos requisitos de encadernação de canais LDAP da Microsoft e assinatura de LDAP

Com atualizações recentes da Microsoft, o Active Directory (AD) sinaliza os clientes que não utilizam as configurações padrão do Windows para encadernação de canais LDAP e assinatura LDAP. Como conseqüência, os sistemas RHEL que utilizam o Daemon System Security Services (SSSD) para integração direta ou indireta com o AD podem acionar IDs de eventos de erro no AD após operações bem sucedidas de Autenticação Simples e Camada de Segurança (SASL) que utilizam a Interface do Programa de Aplicação de Serviços Genéricos de Segurança (GSSAPI).

Para evitar estas notificações, configure as aplicações do cliente para usar o mecanismo SASL do Mecanismo de Negociação Simples e Protegido GSSAPI (GSS-SPNEGO) em vez do GSSAPI. Para configurar o SSSD, defina a opção **ldap_sasl_mech** para **GSS-SPNEGO**.

Além disso, se a encadernação de canais for aplicada no lado AD, configure quaisquer sistemas que utilizem SASL com SSL/TLS da seguinte maneira:

1. Instale as últimas versões dos pacotes **cyrus-sasl**, **openldap** e **krb5-libs** que são enviados com o RHEL 8.3 e posteriores.
2. No arquivo **/etc/openldap/ldap.conf**, especifique o tipo correto de encadernação do canal definindo a opção **SASL_CBINDING** para **tls-endpoint**.

Para mais informações, consulte Impacto da Consultoria de Segurança da Microsoft ADV190023 | LDAP Channel Binding e LDAP Signing on RHEL and AD integration.

(BZ#1873567)

SSSD, adcli e realmd agora suportam o desvalorizado conjunto de cifras RC4 com uma nova subpolítica criptográfica de todo o sistema

Esta atualização introduz a nova subpolítica criptográfica **AD-SUPPORT** que permite o conjunto de cifras Rivest Cipher 4 (RC4) para as seguintes utilidades:

- o Serviço de Segurança do Sistema Daemon (SSSD)
- **adcli**
- **reinod**

Como administrador, você pode ativar a nova subpolítica **AD-SUPPORT** quando o Active Directory (AD) não estiver configurado para usar o Advanced Encryption Standard (AES) nos seguintes cenários:

- O SSSD é usado em um sistema RHEL conectado diretamente ao AD.
- **adcli** é usado para entrar em um domínio AD ou para atualizar atributos do host, por exemplo, a chave do host.
- **realmd** é usado para ingressar em um domínio AD.

A Red Hat recomenda a habilitação da nova subpolítica se uma das seguintes condições se aplicar:

- As contas de usuário ou serviço no AD possuem chaves de criptografia RC4 e não possuem chaves de criptografia AES.
- Os links de confiança entre domínios individuais do Active Directory possuem chaves de criptografia RC4 e não possuem chaves de criptografia AES.

Para ativar a subpolítica **AD-SUPPORT** além da política de criptografia **DEFAULT**, entre:

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

(BZ#1866695)

authselect tem um novo perfil mínimo

O utilitário **authselect** tem um novo perfil **mínimo**. Você pode usar este perfil para atender apenas usuários e grupos locais diretamente dos arquivos do sistema, em vez de usar outros provedores de autenticação. Portanto, você pode remover com segurança os pacotes **SSSD**, **winbind** e **fprintd** e pode usar este perfil em sistemas que requerem instalação mínima para economizar espaço em disco e memória.

(BZ#1654018)

O SSSD agora atualiza o arquivo Samba's secrets.tdb ao girar uma senha

Uma nova opção **ad_update_samba_machine_account_password** no arquivo **sssd.conf** está agora disponível em RHEL. Você pode usá-lo para configurar o SSSD para atualizar automaticamente o arquivo Samba **secrets.tdb** ao girar a senha de domínio de uma máquina enquanto usa o Samba.

Entretanto, se o SELinux estiver em modo de aplicação, o SSSD não atualiza o arquivo **secrets.tdb**. Consequentemente, o Samba não tem acesso à nova senha. Para contornar este problema, configure o SELinux para o modo permissivo.

(BZ#1793727)

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/sssd/sssd.conf** para **permissivo**.

(JIRA:RHELPLAN-51289)

O Servidor de Diretório agora suporta o atributo de operação pwdReset

Esta melhoria adiciona suporte ao atributo de operação **pwdReset** ao Directory Server. Quando um administrador muda a senha de um usuário, o Servidor de Diretório define o **pwdReset** na entrada do usuário como **verdadeiro**. Como resultado, os aplicativos podem usar este atributo para identificar se a senha de um usuário foi redefinida por um administrador.

Note que **pwdReset** é um atributo operacional e, portanto, os usuários não podem editá-lo.

(BZ#1775285)

O servidor de diretório agora registra o trabalho e o tempo de operação em entradas de RESULTADO

Com esta atualização, o Directory Server agora registra dois valores de tempo adicionais em **RESULTADOS `/var/log/dirsrv/slapd-**

- O valor **do tempo de trabalho** indica quanto tempo levou para que uma operação passasse da fila de trabalho para uma linha de operários.
- O valor do **tempo de operação** mostra o tempo que a operação real levou para ser concluída uma vez que um fio operário iniciou a operação.

Os novos valores fornecem informações adicionais sobre como o Servidor de Diretório trata as operações de carga e processamento.

Para mais detalhes, veja a seção Referência do Log de Acesso na Configuração, Comando e Referência do Servidor de Diretório da Red Hat.

(BZ#1850275)

6.1.14. Desktop

Sessão de aplicação única agora está disponível

Agora você pode iniciar o GNOME em uma sessão de uma única aplicação, também conhecida como modo quiosque. Nesta sessão, o GNOME exibe apenas uma janela de tela cheia de uma aplicação que você configurou.

Para habilitar a sessão de aplicação única:

1. Instalar o pacote **gnome-session-kiosk-session**:

   ```
   # yum instalar gnome-session-kiosk-session
   ```

2. Criar e editar o arquivo **$HOME/.local/bin/redhat-kiosk** do usuário que abrirá a sessão de aplicação única.
   No arquivo, digite o nome executável do aplicativo que você deseja lançar.

   Por exemplo, para lançar o aplicativo **Text Editor**:

   ```
   #!/bin/sh

   gedit &
   ```

3. Tornar o arquivo executável:

```
$ chmod x $HOME/.local/bin/redhat-kiosk
```

4. Na tela de login do GNOME, selecione a sessão **Kiosk** no menu de botões da roda dentada e faça o login como usuário de uma única aplicação.

(BZ#1739556)

tigervnc foi rebaseado para a versão 1.10.1

O conjunto **tigervnc** foi rebaseado para a versão 1.10.1. A atualização contém número de correções e melhorias. Mais notadamente:

- o tigervnc agora suporta apenas o início do servidor de computação de rede virtual (VNC) usando o gerenciador de serviços **systemd**.
- O clipboard agora suporta Unicode completo no visualizador nativo, **WinVNC** e Xvnc/libvnc.so.
- O cliente nativo agora vai respeitar a loja de confiança do sistema ao verificar os certificados do servidor.
- O servidor web Java foi removido.
- **x0vncserver** agora pode ser configurado para permitir apenas conexões locais.
- **x0vncserver** recebeu correções para quando apenas parte do display é compartilhada.
- A votação agora é padrão no **WinVNC**.
- A compatibilidade com o servidor VNC da VMware foi melhorada.
- A compatibilidade com alguns métodos de entrada no MacOS foi melhorada.
- O "reparo" automático de artefatos JPEG foi melhorado.

(BZ#1806992)

6.1.15. Infra-estruturas gráficas

Suporte para novas placas gráficas

As seguintes placas gráficas são agora totalmente suportadas:

- A família AMD Navi 14, que inclui os seguintes modelos:
  - Radeon RX 5300
  - Radeon RX 5300 XT
  - Radeon RX 5500
  - Radeon RX 5500 XT
- A família AMD Renoir APU, que inclui os seguintes modelos:
  - Ryzen 3 4300U
  - Ryzen 5 4500U, 4600U, e 4600H

    - Ryzen 7 4700U, 4800U, e 4800H
- A família AMD Dali APU, que inclui os seguintes modelos:
    - Prata Athlon 3050U
    - Athlon Gold 3150U
    - Ryzen 3 3250U

Além disso, os seguintes drivers gráficos foram atualizados:

- O motorista Matrox **mgag200**

(JIRA:RHELPLAN-55009)

Aceleração de ferragens com Nvidia Volta e Turing

O **novo** driver gráfico agora suporta aceleração de hardware com as famílias Nvidia Volta e Turing GPU. Como resultado, o desktop e os aplicativos que usam gráficos 3D agora renderizam eficientemente na GPU. Além disso, isto libera a CPU para outras tarefas e melhora a capacidade de resposta do sistema como um todo.

(JIRA:RHELPLAN-57564)

Redução do rasgo da tela no XWayland

O display XWayland back end agora permite a extensão XPresent. Usando o XPresent, as aplicações podem atualizar eficientemente o conteúdo de suas janelas, o que reduz o rasgo da tela.

Este recurso melhora significativamente a renderização da interface do usuário de aplicações OpenGL em tela cheia, tais como editores 3D.

(JIRA:RHELPLAN-57567)

6.1.16. O console web

Definir privilégios de dentro da sessão do console web

Com esta atualização, o console web oferece uma opção para alternar entre acesso administrativo e acesso limitado de dentro de uma sessão do usuário. Você pode alternar entre os modos clicando no indicador **Administrative access** ou **Limited access** em sua sessão do console web.

(JIRA:RHELPLAN-42395)

Melhorias na busca de logs

Com esta atualização, o console web introduz uma caixa de busca que suporta várias novas maneiras de como os usuários podem pesquisar entre os logs. A caixa de busca suporta a busca de expressões regulares em mensagens de log, especificando serviço ou busca de entradas com campos de log específicos.

(BZ#1710731)

A página de visão geral mostra relatórios mais detalhados Insights

Com esta atualização, quando uma máquina é conectada ao Red Hat Insights, o cartão **Health** na página **Overview** no console web mostra informações mais detalhadas sobre o número de acessos e sua prioridade.

(JIRA:RHELPLAN-42396)

6.1.17. Funções do Sistema Red Hat Enterprise Linux

Terminal log função adicionada aos papéis do sistema RHEL

Com esta melhoria, uma nova função *Terminal log* (TLOG) foi adicionada às funções do sistema RHEL enviada com o pacote **rhel-system-roles**. Os usuários podem agora usar a função **tlog** para configurar e configurar a gravação da sessão usando o Ansible.

Atualmente, o papel **do tlog** apóia as seguintes tarefas:

- Configurar **o tlog** para registrar os dados de registro no diário **do sistema**
- Habilitar a gravação de sessões para usuários e grupos explícitos, via SSSD

(BZ#1822158)

A função do Sistema de Registro RHEL está agora disponível para Ansible

Com o papel do sistema de registro, você pode implantar várias configurações de registro de forma consistente em hosts locais e remotos. Você pode configurar um host RHEL como um servidor para coletar logs de muitos sistemas clientes.

(BZ#1677739)

rhel-system-roles-sap totalmente apoiado

O pacote **rhel-system-roles-sap**, anteriormente disponível como um Technology Preview, agora é totalmente suportado. Ele 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** são totalmente suportados:

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

Para mais informações, veja as funções do sistema Red Hat Enterprise Linux para SAP .

(BZ#1660832)

A métrica RHEL System Role está agora disponível para Ansible.

Com a **métrica** RHEL System Role, você pode configurar, para hosts locais e remotos:

- serviços de análise de desempenho através da aplicação **pcp**
- visualização destes dados usando um servidor **grafana**

- consulta destes dados usando a fonte de dados **redis** sem ter que configurar manualmente estes serviços separadamente.

(BZ#1890499)

rhel-system-roles-sap atualizado

O ***rhel-system-roles-sap*** os pacotes foram atualizados para a versão upstream 2.0.0, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Melhorar a configuração e verificação dos nomes das mangueiras
- Melhorar a detecção e manuseio do status do **uuidd**
- Adicionar suporte para a opção **--check (-c)**
- Aumentar os limites de **nofile** de 32800 para 65536
- Adicione o arquivo **nfs-utils** a **sap_preconfigure_packages***
- Desativar **firewalld**. Com esta mudança, desativamos o **firewalld** somente quando ele é instalado.
- Adicionar versões mínimas exigidas do pacote de **configuração** para RHEL 8.0 e RHEL 8.1.
- Melhorar o manuseio dos arquivos **tmpfiles.d/sap.conf**
- Apoiar a execução em uma única etapa ou verificação das notas SAP
- Adicionar os pacotes de **compatriotas** necessários
- Melhorar o manuseio da instalação mínima da embalagem
- Detectar se uma reinicialização é necessária após a aplicação das funções do Sistema RHEL
- Suporte de definição de qualquer estado SElinux. O estado padrão é **"deficiente**"
- Não falhar mais se houver mais de uma linha com endereços IP idênticos
- Não modificar mais **/etc/hosts** se houver mais de uma linha contendo **sap_ip**
- Apoio para HANA no RHEL 7.7
- Suporte para adicionar um repositório para as ferramentas de serviço e produtividade IBM para Power, necessário para SAP HANA na plataforma **ppc64le**

(BZ#1844190)

6.1.18. Virtualização

A migração de uma máquina virtual para um host com configuração de TSC incompatível agora falha mais rapidamente

Anteriormente, a migração de uma máquina virtual para um host com configuração incompatível do contador de carimbos de tempo (TSC) falhou no final do processo. Com esta atualização, a tentativa de tal migração gera um erro antes do início do processo de migração.

(JIRA:RHELPLAN-45950)

Suporte de virtualização para processadores AMD EPYC de segunda geração

Com esta atualização, a virtualização no RHEL 8 adiciona suporte aos processadores AMD EPYC de segunda geração, também conhecidos como EPYC Rome. Como resultado, as máquinas virtuais hospedadas no RHEL 8 podem agora usar o modelo de CPU **EPYC-Roma** e utilizar os novos recursos que os processadores oferecem.

(JIRA:RHELPLAN-45959)

Novo comando: virsh iothreadset

Esta atualização introduz o comando **virsh iothreadset**, que pode ser usado para configurar a sondagem dinâmica IOThread. Isto torna possível a configuração de máquinas virtuais com latências mais baixas para cargas de trabalho IO-intensivas à custa de um maior consumo de CPU para o IOThread. Para opções específicas, consulte a página virsh man.

(JIRA:RHELPLAN-45958)

A UMIP é agora suportada pela KVM na 10ª geração de processadores Intel Core

Com esta atualização, o recurso User-mode Instruction Prevention (UMIP) é agora suportado pela KVM para hosts executados em processadores Intel Core da 10ª geração, também conhecidos como Ice Lake Servers. O recurso UMIP emite uma exceção geral de proteção se certas instruções, tais como **sgdt**, **sidt**, **sldt**, **smsw** e **str**, forem executadas quando o Nível de Privilégios Atual (CPL) for maior que 0. Como resultado, o UMIP garante a segurança do sistema, impedindo que aplicações não autorizadas acessem certas configurações em todo o sistema que podem ser usadas para iniciar ataques de escalada de privilégios.

(JIRA:RHELPLAN-45957)

A biblioteca libvirt agora suporta alocação de largura de banda de memória

libvirt agora suporta a alocação de largura de banda de memória (MBA). Com o MBA, você pode alocar partes da largura de banda de memória do host em threads vCPU usando o elemento **<memorytune>** na seção **<cputune>**.

MBA é uma extensão do Cache QoS Enforcement (CQE) existente encontrado nos processadores Intel Xeon v4, também conhecido como servidor Broadwell. Para tarefas que estão associadas à afinidade com a CPU, o mecanismo usado pelo MBA é o mesmo que no CQE.

(JIRA:RHELPLAN-45956)

As máquinas virtuais RHEL 6 agora suportam o tipo de máquina Q35

Máquinas virtuais (VMs) hospedadas no RHEL 8 que usam o RHEL 6 como seu sistema operacional convidado podem agora usar o Q35, um tipo de máquina mais moderno baseado no PCI Express. Isto fornece uma variedade de melhorias nas características e desempenho dos dispositivos virtuais, e garante que uma gama mais ampla de dispositivos modernos seja compatível com as máquinas virtuais RHEL 6.

(JIRA:RHELPLAN-45952)

Todos os eventos de QEMU registrados agora têm um carimbo de tempo. Como resultado, os usuários podem mais facilmente solucionar problemas em suas máquinas virtuais usando os logs salvos no diretório /var/log/libvirt/qemu/qemu/.

Os registros da QEMU agora incluem carimbos de tempo para eventos do servidor de temperos

Esta atualização adiciona carimbos de tempo aos registros de eventos do servidor do Spice-server.

Portanto, todos os eventos de QEMU registrados agora têm um carimbo de tempo. Como resultado, os usuários podem mais facilmente solucionar problemas em suas máquinas virtuais usando os logs salvos no diretório **/var/log/libvirt/qemu/**.

(JIRA:RHELPLAN-45945)

O dispositivo bochs-display é agora suportado

RHEL 8.3 e posteriormente introduz o dispositivo de exibição Bochs, que é mais seguro do que o dispositivo **stdvga** atualmente utilizado. Note que todas as máquinas virtuais (VMs) compatíveis com o **bochs-display** o utilizarão por padrão. Isto inclui principalmente as VMs que utilizam a interface UEFI.

(JIRA:RHELPLAN-45939)

Proteção MDS otimizada para máquinas virtuais

Com esta atualização, um host RHEL 8 pode informar suas máquinas virtuais (VMs) se elas são vulneráveis à Amostragem de Dados Microarquitetônicos (MDS). VMs que não são vulneráveis não usam medidas contra MDS, o que melhora seu desempenho.

(JIRA:RHELPLAN-45937)

Criação de imagens de disco QCOW2 no RBD agora suportada

Com esta atualização, é possível criar imagens de disco QCOW2 no armazenamento do RADOS Block Device (RBD). Como resultado, as máquinas virtuais podem utilizar servidores RBD para seus back ends de armazenamento com imagens QCOW2.

Observe, entretanto, que o desempenho de gravação das imagens de disco QCOW2 no armazenamento RBD é atualmente menor do que o pretendido.

(JIRA:RHELPLAN-45936)

O máximo de dispositivos VFIO suportados aumentou para 64

Com esta atualização, você pode anexar até 64 dispositivos PCI que utilizam VFIO a uma única máquina virtual em um host RHEL 8. Esta é a partir de 32 no RHEL 8.2 e anteriores.

(JIRA:RHELPLAN-45930)

os comandos dedescarte e escrever-zeroes são agora suportados em QEMU/KVM

Com esta atualização, os comandos de **descarte** e **escrever-zeroes** para **virtio-blk** são agora suportados em QEMU/KVM. Como resultado, as máquinas virtuais podem usar o dispositivo **virtio-blk** para descartar setores não utilizados de um SSD, encher setores com zeros quando eles são esvaziados, ou ambos. Isto pode ser usado para aumentar o desempenho do SSD ou para garantir que um drive seja apagado com segurança.

(JIRA:RHELPLAN-45926)

RHEL 8 agora suporta IBM POWER 9 XIVE

Esta atualização introduz o suporte ao recurso de Mecanismo de Virtualização de Interrupção Externa (XIVE) do IBM POWER9 ao RHEL 8. Como resultado, máquinas virtuais (VMs) rodando em um hipervisor RHEL 8 em um sistema IBM POWER 9 podem usar o XIVE, o que melhora o desempenho de VMs I/O-intensivas.

(JIRA:RHELPLAN-45922)

Suporte do Control Group v2 para máquinas virtuais

Com esta atualização, o conjunto libvirt suporta os grupos de controle v2. Como resultado, as máquinas virtuais hospedadas no RHEL 8 podem tirar proveito das capacidades de controle de recursos do grupo de controle v2.

(JIRA:RHELPLAN-45920)

Os IPIs paravirtualizados são agora suportados para máquinas virtuais Windows

Com esta atualização, a bandeira **hv_ipi** foi adicionada às iluminações de hipervisor suportadas para máquinas virtuais Windows (VMs). Isto permite que interrupções inter-processador (IPIs) sejam enviadas através de um hipercall. Como resultado, os IPIs podem ser executados mais rapidamente em VMs rodando um sistema operacional Windows.

(JIRA:RHELPLAN-45918)

Migração de máquinas virtuais com cache de disco habilitado agora é possível

Esta atualização torna o hipervisor RHEL 8 KVM compatível com a migração ao vivo do cache de disco. Como resultado, agora é possível migrar máquinas virtuais ao vivo com cache em disco habilitado.

(JIRA:RHELPLAN-45916)

as interfaces macvtap podem agora ser utilizadas por máquinas virtuais em sessões não-privilegiadas

Agora é possível que as máquinas virtuais (VMs) utilizem uma interface macvtap previamente criada por um processo privilegiado. Notavelmente, isto permite que as VMs iniciadas pela sessão de **usuários** não privilegiados da **libvirtd** utilizem uma interface macvtap.

Para fazer isso, primeiro crie uma interface macvtap em um ambiente privilegiado e configure-a para ser propriedade do usuário que estará executando **libvirtd** em uma sessão não-privilegiada. Você pode fazer isso usando um aplicativo de gerenciamento como o console web, ou usando utilitários de linha de comando como root, por exemplo:

```
# ip link add link en2 name mymacvtap0 address 52:54:00:11:11:11 type macvtap mode bridge
# chown myuser /dev/tap$(cat /sys/class/net/mymacvtap0/ifindex)
# ip link set mymacvtap0 up
```

Em seguida, modifique o subelemento **<target>** da configuração **<interface>** da VM para fazer referência à interface macvtap recém-criada:

```
<interface type='ethernet'>
  <model type='virtio'/>
  <mac address='52:54:00:11:11:11'/>
  <target dev='mymacvtap0' managed='no'/>
</interface>
```

Com esta configuração, se **a libvirtd** for executada como o usuário **myuser**, a VM utilizará a interface macvtap existente quando iniciada.

(JIRA:RHELPLAN-45915)

Máquinas virtuais podem agora usar recursos da 10ª geração de processadores Intel Core

Os nomes dos modelos de CPU **Icelake-Server** e **Icelake-Client** estão agora disponíveis para máquinas virtuais (VMs). Em hosts com processadores Intel Core de 10ª geração, utilizando **Icelake-Server** ou

Icelake-Client como o tipo de CPU na configuração XML de uma VM faz com que as novas características destas CPUs sejam expostas à VM.

(JIRA:RHELPLAN-45911)

QEMU agora suporta a criptografia LUKS

Com esta atualização, é possível criar discos virtuais usando criptografia Linux Unified Key Setup (LUKS). Você pode criptografar os discos ao criar o volume de armazenamento, incluindo o campo **<encryption>** na configuração XML da máquina virtual (VM). Você também pode tornar o disco virtual encriptado **LUKS** completamente transparente para a VM, incluindo o campo **<encryption>** na definição de domínio do disco no arquivo de configuração XML.

(JIRA:RHELPLAN-45910)

Logs melhorados para o nbdkit

O registro de serviços **nbdkit** foi modificado para ser menos verboso. Como resultado, os logs do **nbdkit** são apenas mensagens potencialmente importantes, e os logs criados durante as conversões **virt-v2v** são mais curtos e fáceis de analisar.

(JIRA:RHELPLAN-45909)

Maior consistência para as máquinas virtuais SELinux etiquetas e permissões de segurança

Com esta atualização, o serviço **libvirt** pode gravar as etiquetas de segurança e permissões SELinux associadas aos arquivos, e restaurar as etiquetas após a modificação dos arquivos. Como resultado, por exemplo, utilizando utilitários **libguestfs** para modificar uma imagem de disco de uma máquina virtual (VM) de propriedade de um usuário específico, não muda mais o proprietário da imagem para root.

Note que este recurso não funciona em sistemas de arquivos que não suportam atributos de arquivos estendidos, tais como NFS.

(JIRA:RHELPLAN-45908)

QEMU agora usa a biblioteca de criptografia para cifras XTS

Com esta atualização, o emulador QEMU foi alterado para usar a implementação do modo cifra XTS fornecido pela biblioteca **gcrypt**. Isto melhora o desempenho de E/S de máquinas virtuais cujo armazenamento no host utiliza o driver de criptografia nativo **da** QEMU.

(JIRA:RHELPLAN-45904)

Os drivers de Windows Virtio agora podem ser atualizados usando Windows Updates

Com esta atualização, uma nova cadeia padrão **SMBIOS** é iniciada por padrão quando a QEMU inicia. Os parâmetros fornecidos nos campos **SMBIOS** tornam possível gerar IDs para o hardware virtual rodando na máquina virtual (VM). Como resultado, Windows Update pode identificar o hardware virtual e o tipo de máquina hypervisor RHEL, e atualizar os drivers Virtio nas VMs rodando Windows 10 , Windows Server 2016, e Windows Server 2019 .

(JIRA:RHELPLAN-45901)

Novo comando: virsh guestinfo

O comando **virsh guestinfo** foi introduzido no RHEL 8.3. Isto torna possível relatar os seguintes tipos de informações sobre uma máquina virtual (VM):

- Informações do sistema de arquivos e do sistema de arquivos para convidados

- Usuários ativos
- O fuso horário utilizado

Antes de executar o **virsh guestinfo**, assegure-se de que o pacote *qemu-guest-agent* esteja instalado. Além disso, o canal **guest_agent** deve ser habilitado na configuração XML da VM, por exemplo, como a seguir:

```
<channel type='unix'>
  <target type='virtio' name='org.qemu.guest_agent.0'/>
</channel>
```

(JIRA:RHELPLAN-45900)

As entradas VNNI para BFLOAT16 são agora suportadas pela KVM

Com esta atualização, as Vector Neural Network Instructions (VNNI) suportam as entradas **BFLOAT16**, também conhecidas como instruções **AVX512_BF16**, agora são suportadas pela KVM para os processadores escaláveis Intel Xeon de terceira geração, também conhecidos como Cooper Lake. Como resultado, o software convidado pode agora usar as instruções do **AVX512_BF16** dentro de máquinas virtuais, habilitando-o na configuração da CPU virtual.

(JIRA:RHELPLAN-45899)

Novo comando: virsh-capacidades do pool

RHEL 8.3 introduz a opção de comando de **capacidade de piscina virsh**. Este comando exibe informações que podem ser usadas para criar pools de armazenamento, bem como volumes de armazenamento dentro de cada pool, em seu host. Isto inclui:

- Tipos de piscina de armazenagem
- Formatos de fonte do pool de armazenamento
- Tipos de formatos de volume de armazenamento de destino

(JIRA:RHELPLAN-45884)

Suporte para CPUID.1F em máquinas virtuais com processadores Intel Xeon Platinum série 9200

Com esta atualização, as máquinas virtuais hospedadas no RHEL 8 podem ser configuradas com uma topologia de CPU virtual de múltiplas matrizes, usando a função Folha de Enumeração Topológica Estendida (CPUID.1F). Esta característica é suportada pelos processadores Intel Xeon Platinum série 9200, anteriormente conhecidos como Cascade Lake. Como resultado, agora é possível em hosts que usam processadores Intel Xeon Platinum série 9200 para criar uma topologia vCPU que espelha a topologia física da CPU do host.

(JIRA:RHELPLAN-37573, JIRA:RHELPLAN-45934)

Máquinas virtuais podem agora usar recursos de Processadores Escaláveis Intel Xeon de 3ª Geração

O nome do modelo de CPU **Cooperlake** está agora disponível para máquinas virtuais (VMs). Usando **Cooperlake** como o tipo de CPU na configuração XML de uma VM faz novas características dos Processadores Escaláveis Intel Xeon de 3ª Geração expostos à VM, se o host usar esta CPU.

(JIRA:RHELPLAN-37570)

Memória persistente Intel Optane agora suportada pela KVM

Com esta atualização, as máquinas virtuais hospedadas no RHEL 8 podem se beneficiar da tecnologia de memória persistente Intel Optane, anteriormente conhecida como Intel Crystal Ridge. Os dispositivos de armazenamento de memória persistente Intel Optane fornecem tecnologia de memória persistente de classe data center, que pode aumentar significativamente o rendimento das transações.

(JIRA:RHELPLAN-14068)

Máquinas virtuais podem agora usar o processador Intel Processor Trace

Com esta atualização, as máquinas virtuais (VMs) hospedadas no RHEL 8 são capazes de usar o recurso Intel Processor Trace (PT). Quando seu host usa uma CPU que suporta Intel PT, você pode usar um software Intel especializado para coletar uma variedade de métricas sobre o desempenho da CPU de sua VM. Note que isto também requer a habilitação do recurso **intel-pt** na configuração XML da VM.

(JIRA:RHELPLAN-7788)

Os dispositivos DASD podem agora ser atribuídos a máquinas virtuais no IBM Z

Os dispositivos de armazenamento de acesso direto (DASDs) fornecem uma série de características específicas de armazenamento. Usando o recurso **vfio-ccw**, você pode atribuir DASDs como dispositivos mediados para suas máquinas virtuais (VMs) em hosts IBM Z. Isto, por exemplo, torna possível para a VM acessar um conjunto de dados z/OS, ou compartilhar os DASDs atribuídos com uma máquina z/OS.

(JIRA:RHELPLAN-40234)

IBM Secure Execution apoiado para IBM Z

Ao utilizar o hardware IBM Z para executar seu host RHEL 8, você pode melhorar a segurança de suas máquinas virtuais (VMs) configurando o IBM Secure Execution para as VMs. O IBM Secure Execution, também conhecido como Virtualização Protegida, impede que o sistema host acesse o estado e o conteúdo da memória de uma VM.

Como resultado, mesmo que o hospedeiro esteja comprometido, ele não pode ser usado como um vetor para atacar o sistema operacional convidado. Além disso, o Secure Execution pode ser usado para evitar que hospedeiros não confiáveis obtenham informações sensíveis do VM.

(JIRA:RHELPLAN-14754)

6.1.19. RHEL em ambientes de nuvens

parte de crescimento de nuvens-utils rebaixadas para 0,31

O pacote **de partes de crescimento de nuvens** foi atualizado para a versão 0.31, que fornece múltiplas correções e melhorias de bugs. Mudanças notáveis incluem:

- Um bug que impediu que os discos GPT crescessem além dos 2TB foi corrigido.
- A operação de **growpart** não falha mais quando o setor de partida e o tamanho são os mesmos.
- O redimensionamento de uma partição usando a utilidade **sgdisk** anteriormente, em alguns casos, falhou. Este problema agora foi resolvido.

(BZ#1846246)

6.1.20. Contêineres

imagem do recipienteskopeo já está disponível

A imagem do contêiner **registry.redhat.io/rhel8/skopeo** é uma implementação contentorizada do pacote **skopeo**. A ferramenta **skopeo** é um utilitário de linha de comando que realiza várias operações em imagens de contêineres e repositórios de imagens. Esta imagem de contêiner permite inspecionar imagens de contêineres em um registro, remover uma imagem de contêiner de um registro e copiar imagens de contêineres de um registro de contêineres não autenticado para outro. Para puxar a imagem do contêiner **Registry.redhat.io/rhel8/skopeo**, você precisa de uma assinatura ativa do Red Hat Enterprise Linux.

(BZ#1627900)

imagem do containerbuildah já está disponível

A imagem do container **register.redhat.io/rhel8/buildah** é uma implementação em container do pacote **buildah**. A ferramenta **buildah** facilita a construção de imagens de contêineres OCI. Esta imagem de container permite a construção de 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. Para obter a imagem do contêiner **register.redhat.io/rhel8/buildah**, você precisa de uma assinatura ativa do Red Hat Enterprise Linux.

(BZ#1627898)

Podman v2.0 RESTful API agora está disponível

A nova API Podman 2.0 baseada em REST substitui a antiga API remota baseada na biblioteca varlink. A nova API funciona tanto em um ambiente sem raízes quanto em um ambiente sem raízes e fornece uma camada de compatibilidade de docas.

(JIRA:RHELPLAN-37517)

A instalação de Podman não requer contentor-selinux

Com este aperfeiçoamento, a instalação do pacote **contentor-selinux** é agora opcional durante a construção do contentor. Como resultado, Podman tem menos dependências em relação a outros pacotes.

(BZ#1806044)

6.1.21. Novos motoristas

Drivers de rede

- Driver CAN para dispositivos Kvaser CAN/USB (kvaser_usb.ko.xz)
- Driver para dispositivos Theobroma Systems UCAN (ucan.ko.xz)
- Driver NIC Pensando Ethernet (ionic.ko.xz)

Drivers gráficos e drivers diversos

- Estrutura genérica de processador remoto (remoteproc.ko.xz)
- Injeção em estado ocioso de nível C para CPUs Intel (intel_powerclamp.ko.xz)
- X86 PKG TEMP Thermal Driver (x86_pkg_temp_thermal.ko.xz)
- INT3402 Condutor térmico (int3402_thermal.ko.xz)

- ACPI INT3403 condutor térmico (int3403_thermal.ko.xz)
- Intel® acpi thermal rel misc dev driver (acpi_thermal_rel.ko.xz)
- INT3400 Condutor térmico (int3400_thermal.ko.xz)
- Intel® INT340x manipulador de zona térmica comum (int340x_thermal_zone.ko.xz)
- Processador de dispositivos de relatório térmico (processor_thermal_device.ko.xz)
- Driver térmico Intel® PCH (intel_pch_thermal.ko.xz)
- Ajudantes DRM gem ttm (drm_ttm_helper.ko.xz)
- Registro de nodo de dispositivo para controladores cec (cec.ko.xz)
- Fairchild FUSB302 Motorista de chip tipo C (fusb302.ko.xz)
- VHOST IOTLB (vhost_iotlb.ko.xz)
- backend para virtio (vhost_vdpa.ko.xz) baseado em vDPA
- Driver de relógio virtual PTP da VMware (ptp_vmw.ko.xz)
- Driver Intel LPSS PCI (intel-lpss-pci.ko.xz)
- Driver central LPSS Intel (intel-lpss.ko.xz)
- Driver Intel® LPSS ACPI (intel-lpss-acpi.ko.xz)
- Motorista do cão de guarda Mellanox (mlx_wdt.ko.xz)
- Mellanox FAN driver (mlxreg-fan.ko.xz)
- Mellanox regmap I/O access driver (mlxreg-io.ko.xz)
- Driver de caixa de correio pci de interface de seleção de velocidade Intel® (isst_if_mbox_pci.ko.xz)
- Driver de caixa de correio de interface de seleção de velocidade Intel® (isst_if_mbox_msr.ko.xz)
- Interface de seleção de velocidade Intel® mmio driver (isst_if_mmio.ko.xz)
- Mellanox LED regmap driver (leds-mlxreg.ko.xz)
- simulador de Dispositivos vDPA (vdpa_sim.ko.xz)
- Driver Intel® Tiger Lake PCH pinctrl/GPIO (pinctrl-tigerlake.ko.xz)
- Controlador SPI PXA2xx SSP (spi-pxa2xx-platform.ko.xz)
- CE4100/LPSS Código de cola PCI-SPI para o driver PXA (spi-pxa2xx-pci.ko.xz)
- Interface Hyper-V PCI (pci-hyperv-intf.ko.xz)
- vDPA motorista de ônibus para dispositivos virtio (virtio_vdpa.ko.xz)

6.1.22. Drivers atualizados

Atualizações de driver de rede

- O driver virtual NIC VMware vmxnet3 (vmxnet3.ko.xz) foi atualizado para a versão 1.5.0.0.0-k.
- O Realtek RTL8152/RTL8153 Adaptadores Ethernet USB (r8152.ko.xz) foi atualizado para a versão 1.09.10.
- O driver de rede Broadcom BCM573xx (bnxt_en.ko.xz) foi atualizado para a versão 1.10.1.
- O controlador Netronome Flow Processor (NFP) (nfp.ko.xz) foi atualizado para a versão 4.18.0-240.el8.x86_64.
- O driver de interface de host do switch Ethernet Intel® (fm10k.ko.xz) foi atualizado para a versão 0.27.1-k.
- O driver Intel® Ethernet Connection E800 Series Linux (ice.ko.xz) foi atualizado para a versão 0.8.2-k.

Atualizações do driver de armazenamento

- O driver SCSI Emulex LightPulse Fibre Channel (lpfc.ko.xz) foi atualizado para a versão 0:12.8.0.1.
- O QLogic FCoE Driver (bnx2fc.ko.xz) foi atualizado para a versão 2.12.13.
- O LSI MPT Fusion SAS 3.0 Device Driver (mpt3sas.ko.xz) foi atualizado para a versão 34.100.00.00.
- O driver para a versão HP Smart Array Controller (hpsa.ko.xz) foi atualizado para a versão 3.4.20-170-RH5.
- O QLogic Fibre Channel HBA Driver (qla2xxx.ko.xz) foi atualizado para a versão 10.01.00.25.08.3-k.
- Broadcom MegaRAID SAS Driver (megaraid_sas.ko.xz) foi atualizado para a versão 07.714.04.00-rh1.

Atualizações gráficas e de drivers diversos

- O driver autônomo drm para o dispositivo VMware SVGA (vmwgfx.ko.xz) foi atualizado para a versão 2.17.0.0.
- Co-processador criptográfico para cartões Chelsio Terminator. (chcr.ko.xz) foi atualizado para a versão 1.0.0.0-ko.

6.2. CORREÇÃO DE ERROS

Esta parte descreve os bugs corrigidos no Red Hat Enterprise Linux 8.3 que têm um impacto significativo sobre os usuários.

6.2.1. Instalador e criação de imagem

A configuração inicial do RHEL 8 agora funciona corretamente via SSH

Anteriormente, a interface de configuração inicial do RHEL 8 não era exibida quando se entrava no

sistema usando SSH. Como conseqüência, era impossível realizar a configuração inicial em uma máquina RHEL 8 gerenciada via SSH. Este problema foi corrigido e a configuração inicial do RHEL 8 agora funciona corretamente quando executada via SSH.

(BZ#1676439)

A instalação falhou ao usar o comando **reboot --kexec**

Anteriormente, a instalação do RHEL 8 falhou quando foi usado um arquivo Kickstart que continha o comando **reboot --kexec**.

Com esta atualização, a instalação com **reboot --kexec** agora funciona como esperado.

(BZ#1672405)

America/New York O fuso horário pode agora ser definido corretamente

Anteriormente, o processo de instalação interativa do Anaconda não permitia aos usuários definir o fuso horário *America/New York* ao usar um arquivo kickstart. Com esta atualização, os usuários agora podem definir *America/New York* como o fuso horário preferido no instalador interativo se um fuso horário não estiver especificado no arquivo de kickstart.

(BZ#1665428)

Os contextos SELinux são agora definidos corretamente

Anteriormente, quando o SELinux estava em modo de aplicação, contextos incorretos do SELinux em algumas pastas e arquivos resultavam em negações inesperadas do AVC ao tentar acessar esses arquivos após a instalação.

Com esta atualização, o Anaconda define os contextos SELinux corretos. Como resultado, você pode agora acessar as pastas e arquivos sem precisar reetiquetar manualmente o sistema de arquivos.

(BZ#1775975)

A partição automática cria agora uma partição **/boot** válida

Anteriormente, ao instalar o RHEL em um sistema usando particionamento automático ou usando um arquivo kickstart com partições pré-configuradas, o instalador criou um esquema de particionamento que poderia conter uma partição **/boot** inválida. Conseqüentemente, o processo de instalação automática terminou prematuramente porque a verificação do esquema de particionamento falhou. Com esta atualização, o Anaconda cria um esquema de particionamento que contém uma partição **/boot** válida. Como resultado, a instalação automática é concluída como esperado.

(BZ#1630299)

Uma instalação GUI utilizando a imagem ISO do DVD Binário agora completa com sucesso sem registro CDN

Anteriormente, ao realizar uma instalação GUI usando o arquivo de imagem ISO do DVD binário, uma condição de corrida no instalador impedia que a instalação prosseguisse até que você registrou o sistema usando o recurso Conectar à Red Hat.

Com esta atualização, você pode agora prosseguir com a instalação sem registrar o sistema usando o recurso Conectar à Red Hat.

(BZ#1823578)

os dispositivos iSCSI ou FCoE criados no Kickstart e usados em comando de uso ignorado --somente para uso -- não interrompem mais o processo de instalação

Anteriormente, quando os dispositivos iSCSI ou FCoE criados no Kickstart eram usados no comando ignoredisk **--only-use**, o programa de instalação falhou com um erro semelhante ao **Disco \i360a9800042566643352b476d674a774a\i360a9800042566643352b476d674a774a\i360a9800042566643352b476d676d674d674a\i360a774a) dado no comando ignoredisk não existe**. Isto interrompeu o processo de instalação.

Com esta atualização, o problema foi resolvido. O programa de instalação continua funcionando.

(BZ#1644662)

O registro do sistema usando CDN falhou com a mensagem de erro Name or service not known

Quando você tentou registrar um sistema usando a Rede de Entrega de Conteúdo (CDN), o processo de registro falhou com a mensagem de erro **Name or service not known**

Esta questão ocorreu porque os valores vazios **Custom server URL** e **Custom Base URL** sobrescreveram os valores padrão para o registro do sistema.

Com esta atualização, os valores vazios agora não sobrescrevem os valores padrão, e o registro do sistema é concluído com sucesso.

(BZ#1862116)

6.2.2. Gestão de software

dnf-automatic agora só atualiza pacotes com as assinaturas GPG corretas

Anteriormente, o arquivo de configuração **dnf-automatic** não verificava as assinaturas GPG dos pacotes baixados antes de realizar uma atualização. Como conseqüência, atualizações não assinadas ou atualizações assinadas por chave que não foram importadas podiam ser instaladas pelo **dnf-automatic** mesmo que a configuração do repositório exigisse a verificação da assinatura GPG**(gpgcheck=1**). Com esta atualização, o problema foi corrigido e o **dnf-automatic** verifica as assinaturas GPG dos pacotes baixados antes de executar a atualização. Como resultado, somente atualizações com assinaturas GPG corretas são instaladas a partir de repositórios que requerem a verificação da assinatura GPG.

(BZ#1793298)

O trailing comma não causa mais a remoção das entradas em uma opção do tipo apêndice

Anteriormente, a adição de uma vírgula (uma entrada vazia no final da lista) a uma opção do tipo **anexo** (por exemplo, **exclude**, **excludepkgs**, **includepkgs**) fez com que todas as entradas da opção fossem removidas. Além disso, a adição de duas vírgulas (uma entrada vazia) fez com que somente as entradas após as vírgulas fossem usadas.

Com esta atualização, as entradas vazias além das vírgulas (uma entrada vazia no início da lista) são ignoradas. Como resultado, apenas a vírgula principal remove agora as entradas existentes da opção de tipo de **apêndice**, e o usuário pode usá-la para sobregravar estas entradas.

(BZ#1788154)

6.2.3. Conchas e ferramentas de linha de comando

O layout do disco ReaR não inclui mais entradas para os dispositivos Rancher 2 Longhorn iSCSI e sistemas de arquivo

Esta atualização remove entradas para os dispositivos Rancher 2 Longhorn iSCSI e sistemas de arquivo do layout do disco criado pela **ReaR**.

(BZ#1843809)

A criação de imagens de salvamento com um arquivo maior que 4 GB está agora habilitada no IBM POWER, little endian

Anteriormente, o utilitário **ReaR** não podia criar imagens de resgate contendo arquivos maiores que 4GB em IBM POWER, arquitetura pouco endian. Com esta atualização, o problema foi resolvido, e agora é possível criar uma imagem de resgate com um arquivo maior que 4 GB em IBM POWER, pequeno endian.

(BZ#1729502)

6.2.4. Segurança

SELinux não impede mais que o systemd-journal-gatewayd chame newfstat() em /dev/shm/ arquivos usados pela corosync

Anteriormente, a política SELinux não continha uma regra que permitisse que o daemon do **sistema-journal-gatewayd** acessasse arquivos criados pelo serviço **corosync**. Como consequência, o SELinux negou o **systemd-journal-gatewayd** para chamar a função **newfstat()** nos arquivos de memória compartilhada criados pela **corosync**. Com esta atualização, o SELinux não mais impede que o **systemd-journal-gatewayd** ligue para **newfstat(**) em arquivos de memória compartilhada criados pela **corosync**.

(BZ#1746398)

Libreswan agora trabalha com seccomp=enabled em todas as configurações

Antes desta atualização, o conjunto de syscalls permitidos na implementação do suporte de **Libreswan** SECCOMP não correspondia ao novo uso das bibliotecas RHEL. Consequentemente, quando a SECCOMP foi habilitada no arquivo **ipsec.conf**, a filtragem da syscall rejeitou até mesmo os syscalls necessários para o funcionamento adequado do daemon **pluto**; o daemon foi morto e o serviço **ipsec** foi reiniciado. Com esta atualização, todos os novos syscalls necessários foram permitidos, e **Libreswan** agora trabalha com a opção **seccomp=enabled** corretamente.

(BZ#1544463)

A SELinux não impede mais que a auditoria interrompa ou desligue o sistema

Anteriormente, a política SELinux não continha uma regra que permitisse que o daemon de Auditoria iniciasse uma unidade do **sistema power_unit_file_t**. Conseqüentemente, **a Auditd** não podia 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.

Esta atualização dos pacotes **selinux-policy** adiciona a regra que falta, e **a auditd** pode agora parar e desligar corretamente o sistema somente com SELinux em modo de aplicação.

(BZ#1826788)

IPTABLES_SAVE_ON_STOP agora funciona corretamente

Anteriormente, o recurso **IPTABLES_SAVE_ON_STOP** do serviço **iptables** não funcionava porque

arquivos com conteúdo de tabelas IP salvas receberam contexto SELinux incorreto. Isto impediu que o script **iptables** mudasse as permissões, e o script posteriormente falhou em salvar as mudanças. Esta atualização define um contexto apropriado para os arquivos **iptables.save** e **ip6tables.save** e cria uma regra de transição de nomes de arquivos. Como conseqüência, o recurso **IPTABLES_SAVE_ON_STOP** do serviço **iptables** funciona corretamente.

(BZ#1776873)

Os bancos de dados NSCD podem agora usar diferentes modos

Os domínios no atributo **nsswitch_domain** têm acesso aos serviços de Name Service Cache Daemon (NSCD). Cada banco de dados do NSCD é configurado no arquivo **nscd.conf**, e a propriedade **compartilhada** determina se o banco de dados usa memória compartilhada ou modo Socket. Anteriormente, todas as bases de dados NSCD tinham que usar o mesmo modo de acesso, dependendo do valor booleano do **nscd_use_shm**. Agora, o uso do soquete Unix é sempre permitido e, portanto, bancos de dados NSCD diferentes podem usar modos diferentes.

(BZ#1772852)

O utilitário oscap-ssh agora funciona corretamente 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 os arquivos de relatório em um diretório temporário como usuário **root**. Anteriormente, se as configurações **umask** na máquina remota fossem alteradas, **o oscap-ssh** poderia ter sido impedido o acesso a estes arquivos. Esta atualização corrige o problema e, como resultado, **o oscap** salva os arquivos como usuário alvo, e **o oscap-ssh** acessa os arquivos normalmente.

(BZ#1803116)

OpenSCAP agora lida corretamente com sistemas de arquivos remotos

Anteriormente, o OpenSCAP não detectava de forma confiável sistemas de arquivos remotos se sua especificação de montagem não começasse com dois cortes. Como conseqüência, OpenSCAP lidou com alguns sistemas de arquivos baseados em rede como locais. Com esta atualização, o OpenSCAP identifica os sistemas de arquivo usando o tipo de sistema de arquivo em vez da especificação de montagem. Como resultado, o OpenSCAP agora lida corretamente com sistemas de arquivo remotos.

(BZ#1870087)

OpenSCAP não remove mais linhas em branco das cordas multi-linhas YAML

Anteriormente, o OpenSCAP removeu linhas em branco das cordas multi-linhas da YAML dentro de um fluxo de dados gerado. Isto afetou as remediações possíveis e fez com que o utilitário **openscap** falhasse nas verificações correspondentes de Vulnerabilidade Aberta e Linguagem de Avaliação (OVAL), produzindo resultados falsos positivos. O problema agora está resolvido e, como resultado, o **openscap** não remove mais as linhas em branco das cadeias de caracteres de várias linhas da YAML.

(BZ#1795563)

OpenSCAP agora pode escanear sistemas com grande número de arquivos sem esgotar a memória

Anteriormente, ao digitalizar sistemas com baixa RAM e grande número de arquivos, o scanner OpenSCAP às vezes fazia com que o sistema ficasse sem memória. Com esta atualização, o gerenciamento da memória do scanner OpenSCAP foi melhorado. Como resultado, o scanner não fica

mais sem memória em sistemas com pouca memória RAM ao digitalizar um grande número de arquivos, por exemplo, grupos de pacotes **Servidor com GUI** e **Estação de Trabalho**.

(BZ#1824152)

config.enabled agora controla as declarações corretamente

Anteriormente, o **rsyslog** avaliou incorretamente a diretiva **config.enable** durante o processamento da configuração de uma declaração. Como conseqüência, o **parâmetro** erros **não conhecidos** eram exibidos para cada declaração, exceto para a declaração **include()**. Com esta atualização, a configuração é processada para todas as afirmações igualmente. Como resultado, o **config.enabled** agora desativa ou habilita corretamente as declarações sem exibir nenhum erro.

(BZ#1659383)

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 conseqüência, o sistema às vezes era incapaz de inicializar após a aplicação de atualizações.

Com o lançamento do RHBA-2020:5242 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#1897090)

O perfil e8 agora pode ser usado para remediar os sistemas RHEL 8 com **Servidor com GUI**

Usando o OpenSCAP Anaconda Add-on para endurecer o sistema no **Servidor Com GUI** grupo de pacotes com perfis que selecionam regras do grupo **Verify Integrity with RPM** não requer mais uma quantidade extrema de RAM no sistema. A causa deste problema foi o scanner OpenSCAP. Para mais detalhes, veja Digitalizando um grande número de arquivos com OpenSCAP faz com que os sistemas fiquem sem memória. Como conseqüência, o endurecimento do sistema usando o perfil RHEL 8 Essential Eight (e8) agora funciona também com o **Server With GUI**.

(BZ#1816199)

6.2.5. Trabalho em rede

O carregamento automático dos módulos de extensão **iptables** pelo módulo **nft_compat** não fica mais pendurado

Anteriormente, quando o módulo **nft_compat** carregou um módulo de extensão enquanto uma operação nos espaços de nomes de rede(**netns**) acontecia em paralelo, poderia ocorrer uma colisão de trava se essa extensão registrasse um subsistema **pernet** durante a inicialização. Como conseqüência, o comando **modprobe** chamado de kernel pendia. Isto também poderia ser causado por outros serviços, como o **libvirtd**, que também executam comandos **iptables**. Este problema foi resolvido. Como resultado, o carregamento dos módulos de extensão do **iptables** pelo módulo **nft_compat** não fica mais pendurado.

(BZ#1757933)

O serviço **firewalld** remove agora os **ipsets** quando o serviço pára

Anteriormente, a interrupção do serviço **firewalld** não removia os **ipsets**. Esta atualização corrige o problema. Como resultado, os **ipsets** não são mais deixados no sistema após a parada do **firewalld**.

(BZ#1790948)

firewalld não retém mais as entradas do ipset após o desligamento

Anteriormente, o desligamento do **firewalld** não removia as entradas do **ipset**. Consequentemente, as entradas do **ipset** permaneceram ativas no núcleo mesmo após a interrupção do serviço **firewalld**. Com esta correção, o desligamento do **firewalld** remove as entradas do **ipset**, como esperado.

(BZ#1682913)

firewalld agora restaura as entradas do ipset após a recarga

Anteriormente, **o firewalld** não retinha as entradas de tempo de execução do **ipset** após a recarga. Conseqüentemente, os usuários tinham que adicionar manualmente as entradas que faltavam novamente. Com esta atualização, **o firewalld** foi modificado para restaurar as entradas do **ipset** após o recarregamento.

(BZ#1809225)

nftables e serviços firewalld são agora mutuamente exclusivos

Anteriormente, era possível habilitar os serviços **nftables** e **firewalld** ao mesmo tempo. Como conseqüência, **a nftables** estava sobrepondo-se ao conjunto de regras **firewalld**. Com esta atualização, a **nftables** e os serviços **firewalld** agora são mutuamente exclusivos, de modo que estes não podem ser habilitados ao mesmo tempo.

(BZ#1817205)

6.2.6. Kernel

A enorme_página_setup_helper.py script agora funciona corretamente

Um patch que atualizou o **enorme_page_setup_helper.py** script para Python 3 foi removido acidentalmente. Consequentemente, após executar o arquivo **huge_page_setup_helper.py**, a seguinte mensagem de erro apareceu:

```
SintaxeError: Parênteses em falta na chamada para "imprimir
```

Com esta atualização, o problema foi resolvido atualizando o arquivo **libhugetlbfs.spec**. Como resultado, o arquivo **huge_page_setup_helper.py** não mostra nenhum erro no cenário descrito.

(BZ#1823398)

Os scripts bcc agora compilam com sucesso um módulo BPF

Durante a compilação do código do script para criar um módulo Berkeley Packet Filter (BPF), o conjunto de ferramentas **bcc** usou cabeçalhos do kernel para a definição do tipo de dados. Alguns cabeçalhos do kernel precisavam da macro **KBUILD_MODNAME** para serem definidos. Consequentemente, aqueles scripts **bcc** que não adicionavam **KBUILD_MODNAME**, provavelmente não compilariam um módulo BPF em várias arquiteturas de CPU. Os seguintes scripts **bcc** foram afetados:

- **bindsnoop**
- **sofdsnoop**

- **solisten**
- **tcpaccept**
- **tcpconnect**
- **tcpconnlat**
- **tcpdrop**
- **tcpretrans**
- **tcpsubnet**
- **tcptop**
- **tcptracer**

Com esta atualização, o problema foi resolvido adicionando **KBUILD_MODNAME** ao parâmetro padrão de **cflags** para **bcc**. Como resultado, este problema não aparece mais no cenário descrito. Além disso, os scripts dos clientes também não precisam definir **KBUILD_MODNAME** em si.

(BZ#183737906)

bcc-tools e bpftrace funcionam corretamente no IBM Z

Anteriormente, um backport de recursos introduziu a opção **ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE** kernel. Entretanto, o pacote **bcc-tools** e o pacote de linguagem de rastreamento **bpftrace** para arquiteturas IBM Z não tinham suporte adequado para esta opção. Consequentemente, a chamada ao sistema **bpf()** falhou com a exceção do **argumento Inválido** e **o bpftrace** falhou com um erro ao tentar carregar o **programa** BPF. Com esta atualização, a opção **ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE** é agora removida. Como resultado, o problema não aparece mais no cenário descrito.

(BZ#1847837, BZ#1853964)

O processo de inicialização não falha mais devido à falta de entropia

Anteriormente, o processo de inicialização falhou devido à falta de entropia. Um mecanismo melhor agora é usado para permitir que o núcleo colete a entropia no início do processo de inicialização, o que não depende de nenhuma interrupção específica do hardware. Esta atualização corrige o problema, garantindo a disponibilidade de entropia suficiente para garantir a geração aleatória no início do boot. Como resultado, a correção evita o tempo de kickstart ou arranque lento e o processo de arranque funciona como esperado.

(BZ#1778762)

Reinicializações repetidas usando o kexec agora funcionam como esperado

Anteriormente, durante a reinicialização do kernel na plataforma Amazon EC2 Nitro, o módulo de remoção**(rmmod**) não era chamado durante o **desligamento()** chamada do caminho de execução do kernel. Consequentemente, reinicializações repetidas do kernel usando a chamada do sistema **kexec** levaram a uma falha. Com esta atualização, o problema foi resolvido com a adição do manipulador PCI **shutdown()** que permite a execução segura do kernel. Como resultado, reinicializações repetidas usando **o kexec** nas plataformas EC2 Nitro da Amazon não falham mais.

(BZ#1758323)

Reinicializações repetidas usando a memória vPMEM como alvo de despejo agora funciona como esperado

Anteriormente, o uso da Memória Virtual Persistente (vPMEM) como alvo de despejo para **kdump** ou **fadump** fez com que o módulo **papr_scm** desmaiasse e refizesse a memória apoiada pelo vPMEM e readicionasse a memória em seu mapa linear.

Consequentemente, este comportamento desencadeou Chamadas de Hipervisor (HCalls) para o Hypervisor POWER. Como resultado, isto retarda consideravelmente a inicialização do kernel de captura e leva muito tempo para salvar o arquivo dump. Esta atualização corrige o problema e o processo de inicialização agora funciona como esperado no cenário descrito

(BZ#1792125)

Tentativa de adicionar a porta NIC do driver ICE a uma interface mestre de ligação do modo 5 não falha mais

Anteriormente, a tentativa de adicionar a porta NIC do driver **ICE** a um modo 5(**balance-tlb**) bonding master interface levou a uma falha com um erro **Master 'bond0', Slave 'ens1f0': Erro: Escravo falhou**. Conseqüentemente, você sofreu uma falha intermitente ao adicionar a porta NIC à interface mestre de colagem. Esta atualização corrige o problema e a adição da interface não falha mais.

(BZ#1791664)

6.2.7. Alta disponibilidade e clusters

Quando um sistema de arquivo GFS2 é usado com o agente de sistema de arquivos, a opção fast_stop agora tem como padrão não

Anteriormente, quando um sistema de arquivo GFS2 era usado com o agente do sistema de arquivos, a opção **fast_stop** era padronizada para **sim**. Este valor poderia resultar em eventos de cerca desnecessários devido ao tempo que pode levar para desmontar um sistema de arquivo GFS2. Com esta atualização, esta opção padrão é o **não**. Para todos os outros sistemas de arquivos, ela continua a padrão para **sim**.

(BZ#1814896)

fence_compute e fence_evacuate agents agora interpretam a opção insegura de uma maneira mais padrão

Anteriormente, o **fence_compute** e **fence_evacuate** agents trabalhavam como se **--insecura** fosse especificada por padrão. Com esta atualização, os clientes que não utilizam certificados válidos para seus cálculos ou serviços de evacuação devem definir **inseguro=verdadeiro** e usar a opção **--insecuro** ao executar manualmente a partir do CLI. Isto é consistente com o comportamento de todos os outros agentes.

(BZ#1830776)

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

Consumo otimizado da CPU pela libdb

Uma atualização anterior no banco de dados **da libdb** causou um consumo excessivo de CPU na rosca trickle. Com esta atualização, o uso da CPU foi otimizado.

(BZ#1670768)

O did_you_mean Ruby gem não contém mais um arquivo com uma licença não-comercial

Anteriormente, a jóia **did_you_mean** disponível no fluxo do módulo **ruby:2.5** continha um arquivo com uma licença não-comercial. Esta atualização remove o arquivo afetado.

(BZ#1846113)

nginx pode agora carregar certificados de servidor de fichas de segurança de hardware através do URI PKCS#11

A diretiva **ssl_certificate** do servidor web **nginx** suporta o carregamento de certificados de servidor TLS a partir de fichas de segurança de hardware diretamente dos módulos PKCS#11. Anteriormente, era impossível carregar certificados de servidor a partir de fichas de segurança de hardware através do URI PKCS#11.

(BZ#1668717)

6.2.9. Compiladores e ferramentas de desenvolvimento

O carregador dinâmico glibc não falha mais enquanto carrega uma biblioteca compartilhada que usa DT_FILTER e tem um construtor

Antes desta atualização, um defeito na implementação do carregador dinâmico de objetos compartilhados como filtros fez com que o carregador dinâmico falhasse ao carregar uma biblioteca compartilhada que usa um filtro e tem um construtor. Com este lançamento, a implementação do carregador dinâmico de filtros(**DT_FILTER**) foi corrigida para lidar corretamente com tais bibliotecas compartilhadas. Como resultado, o carregador dinâmico agora funciona como esperado no cenário mencionado.

(BZ#1812756)

glibc pode agora remover pseudo-montagens da lista getmntent()

O kernel inclui pseudo-entradas **automáticas** nas tabelas expostas ao espaço do usuário. Consequentemente, os programas que utilizam o **getmntent()** API vêem tanto as montagens regulares como estas pseudo-montagens na lista. As pseudo-montagens não correspondem a montagens reais, nem incluem informações válidas.

Com esta atualização, se a entrada de montagem tiver a opção **ignorar** montagem presente na configuração **automount(8**), a biblioteca **glibc** agora remove estas pseudo-montagens da lista **getmntent()**. Os programas que esperam o comportamento anterior têm que usar uma API diferente.

(BZ#1743445)

O padrão movv1qi não causa mais erros de compilação no código auto-vetorizado no IBM Z

Antes desta atualização, foram emitidas instruções de carga erradas para o padrão **movv1qi**. Como conseqüência, quando a auto-vetorização estava em vigor, uma miscompilação poderia ocorrer em sistemas IBM Z. Esta atualização corrige o padrão **movv1qi**, e como resultado, o código compila e roda corretamente agora.

(BZ#1784758)

PAPI_event_name_to_code() agora funciona corretamente em várias roscas

Antes desta atualização, o código interno do PAPI não tratava adequadamente da coordenação dos fios. Como conseqüência, quando múltiplas roscas usaram a operação **PAPI_nome_do_código()**, ocorreu uma condição de corrida e a operação falhou. Esta atualização melhora o manuseio de múltiplas

roscas no código interno do PAPI. Como resultado, o código multithreaded usando a operação **PAPI_event_name_to_code()** agora funciona corretamente.

(BZ#1807346)

Melhor desempenho para as funções de matemática glibc em sistemas IBM Power

Anteriormente, as funções matemáticas **da glibc** realizavam atualizações desnecessárias do status do ponto flutuante e chamadas de sistema nos sistemas IBM Power Systems, o que afetava negativamente o desempenho. Esta atualização remove a atualização desnecessária do status do ponto flutuante e melhora as implementações de: **ceil()**, **ceilf()**, **fegetmode()**, **fesetmode()**, **fesetenv()**, **fegetexcept()**, **feenableexcept()**, **fedisablexcept()**, **fegetround()** e **fesetround()**. Como resultado, o desempenho da biblioteca matemática é melhorado nos sistemas IBM Power.

(BZ#1783303)

As chaves de proteção de memória são agora suportadas pela IBM Power

Na IBM Power Systems, as interfaces da chave de proteção de memória **pkey_set** e **pkey_get** eram funções anteriormente stub, e conseqüentemente sempre falharam. Esta atualização implementa as interfaces, e como resultado, a Biblioteca C GNU**(glibc**) agora suporta chaves de proteção de memória em sistemas IBM Power.

Observe que as chaves de proteção de memória atualmente requerem a unidade de gerenciamento de memória baseada em hash (MMU), portanto você pode ter que inicializar certos sistemas com o parâmetro **desabilitar_radix** kernel.

(BZ#1642150)

papi-testsuite e papi-devel instalam agora o pacote de papi-libs necessário

Anteriormente, os pacotes **papi-teste** e **papi-devel** RPM não declaravam uma dependência do pacote **papi-libs** correspondente. Consequentemente, os testes falharam e os desenvolvedores não tinham a versão necessária da biblioteca compartilhada **papi** disponível para suas aplicações.

Com esta atualização, quando o usuário instala tanto a embalagem **papi-teste** quanto a embalagem **papi-devel**, a embalagem **papi-libs** também é instalada. Como resultado, o **papi-testsuite** agora tem a biblioteca correta permitindo que os testes sejam executados, e os desenvolvedores que usam **o papi-devel** têm seus executáveis ligados com a versão apropriada da biblioteca compartilhada **papi**.

(BZ#1664056)

A instalação dos pacotes lldb para arquiteturas múltiplas não leva mais a conflitos de arquivos

Anteriormente, os pacotes **lldb** instalavam arquivos dependentes de arquitetura em locais independentes da arquitetura. Como conseqüência, a instalação das versões 32-bit e 64-bit dos pacotes levou a conflitos de arquivos. Esta atualização empacota os arquivos em locais corretos dependentes da arquitetura. Como resultado, a instalação do **lldb** no cenário descrito se completa com sucesso.

(BZ#1841073)

getaddrinfo agora lida corretamente com uma falha na alocação de memória

Anteriormente, após uma falha na alocação de memória, a função **getaddrinfo** da **glibc** Biblioteca C GNU não liberava o contexto do resolvedor interno. Como conseqüência, **getaddrinfo** não foi capaz de recarregar o arquivo **/etc/resolv.conf** pelo resto da vida útil da linha de chamada, resultando em um

possível vazamento de memória.

Esta atualização modifica o caminho de tratamento de erros com uma operação de liberação adicional para o contexto do resolvedor. Como resultado, **getaddrinfo** reloads /**etc/resolv.conf** com novos valores de configuração mesmo após uma falha intermitente na alocação de memória.

(BZ#1810146)

glibc evita certas falhas causadas pela resolução de pedidos IFUNC

Anteriormente, a implementação das bibliotecas **librt** e **libpthread** da **glibc** Biblioteca GNU C continha os resolvedores de funções indiretas (IFUNC) para as seguintes funções: **clock_gettime**, **clock_getcpuclockid**, **clock_nanosleep**, **clock_settime**, **vfork**. Em alguns casos, os resolvedores IFUNC podiam executar antes que as bibliotecas **librt** e **libpthread** fossem realocadas. Conseqüentemente, as aplicações falhariam no carregador dinâmico **glibc** durante a inicialização inicial do programa.

Com este lançamento, as implementações destas funções foram movidas para o componente **libc** da **glibc**, o que impede que o problema descrito ocorra.

(BZ#1748197)

As falhas de asserção não ocorrem mais durante a criação do pthread_create

Anteriormente, a carregadeira dinâmica **glibc** não fazia roll back das mudanças no contador de identificação interno do módulo Thread Local Storage (TLS). Como conseqüência, uma falha de afirmação na função **pthread_create** podia ocorrer após a função **dlopen** ter falhado de certas maneiras. Com esta correção, o carregador dinâmico **glibc** atualiza o contador de identificação do módulo TLS em um momento posterior, depois que certas falhas não podem mais acontecer. Como resultado, as falhas de asserção não ocorrem mais.

(BZ#1774115)

glibc agora instala as dependências corretas para aplicações de 32 bits usando nss_db

Anteriormente, o pacote **nss_db.x86_64** não declarava as dependências do pacote **nss_db.i686**. Portanto, a instalação automatizada não instalava **o nss_db.i686** no sistema, apesar de ter um **glibc.i686** de 32 bits de ambiente instalado. Como conseqüência, aplicações de 32 bits usando **o nss_db** falharam em realizar buscas precisas no banco de dados do usuário, enquanto aplicações de 64 bits na mesma configuração funcionaram corretamente.

Com esta atualização, os pacotes **glibc** agora têm dependências fracas que acionam a instalação do pacote **nss_db.i686** quando ambos **glibc.i686** e **nss_db** são instalados no sistema. Como resultado, aplicações de 32 bits usando **o nss_db** agora funcionam corretamente, mesmo que o administrador do sistema não tenha instalado explicitamente o pacote **nss_db.i686**.

(BZ#1807824)

glibc locale informações atualizadas com o idioma Odia

O nome do estado indiano anteriormente conhecido como Orissa mudou para Odisha, e o nome de sua língua oficial mudou de Oriya para Odia. Com esta atualização, as informações da **glibc** locale refletem o novo nome do idioma.

(BZ#1757354)

Os subpacotes LLVM agora instalam arquivos dependentes de arco em locais dependentes de arco

Anteriormente, os sub pacotes LLVM instalavam arquivos dependentes de arquivos em locais independentes de arquivos. Isto resultou em conflitos ao instalar versões de 32 e 64 bits da LLVM. Com esta atualização, os arquivos de pacotes agora são instalados corretamente em locais dependentes de arquivos, evitando conflitos de versão.

(BZ#1820319)

Senha e pesquisa de grupo não falham mais na glibc

Anteriormente, o módulo **nss_compat** da biblioteca **glibc** substituía o status **errôneo** por códigos de erro incorretos durante o processamento das entradas de senha e grupo. Conseqüentemente, as aplicações não redimensionavam os buffers como esperado, fazendo com que as buscas por senha e grupo falhassem. Esta atualização corrige o problema, e as buscas agora são concluídas como esperado.

(BZ#1836867)

6.2.10. Gestão da Identidade

SSSD não baixa mais todas as regras com um caractere curinga por padrão

Anteriormente, a opção **ldap_sudo_include_regexp** era definida incorretamente como **verdadeira** por padrão. Como conseqüência, quando o SSSD começou a funcionar ou após a atualização das regras do SSSD, o SSSD baixou todas as regras que continham um caractere curinga(*) no atributo **sudoHost**. Esta atualização corrige o erro, e a opção **ldap_sudo_include_regexp** está agora corretamente definida como **falsa** por padrão. Como resultado, o problema descrito não ocorre mais.

(BZ#1827615)

a krb5 agora só solicita tipos de criptografia permitidos

Anteriormente, os tipos de criptografia permitidos especificados na variável **permitted_enctypes** no arquivo **/etc/krb5.conf** não se aplicavam aos tipos de criptografia padrão se os atributos **default_tgs_enctypes** ou **default_tkt_enctypes** não estivessem definidos. Conseqüentemente, os clientes Kerberos puderam solicitar conjuntos de cifras depreciadas como RC4, o que pode fazer com que outros processos falhem. Com esta atualização, os tipos de criptografia especificados na variável **permitted_enctypes** também se aplicam aos tipos de criptografia padrão, e somente os tipos de criptografia permitidos são solicitados.

O conjunto de cifras RC4, que foi depreciado no RHEL 8, é o tipo de criptografia padrão para usuários, serviços e trusts entre domínios do Active Directory (AD) em uma floresta AD.

- Para garantir suporte para tipos de criptografia AES forte entre domínios AD em uma floresta AD, consulte o AD DS: Segurança: Kerberos Erro de tipo "Unsupported etype" ao acessar um recurso em um artigo da Microsoft de domínio confiável.

- Para permitir o suporte para o tipo de criptografia RC4 depreciado em um servidor IdM para compatibilidade com AD, use o comando **update-crypto-policies --set DEFAULT:AD-SUPPORT**.

(BZ#1791062)

Os KDCs agora aplicam corretamente a política de senha vitalícia dos backends LDAP

Anteriormente, os Centros de Distribuição Kerberos (KDCs) que não são da IPA não garantiam o máximo de vida útil das senhas porque o backend LDAP da Kerberos aplicava as políticas de senhas de forma incorreta. Com esta atualização, o backend Kerberos LDAP foi corrigido, e os tempos de vida útil da senha se comportam como esperado.

(BZ#1784655)

Notificações de expiração de senha enviadas a clientes AD usando SSSD

Anteriormente, os clientes do Active Directory (não IdM) que usavam SSSD não recebiam avisos de expiração de senha devido a uma mudança recente na interface SSSD para adquirir as credenciais da Kerberos.

A interface Kerberos foi atualizada e os avisos de expiração agora são enviados corretamente.

(BZ#1820311)

O servidor de diretório não mais vaza memória ao usar definições COS indiretas

Anteriormente, após processar uma definição indireta de Classe de Serviço (COS), o Directory Server vazava memória para cada operação de busca que utilizava uma definição de COS indireta. Com esta atualização, o Servidor de Diretório libera todas as estruturas COS internas associadas à entrada do banco de dados após ter sido processado. Como resultado, o servidor não mais vaza memória ao usar definições de COS indireto.

(BZ#1816862)

A adição de anulações de ID de usuários AD agora funciona na IdM Web UI

Anteriormente, a adição de anulações de ID de usuários do Active Directory (AD) aos grupos de Gerenciamento de Identidade (IdM) no Default Trust View com o propósito de conceder acesso a funções de gerenciamento falhou ao usar a interface web do IdM. Esta atualização corrige o erro. Como resultado, agora você pode usar tanto a Web UI quanto a interface de linha de comando (CLI) do IdM neste cenário.

(BZ#1651577)

FreeRADIUS não gera mais certificados durante a instalação do pacote

Anteriormente, o FreeRADIUS gerava certificados durante a instalação do pacote, resultando nos seguintes problemas:

- Se o FreeRADIUS fosse instalado usando Kickstart, os certificados poderiam ser gerados em um momento em que a entropia no sistema fosse insuficiente, resultando em uma instalação falhada ou em um certificado menos seguro.
- A embalagem foi difícil de construir como parte de uma imagem, como um recipiente, porque a instalação da embalagem ocorre na máquina construtora em vez da máquina alvo. Todas as instâncias que são geradas a partir da imagem tinham a mesma informação de certificado.
- Era difícil para um usuário final gerar uma simples VM em seu ambiente, pois os certificados teriam que ser removidos e regenerados manualmente.

Com esta atualização, a instalação do FreeRADIUS não gera mais certificados CA autoassinados por padrão nem certificados CA subordinados. Quando o FreeRADIUS é lançado via **sistemad**:

- Se todos os certificados exigidos estiverem faltando, um conjunto de certificados padrão é gerado.
- Se um ou mais dos certificados esperados estiver presente, não gera novos certificados.

(BZ#1672285)

FreeRADIUS gera agora parâmetros Diffie-Hellman compatíveis com FIPS

Devido aos novos requisitos FIPS que não permitem que **o openssl** gere parâmetros Diffie-Hellman (dh) via **dhparam**, a geração de parâmetros dh foi removida dos scripts de bootstrap do FreeRADIUS e o arquivo, **rfc3526-group-18-8192.dhparam**, está incluído com os pacotes FreeRADIUS para todos os sistemas, e assim permite que o FreeRADIUS inicie no modo FIPS.

Observe que você pode personalizar **/etc/raddb/certs/bootstrap** e **/etc/raddb/certs/Makefile** para restaurar a geração de parâmetros DH, se necessário.

(BZ#1859527)

Atualização do Healthcheck agora atualiza corretamente tanto o ipa-healthcheck-core quanto o ipa-healthcheck

Anteriormente, a entrada do **yum update healthcheck** não atualizava o pacote **ipa-healthcheck**, mas o substituía pelo pacote **ipa-healthcheck-core**. Como conseqüência, o comando **ipa-healthcheck** não funcionava após a atualização.

Esta atualização corrige o bug, e a atualização do **ipa-healthcheck** agora atualiza corretamente tanto o pacote **ipa-healthcheck** quanto o pacote **ipa-healthcheck-core**. Como resultado, a ferramenta **Healthcheck** funciona corretamente após a atualização.

(BZ#1852244)

6.2.11. Infra-estruturas gráficas

Os laptops com GPUs híbridas Nvidia podem agora retomar com sucesso a partir de suspensão

Anteriormente, o **novo** driver gráfico às vezes não conseguia ligar as GPUs híbridas Nvidia em certos laptops a partir do modo de economia de energia. Como resultado, os laptops não conseguiram retomar a suspensão.

Com esta atualização, vários problemas no sistema de Gerenciamento de Energia em Tempo de Execução**(runpm**) foram resolvidos. Como resultado, os laptops com gráficos híbridos podem agora ser retomados com sucesso a partir da suspensão.

(JIRA:RHELPLAN-57572)

6.2.12. Virtualização

Migração de máquinas virtuais com o modelo padrão de CPU agora funciona de forma mais confiável

Anteriormente, se uma máquina virtual (VM) fosse criada sem um modelo de CPU específico, QEMU utilizava um modelo padrão que não era visível para o serviço **libvirt**. Como conseqüência, era possível migrar a VM para um host que não suportava o modelo padrão de CPU da VM, o que às vezes causava falhas e comportamento incorreto no sistema operacional convidado após a migração.

Com esta atualização, **a libvirt** usa explicitamente o modelo **qemu64** como padrão na configuração XML da VM. Como resultado, se o usuário tentar migrar uma VM com o modelo padrão da CPU para um host que não suporta esse modelo, **a libvirt** gera corretamente uma mensagem de erro.

Observe, entretanto, que a Red Hat recomenda fortemente o uso de um modelo de CPU específico para suas VMs.

(JIRA:RHELPLAN-45906)

6.2.13. Contêineres

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. O comando **update-crypto-policies --set FIPS** não é mais necessário com esta correção.

(BZ#1804193)

6.3. ANTEVISÕES TECNOLÓGICAS

Esta parte fornece uma lista de todas as Análises de Tecnologia disponíveis no Red Hat Enterprise Linux 8.3.

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

6.3.1. Trabalho em rede

Ativado o módulo Netfilter xt_u32

O módulo Netfilter **xt_u32** está agora disponível no **módulo kernel-modules-extra** rpm. Este módulo ajuda no encaminhamento de pacotes com base nos dados que são inacessíveis a outros filtros de pacotes baseados em protocolos e assim facilita a migração manual para **nftables**. Entretanto, o módulo Netfilter **xt_u32** não é suportado pela Red Hat.

(BZ#1834769)

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)

Características do XDP que estão disponíveis como Technology Preview

A Red Hat fornece o uso dos seguintes recursos do eXpress Data Path (XDP) como uma visualização tecnológica não suportada:

- Carregamento de programas XDP em arquiteturas que não AMD e Intel 64 bits. Note que a biblioteca **libxdp** não está disponível para outras arquiteturas além da AMD e Intel 64-bit.
- Os códigos de retorno **XDP_TX** e **XDP_REDIRECT**.
- A descarga de hardware do XDP. Antes de utilizar este recurso, consulte Descarregando programas XDP em placas de rede Netronome que utilizam o driver **nfp** falham.

(BZ#1889737)

móduloact_mpls disponível como uma Pré-visualização Tecnológica

O módulo **act_mpls** está agora disponível no **módulo kernel-modules-extra** rpm como uma Visualização de Tecnologia. O módulo permite a aplicação de ações de Comutação de Etiquetas Multiprotocolo (MPLS) com filtros de Controle de Tráfego (TC), por exemplo, entradas de empilhamento de etiquetas MPLS push e pop com filtros TC. O módulo também permite que os campos Label, Traffic Class, Bottom of Stack e Time to Live sejam definidos independentemente.

(BZ#1839311)

O TCP Multipath está agora disponível como uma Pré-visualização Tecnológica

Multipath TCP (MPTCP), uma extensão do TCP, está agora disponível como uma Pré-visualização Tecnológica. O MPTCP melhora o uso de recursos dentro da rede e a resiliência a falhas na rede. Por exemplo, com o Multipath TCP no servidor RHEL, os smartphones com MPTCP v1 habilitado podem se conectar a uma aplicação rodando no servidor e alternar entre Wi-Fi e redes celulares sem interromper a conexão ao servidor.

Note que ou as aplicações rodando no servidor devem suportar nativamente MPTCP ou os administradores devem carregar um programa **eBPF** no kernel para mudar dinamicamente **IPPROTO_TCP** para **IPPROTO_MPTCP**.

Para mais detalhes veja, Começando com o Multipath TCP.

(JIRA:RHELPLAN-41549)

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 resolvedor de stub DNS de cache e validação, uma Resolução de nomes Multicast local (LLMNR) e um resolvedor 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)

6.3.2. Kernel

O recurso de reinicialização rápida do kexec está disponível como Technology Preview

O recurso de **reinicialização rápida do kexec** continua a estar disponível como uma Pré-visualização tecnológica. A **reinicialização rápida do kexec** acelera significativamente o processo de inicialização, permitindo que o kernel inicialize diretamente no segundo kernel sem passar primeiro pelo Sistema Básico de Entrada/Saída (BIOS). Para usar este recurso:

1. Carregar manualmente o **kexec** kernel.
2. Reinicializar 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:

- **bpftrace**, uma linguagem de rastreamento de alto nível que utiliza a máquina virtual **eBPF**.
- **AF_XDP**, um soquete para conectar o caminho **eXpress Data Path (XDP)**ao espaço do usuário para aplicações que priorizam o desempenho do processamento de pacotes.

(BZ#1559616)

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)

6.3.3. 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, 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.

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. Você pode usar apenas a configuração padrão do motor de contêiner: 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 não são considerados estáveis, e podem mudar 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.
- Para determinar se um sistema de arquivo XFS existente é elegível para uso como uma sobreposição, use o seguinte comando e veja se a opção **ftype=1** está habilitada:

```
# xfs_info /mount-point | grep ftype
```

- As etiquetas de segurança SELinux são habilitadas por padrão em todos os motores de contêineres suportados com OverlayFS.
- Vários problemas conhecidos estão 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.

Para mais informações sobre OverlayFS, veja a 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 8.3 atualiza Stratis para a versão 2.1.0. Para mais informações, consulte as Notas de Lançamento do Stratis 2.1.0.

(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 conseqüência, 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)

6.3.4. Alta disponibilidade e clusters

Versão em modo local do comando de configuração de clusters pcs disponível como uma pré-visualização tecnológica

Por padrão, o comando de **configuração do cluster pcs** sincroniza automaticamente todos os arquivos de configuração com os nós do cluster. No Red Hat Enterprise Linux 8.3, o comando de **configuração do cluster pcs** fornece a opção **--corosync-conf** como uma prévia da tecnologia. Especificar esta opção muda o comando para o modo **local**. Neste modo, **o pcs** cria um arquivo **corosync.conf** e o salva em um arquivo especificado apenas no nó local, sem se comunicar com nenhum outro nó. Isto permite criar um arquivo **corosync.conf** em um script e manipular esse arquivo por meio do script.

(BZ#1839637)

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)

6.3.5. 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)

6.3.6. 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 conseqüência, 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#1667225, BZ#1667516)

O desktop GNOME na IBM Z está disponível como Technology Preview

O desktop do GNOME, incluindo o navegador Firefox, está agora disponível como Technology Preview na arquitetura IBM Z. Agora você pode se conectar a uma sessão gráfica remota rodando GNOME usando VNC para configurar e gerenciar seus servidores IBM Z.

(JIRA:RHELPLAN-27737)

6.3.7. 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)

Gráficos da Intel Tiger Lake disponíveis como uma prévia tecnológica

Os gráficos UP3 e UP4 Xe da Intel Tiger Lake estão agora disponíveis como uma Pré-visualização Tecnológica.

Para permitir a aceleração de hardware com gráficos Intel Tiger Lake, adicione a seguinte opção na linha de comando do kernel:

```
i915.force_probe=pci-id
```

Nesta opção, substitua *pci-id* por uma das seguintes opções:

- A ID PCI de sua GPU Intel
- O caracter ***** para habilitar o driver **i915** com todo o hardware de qualidade alfa

(BZ#1783396)

6.3.8. 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)

6.3.9. Virtualização

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)

Criando máquinas virtuais aninhadas

A virtualização da KVM aninhada é fornecida como uma Pré-visualização Tecnológica para máquinas virtuais KVM (VMs) rodando em sistemas AMD64 e IBM Z com RHEL 8. Com este recurso, uma VM RHEL 7 ou RHEL 8 que roda em um host físico RHEL 8 pode atuar como um hipervisor, e hospedar suas próprias VMs.

Note que no RHEL 8.2 e posteriores, a virtualização aninhada é totalmente suportada para VMs rodando em um host Intel 64.

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

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 **iavf**. 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)

6.3.10. Contêineres

a imagem do contêiner **podman** está disponível como uma Technology Preview

A imagem do container **register.redhat.io/rhel8/podman** é uma implementação contentorizada do pacote **podman**. A ferramenta **podman** é utilizada para gerenciar recipientes e imagens, volumes montados nesses recipientes e cápsulas feitas a partir de grupos de recipientes. Podman é baseado na biblioteca **libpod** para o gerenciamento do ciclo de vida dos contêineres. A biblioteca **libpod** fornece APIs para o gerenciamento de recipientes, pods, imagens de recipientes e volumes. Esta imagem de container permite criar, modificar e executar imagens de container sem a necessidade de instalar o pacote **podman** em seu sistema. O caso de uso não cobre a execução desta imagem no modo rootless como um usuário não-root. Para puxar a imagem do contêiner **Registry.redhat.io/rhel8/podman**, você precisa de uma assinatura ativa do Red Hat Enterprise Linux.

(BZ#1627899)

crun está disponível como uma Pré-visualização Tecnológica

O **crun** OCI foi adicionado ao módulo **container-rools:rhl8**. A **crun** fornece um acesso para rodar com o cgoupsV2. O **crun** suporta uma anotação que permite que o container acesse os grupos adicionais de usuários sem raiz. Isto é útil para a montagem do volume em um diretório ao qual o usuário só tem acesso em grupo, ou o diretório é colocado no mesmo.

(BZ#1841438)

6.4. FUNCIONALIDADE DEPRECIADA

Esta parte fornece uma visão geral da funcionalidade que tem sido *deprecated* no Red Hat Enterprise Linux 8.

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 .

6.4.1. 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)

lorax-composer back end para Image Builder é depreciado em RHEL 8

O anterior back end **lorax-composer** para Image Builder é considerado depreciado. Ele só receberá correções selecionadas para o resto do ciclo de vida do Red Hat Enterprise Linux 8 e será omitido de futuros lançamentos principais. A Red Hat recomenda que você desinstale o **lorax-composer** e instale **osbuild-composer** back end em seu lugar.

Consulte Composição de uma imagem personalizada do sistema RHEL para obter mais detalhes.

(BZ#1893767)

6.4.2. 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)

6.4.3. Serviços de infra-estrutura

ocarteiro é depreciado

Com esta atualização, os pacotes de **correio** foram marcados como depreciados e não estarão disponíveis nos futuros grandes lançamentos do Red Hat Enterprise Linux.

(BZ#1890976)

6.4.4. 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 garantir uma transição suave das implementações que dependem das cifras SEED quando o NSS remover o suporte, a Red Hat recomenda habilitar o suporte para outras suítes de cifras.

Observe que as cifras SEED já estão desabilitadas 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)

6.4.5. 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)

6.4.6. 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 propenso 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)

6.4.7. 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)

a peripécia é depreciada

O pacote de **peripécia** é depreciado desde o RHEL 8.3.

O sistema de notificação de eventos de armazenamento Peripety daemon parses registra em eventos de armazenamento estruturado. Ele o ajuda a investigar problemas de armazenamento.

(BZ#1871953)

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)

6.4.8. Gestão da Identidade

oopenssh-ldap foi depreciado

O subpacote **openssh-ldap** foi depreciado no Red Hat Enterprise Linux 8 e será removido no RHEL 9. Como o subpacote **openssh-ldap** não é mantido a montante, a Red Hat recomenda o uso do SSSD e do helper **sss_ssh_authorizedkeys**, que se integram melhor com outras soluções IdM e são mais seguros.

Por padrão, os provedores SSSD **ldap** e **ipa** lêem o atributo **sshPublicKey** LDAP do objeto do usuário, se disponível. Note que você não pode usar a configuração padrão do SSSD para o provedor de **anúncios** ou domínios confiáveis do IdM para recuperar chaves públicas SSH do Active Directory (AD), uma vez que o AD não tem um atributo LDAP padrão para armazenar uma chave pública.

Para permitir que o ajudante de **chaves autorizadas sss_ssh_authorizedkeys** obtenha a chave do SSSD, habilite o ajudante **ssh** adicionando **ssh** à opção de **serviços** no arquivo **sssd.conf**. Veja a página de manual **sssd.conf(5)** para detalhes.

Para permitir que **o sshd** utilize **sss_ssh_authorizedkeys**, adicione o arquivo **/usr/bin/ssh_authorizedkeys** e **AuthorizedKeysCommandUser nobody** options ao arquivo **/etc/ssh/sshd_config** como descrito pela página de manual **sss_ssh_authorizedkeys(1)**.

(BZ#1871025)

Os tipos de criptografia DES e 3DES foram removidos

Devido a razões de segurança, o algoritmo Data Encryption Standard (DES) foi depreciado e desativado por padrão desde o RHEL 7. Com o recente rebase dos pacotes Kerberos, os tipos de criptografia de um-DES (DES) e de três-DES (3DES) foram removidos do RHEL 8.

Se você tiver configurado serviços ou usuários para usar somente a criptografia DES ou 3DES, você poderá sofrer interrupções de serviço como, por exemplo:

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

Realizar as seguintes ações para se preparar para a atualização:

1. Verifique se seu KDC usa criptografia DES ou 3DES com os scripts Python de código aberto **krb5check**. Veja krb5check no GitHub.
2. Se você estiver usando a criptografia DES ou 3DES com quaisquer diretores Kerberos, digite-os novamente com um tipo de criptografia suportada, como a AES (Advanced Encryption Standard). Para instruções de re-keying, veja Retirada de DES da Documentação do MIT Kerberos.
3. Teste a independência do DES e 3DES definindo temporariamente as seguintes opções Kerberos antes da atualização:
   a. In **/var/kerberos/krb5kdc/kdc.conf** sobre o KDC, definir os **tipos_apoiados** e não incluir **des** ou **des3**.
   b. Para cada host, em **/etc/krb5.conf** e quaisquer arquivos em **/etc/krb5.conf.d**, defina **allow_weak_crypto** para **falso**. É falso por padrão.
   c. Para cada host, em **/etc/krb5.conf** e quaisquer arquivos em **/etc/krb5.conf.d**, defina os **tipos_permitidos**, os **tipos_tgs_padrão**, e os **tipos_tkt_padrão** e não inclua **des** ou **des3**.
4. Se você não experimentar nenhuma interrupção de serviço com as configurações de teste Kerberos da etapa anterior, remova-as e atualize. Você não precisa dessas configurações após atualizar para os pacotes mais recentes do Kerberos.

(BZ#1877991)

6.4.9. 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)

6.4.10. 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)

6.4.11. 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)

6.4.12. Funções do Sistema Red Hat Enterprise Linux

O pacote **geoipupdate** foi depreciado

O pacote **geoipupdate** requer uma assinatura de terceiros e também baixa conteúdo proprietário. Portanto, o pacote **geoipupdate** foi depreciado, e será removido na próxima grande versão da RHEL.

(BZ#1874892)

6.4.13. 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 conseqüência, 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 SPICE foi depreciado

No RHEL 8.3, o protocolo de exibição remota SPICE foi depreciado. Note que o SPICE permanecerá compatível com o RHEL 8, mas a Red Hat recomenda o uso de soluções alternativas para o fluxo de exibição remota:

- Para acesso ao console remoto, use o protocolo VNC.
- Para funções avançadas de exibição remota, use ferramentas de terceiros como RDP, HP RGS, ou Mechdyne TGX.

(BZ#1849563)

6.4.14. Contêineres

Podman varlink baseado em REST API V1 foi depreciado

O Podman REST API V1 baseado em varlink foi depreciado a montante em favor do novo Podman REST API V2. Esta funcionalidade será removida em um lançamento posterior do Red Hat Enterprise Linux 8.

(JIRA:RHELPLAN-60226)

6.4.15. 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
- lorax-composer
- mercurial
- net-tools
- textos em rede
- nss-pam-ldapd
- sendmail
- yp-tools
- ypbind
- ypserv

6.5. PROBLEMAS CONHECIDOS

Esta parte descreve questões conhecidas no Red Hat Enterprise Linux 8.3.

6.5.1. 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 conseqüência, 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)

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 novo back end osbuild-composer não reproduz o estado da planta do lorax-composer em atualizações

Os usuários do Image Builder que estão atualizando do back end **lorax-composer** para o novo back end **osbuild-composer**, as plantas podem desaparecer. Como resultado, uma vez concluída a atualização, as plantas não são exibidas automaticamente. Para contornar este problema, execute os seguintes passos.

Pré-requisitos

- Você tem o utilitário **composer-cli** CLI instalado.

Procedimento

1. Execute o comando para carregar os projetos anteriores baseados em **lorax-compositor** na nova extremidade traseira do **osbuild-compositor**:

```
$ para o projeto em $(find /var/lib/lorax/composer/blueprints/git/ workspace/master -name
'*.toml'); faça o composer-cli blueprints empurrar {{{blueprint}\i1}(find
```

```
/var/lib/lorax/composer/blueprints/git/ workspace/master -name '*.toml'); faça o composer-cli blueprints empurrar
```

Como resultado, as mesmas plantas estão agora disponíveis na parte traseira do **osbuild-composer**.

Recursos adicionais

- Para mais detalhes sobre esta edição conhecida, veja os projetos do Image Builder não estão mais presentes após uma atualização do artigo 8.3 do Red Hat Enterprise Linux .

(BZ#1897383)

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=
```

(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

Desde a 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 conseqüência, 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)

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)

O instalador RHEL não inicia quando as interfaces de rede InfiniBand são configuradas usando as opções de inicialização do instalador

Quando você configura as interfaces de rede InfiniBand em um estágio inicial da instalação da RHEL usando as opções de inicialização do instalador (por exemplo, para baixar a imagem do instalador usando o servidor PXE), o instalador falha ao ativar as interfaces de rede.

Este problema ocorre porque o RHEL NetworkManager não reconhece as interfaces de rede no modo InfiniBand e, em vez disso, configura as conexões Ethernet para as interfaces.

Como resultado, a ativação da conexão falha, e se a conectividade sobre a interface InfiniBand for necessária em um estágio inicial, o instalador RHEL não inicia a instalação.

Para resolver este problema, crie uma nova mídia de instalação incluindo os pacotes Anaconda e NetworkManager atualizados, usando a ferramenta Lorax.

Para mais informações sobre a criação de uma nova mídia de instalação incluindo os pacotes Anaconda e NetworkManager atualizados, usando a ferramenta Lorax, veja Unable to install Red Hat Enterprise Linux 8.3.0 com interfaces de rede InfiniBand

(BZ#1890261)

A instalação do Anaconda falha quando o espaço de nomes do dispositivo NVDIMM é ajustado para o modo devdax.

A instalação do Anaconda falha com um trackback após a inicialização com o namespace do dispositivo NVDIMM ajustado para o modo **devdax** antes da instalação da GUI.

Para solucionar este problema, reconfigure o dispositivo NVDIMM para ajustar o espaço de nomes para um modo diferente do modo **devdax** antes do início da instalação. Como resultado, você pode prosseguir com a instalação.

(BZ#1891827)

A fonte de instalação da **mídia local** não é detectada ao iniciar a instalação a partir de um USB que é criado usando uma ferramenta de terceiros

Ao iniciar a instalação RHEL a partir de um USB que é criado usando uma ferramenta de terceiros, o instalador não detecta a fonte de instalação **Local Media** (apenas 'Red Hat CDN' é detectado).

Este problema ocorre porque a opção de inicialização padrão **int.stage2=** tenta procurar pelo formato de imagem **iso9660**. Entretanto, uma ferramenta de terceiros pode criar uma imagem ISO com um formato diferente.

Como alternativa, use uma das seguintes soluções:

- Ao iniciar a instalação, clique na tecla **Tab** para editar a linha de comando do kernel, e mude a opção boot **inst.stage2=** para **inst.repo=**.
- Para criar um dispositivo USB inicializável no Windows, use o Fedora Media Writer.
- Ao usar uma ferramenta de terceiros como a Rufus para criar um dispositivo USB inicializável, primeiro regenere a imagem ISO RHEL em um sistema Linux, e depois use a ferramenta de terceiros para criar um dispositivo USB inicializável.

Para mais informações sobre as etapas envolvidas na execução de qualquer uma das tarefas especificadas, veja, A mídia de instalação não é detectada automaticamente durante a instalação do RHEL 8.3

(BZ#1877697)

O Anaconda agora mostra um diálogo para discos DASD **ldl** ou sem formatação em modo texto

Anteriormente, durante uma instalação em modo texto, o Anaconda não mostrava um diálogo para o layout de discos Linux**(ldl**) ou discos sem formatação do Dispositivo de Armazenamento Direct-Access (DASD). Como resultado, os usuários não puderam utilizar esses discos para a instalação.

Com esta atualização, em modo texto o Anaconda reconhece discos DASD **ldl** e não formatados e mostra um diálogo onde os usuários podem formatá-los adequadamente para a utilização futura da instalação.

(BZ#1874394)

6.5.2. 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)

6.5.3. Serviços de infra-estrutura

libmaxminddb-devel-debuginfo.rpm é removido ao executar a **atualização dnf**

Ao executar o comando de **atualização dnf**, a ferramenta **mmdblookup** binária é movida do subpacote **libmaxminddb-devel** para o pacote principal da **libmaxmindb**. Consequentemente, a **libmaxminddb-devel-debuginfo.rpm** é removida, o que pode criar um caminho de atualização quebrado para este pacote. Para contornar este problema, remova a **libmaxminddb-devel-debuginfo** antes da execução do comando de **atualização do dnf**.

Nota: **libmaxminddb-debuginfo** é o novo pacote de **debuginfo**.

(BZ#1642001)

6.5.4. Segurança

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. Consequentemente, 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)

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)

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)

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)

As permissões de arquivo de /etc/passwd- não estão alinhadas com o Benchmark CIS RHEL 8 1.0.0

Devido a um problema com o CIS Benchmark, a remediação da regra SCAP que garante permissões no arquivo de backup **/etc/passwd-** configura as permissões para **0644**. Entretanto, o **Benchmark 1.0.0 do CIS Red Hat Enterprise Linux 8** requer as permissões do arquivo **0600** para esse arquivo. Como consequência, as permissões do arquivo **/etc/passwd-** não estão alinhadas com o benchmark após a remediação.

(BZ#1858866)

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)

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)

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 no modo FIPS aceita apenas parâmetros D-H específicos

No modo FIPS, os clientes do Transport Security Layer (TLS) que utilizam OpenSSL retornam um erro de **valor dh ruim** e abortam as conexões TLS a servidores que utilizam parâmetros gerados manualmente. Isto porque OpenSSL, quando configurado para trabalhar em conformidade com FIPS 140-2, trabalha somente com parâmetros D-H em conformidade com NIST SP 800-56A rev3 Apêndice D (grupos 14, 15, 16, 17 e 18 definidos na RFC 3526 e com grupos definidos na RFC 7919). Além disso, os servidores que utilizam OpenSSL ignoram todos os outros parâmetros e selecionam parâmetros conhecidos de tamanho semelhante. Para contornar este problema, use apenas os grupos compatíveis.

(BZ#1810911)

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 conseqüência, 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)

o serviçosystemd não pode executar comandos a partir de caminhos arbitrários

O serviço **systemd** não pode executar comandos de **/home/user/bin** caminhos arbitrários porque o pacote de políticas da SELinux não inclui nenhuma regra desse tipo. Conseqüentemente, os serviços personalizados que são executados em caminhos que não são do sistema falham e eventualmente

registram as mensagens de auditoria de negação de acesso ao Cache Vetor (AVC) quando o SELinux nega o acesso. Para contornar este problema, faça uma das seguintes ações:

- Executar o comando usando um script **shell** com a opção **-c**. Por exemplo,

  ```
  bash -c command
  ```

- Executar o comando a partir de um caminho comum usando **/bin**, **/sbin**, **/usr/sbin**, **/usr/local/bin**, e **/usr/local/sbin** diretórios comuns.

(BZ#1860443)

rpm_verify_permissions fails in the CIS profile

A regra **rpm_verify_permissions** compara as permissões de arquivo com as permissões padrão de pacote. Entretanto, o perfil do Centro de Segurança da Internet (CIS), que é fornecido pelos pacotes **scap-security-guide**, altera algumas permissões de arquivo para ser mais rígido do que o padrão. Como conseqüência, a verificação de certos arquivos usando **rpm_verify_permissions** falha.

Para contornar este problema, verifique manualmente se estes arquivos têm as seguintes permissões:

- **/etc/cron.d** (0700)
- **/etc/cron.hourly** (0700)
- **/etc/cron.mensal** (0700)
- **/etc/crontab** (0600)
- **/etc/cron.semanal** (0700)
- **/etc/cron.daily** (0700)

(BZ#1843913)

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)

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)

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)

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, selecionando o grupo de pacotes *Server with GUI* durante a instalação de um sistema com perfis baseados em OSPP ou OSPP, por exemplo, o Guia de Implementação Técnica de Segurança (STIG), o OpenSCAP exibe um aviso de que o grupo de pacotes selecionado não é compatível com a política de segurança. 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 OSPP e os 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)

Instalação com o Servidor com seleção de software GUI ou Workstation e perfil de segurança CIS não é possível

O perfil de segurança do CIS não é compatível com o **Servidor com** seleção de software **GUI** e **Workstation**. Como consequência, não é possível uma instalação RHEL 8 com o **Servidor** com seleção de software de **GUI** e perfil CIS. Uma tentativa de instalação usando o perfil do CIS e qualquer uma destas seleções de software irá gerar a mensagem de erro:

> o pacote xorg-x11-server-common foi adicionado à lista de pacotes excluídos, mas ele não pode ser removido da seleção de software atual sem quebrar a instalação.

Para contornar o problema, não utilize o perfil de segurança do CIS com o **Servidor com GUI** ou com as seleções de software da **estação de trabalho**.

(BZ#1843932)

Regras corretivas relacionadas a serviços durante instalações de kickstart podem falhar

Durante uma instalação de kickstart, o utilitário OpenSCAP às vezes mostra incorretamente que um serviço **habilita** ou **desabilita** a correção do estado não é necessário. Conseqüentemente, o OpenSCAP pode colocar os serviços no sistema instalado em um estado não-conforme. Como alternativa, você pode escanear e remediar o sistema após a instalação do kickstart. Isto corrigirá os problemas relacionados aos serviços.

(BZ#1834716)

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 políticas criptográficas permitem incorretamente a utilização de cifras de Camellia

As políticas criptográficas do sistema RHEL 8 devem desativar as cifras de Camellia em todos os níveis de políticas, conforme declarado na documentação do produto. Entretanto, o protocolo Kerberos habilita as cifras por padrão.

Para contornar o problema, aplique a subpolítica **NO-CAMELLLIA**:

```
# update-crypto-policies --set DEFAULT:NO-CAMELLLIA
```

No comando anterior, substitua **DEFAULT** pelo nome de nível criptográfico se você tiver trocado de **DEFAULT** anteriormente.

Como resultado, as cifras Camellia são corretamente proibidas em todas as aplicações que utilizam políticas de criptografia em todo o sistema somente quando você as desabilita por meio da solução de trabalho.(BZ#1919155)

6.5.5. Trabalho em rede

O utilitário iptables agora solicita o carregamento de módulos para comandos que atualizam uma cadeia, independentemente da bandeira NLM_F_CREATE

Anteriormente, ao definir a política de uma cadeia, o utilitário **iptables-nft** gerava uma mensagem **NEWCHAIN**, mas não colocava a bandeira **NLM_F_CREATE**. Como conseqüência, o kernel RHEL 8 não carregou nenhum módulo e o comando de corrente de atualização resultante falhou se os módulos do kernel associados não foram carregados manualmente. Com esta atualização, o utilitário **iptables-nft**

agora solicita o carregamento de módulos para todos os comandos que atualizam uma cadeia e os usuários são capazes de definir a política de uma cadeia usando o utilitário **iptables-nft** sem carregar manualmente os módulos associados.

(BZ#1812666)

O suporte para atualização de contadores de pacotes/bytes no kernel foi alterado incorretamente entre o RHEL 7 e o RHEL 8

Ao se referir a um comando **ipset** com contadores habilitados a partir de uma regra **iptables**, que especifica restrições adicionais sobre entradas **ipset** correspondentes, os contadores **ipset** são atualizados somente se todas as restrições adicionais corresponderem. Isto também é problemático com restrições **--packets-gt** ou **--bytes-gt**.

Como resultado, ao migrar um conjunto de regras **iptables** da RHEL 7 para a RHEL 8, as regras que envolvem as pesquisas **ipset** podem parar de funcionar e precisam ser ajustadas. Para contornar este problema, evite usar as opções **--packets-gt** ou **--bytes-gt** e substitua-as pelas opções **--packets-lt** ou **--bytes-lt**.

(BZ#1806882)

O descarregamento de programas XDP falha nos cartões de rede Netronome que utilizam o driver nfp

O driver **nfp** para cartões de rede Netronome contém um bug. Portanto, a descarga dos programas eXpress Data Path (XDP) falha se você usar tais cartões e carregar o programa XDP usando a função **IFLA_XDP_EXPECTED_FD** com a bandeira **XDP_FLAGS_REPLACE**. Por exemplo, este bug afeta os programas XDP que são carregados usando a biblioteca **libxdp**. Atualmente, não há nenhuma solução disponível para o problema.

(BZ#1880268)

O Anaconda não tem acesso à rede quando utiliza DHCP na opção de inicialização do ip

O disco RAM inicial**(initrd**) utiliza o NetworkManager para gerenciar a rede. O módulo NetworkManager **dracut** fornecido pelo arquivo ISO RHEL 8.3 assume incorretamente que o primeiro campo da opção **ip** nas opções de inicialização do Anaconda está sempre definido. Como conseqüência, se você usar DHCP e definir **ip=:**::::

Você tem as seguintes opções para contornar o problema:

1. Defina o primeiro campo na **opção ip` para `.** (período):

   ```
   ip=::::
   ```

   Note que este trabalho não funcionará em versões futuras da RHEL quando o problema tiver sido resolvido.

2. Recriar o arquivo **boot.iso** usando os últimos pacotes do repositório BaseOS que contém uma correção para o bug: .

```
# lorax '--product=Red Hat Enterprise Linux' --version=8.3 --release=8.3 \
    --source=<URL_to_BaseOS_repository> \
    --source=<URL_to_AppStream_repository> \
    --nomacboot --buildarch=x86_64 '--volid=RHEL 8.3' <output_directory>
```

. Note que a Red Hat não suporta arquivos ISO auto-criados.

Como resultado, a RHEL recupera um endereço IP do servidor DHCP, e o acesso à rede está disponível no Anaconda.

(BZ#1902791)

6.5.6. Kernel

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)

O kernel retorna falsos avisos positivos nos sistemas IBM Z

No RHEL 8, os sistemas IBM Z estão faltando uma entrada de lista branca para a zona de memória **ZONE_DMA** para permitir o acesso do usuário. Consequentemente, o kernel retorna avisos falsos positivos, tais como:

```
...
Bad or missing usercopy whitelist? Kernel memory exposure attempt detected from SLUB object
'dma-kmalloc-192' (offset 0, size 144)!
WARNING: CPU: 0 PID: 8519 at mm/usercopy.c:83 usercopy_warn+0xac/0xd8
...
```

Os avisos aparecem ao acessar certas informações do sistema através da interface **sysfs**. Por exemplo, ao executar o script **de debuginfo.sh**.

Para contornar este problema, adicione o parâmetro **hardened_usercopy=off** à linha de comando do kernel.

Como resultado, nenhuma mensagem de advertência é exibida no cenário descrito.

(BZ#1660290)

A espera ocupada do serviço rngd causa o consumo total da CPU no modo FIPS

Uma nova fonte de entropia do kernel para o modo FIPS foi adicionada para kernels a partir da versão 4.18.0-193.10. Conseqüentemente, quando em modo FIPS, o serviço **rngd** ocupado espera na chamada do sistema de **pesquisa()** para o dispositivo **/dev/random**, causando assim um consumo de 100% do tempo da CPU. Para contornar este problema, pare e desabilite **o rngd** executando:

```
# systemctl stop rngd
# systemctl disable rngd
```

Como resultado, **a rngd** não está mais ocupada aguardando a **votação()** no cenário descrito.

(BZ#1884857)

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 poucoendiana do IBM Power System executa o RHEL 8.
- O serviço **kdump** ou **fadump** está habilitado no sistema.

Consequentemente, 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 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 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 conseqüência, 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 conseqüência, 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)

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 freqüência 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. Consequentemente, 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 valor de impressão padrão 7 4 1 7 às vezes causa a falta de resposta temporária do sistema

O valor padrão **7 4 1 7printk** permite uma melhor depuração da atividade do kernel. Entretanto, quando acoplado a um console serial, esta configuração de **impressão** pode causar explosões intensas de E/S que podem fazer com que um sistema RHEL se torne temporariamente não responsivo. Para contornar este problema, adicionamos um novo perfil TuneD do **console serial de otimização**, que reduz o valor padrão da **impressão** para **4 4 1 7**. Os usuários podem instrumentar seu sistema da seguinte forma:

```
# perfil tuned-adm profile throughput performance optimize-console de série
```

Ter um valor de **impressão** mais baixo persistente durante uma reinicialização reduz a probabilidade de que o sistema fique pendurado.

Observe que esta mudança de configuração vem às custas da perda de informações extras de depuração.

Para mais informações sobre o recurso recém-adicionado, veja Um novo perfil TuneD de **otimização-console serial** para reduzir E/S para consoles seriais, baixando o valor da **impressão** .

(JIRA:RHELPLAN-28940)

O driver do kernel ACPI informa que não tem acesso a uma região de memória PCIe ECAM

A tabela Configuração Avançada e Interface de Alimentação (ACPI) fornecida pelo firmware não define uma região de memória no barramento PCI no método Current Resource Settings (_CRS) para o dispositivo de barramento PCI. Conseqüentemente, a seguinte mensagem de aviso ocorre durante a inicialização do sistema:

```
[    2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x30000000-0x31ffffff] not
reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

Entretanto, o kernel ainda é capaz de acessar a região de memória **0x30000000-0x31ffff**, e pode atribuir essa região de memória ao Mecanismo de Acesso à Configuração Melhorada do PCI (ECAM) adequadamente. Você pode verificar se o PCI ECAM funciona corretamente ao acessar o espaço de configuração do PCIe sobre o offset de 256 bytes com a seguinte saída:

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-
if 02 [NVM Express])
 ...
        Capabilities: [900 v1] L1 PM Substates
                L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
                        PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
                L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
                        T_CommonMode=0us LTR1.2_Threshold=0ns
                L1SubCtl2: T_PwrOn=10us
```

Como resultado, você pode ignorar a mensagem de aviso.

Para mais informações sobre o problema, veja o "Firmware Bug: ECAM area **mem 0x30000000-0x31ffffff** not reserved in ACPI namespace" aparece durante a solução de inicialização do sistema.

(BZ#1868526)

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 biblioteca MPI ABERTA pode desencadear falhas no tempo de execução com PML padrão

Na implementação da série 4.0.x da OPEN Message Passing Interface (OPEN MPI), a Comunicação Unificada X (UCX) é o comunicador ponto a ponto (PML) padrão. As versões posteriores da série OPEN MPI 4.0.x depreciaram a camada de transferência de bytes **openib** (BTL).

No entanto, OPEN MPI, quando executada sobre um cluster **homogeneous** (mesma configuração de hardware e software), a UCX ainda usa o **openib** BTL para operações unilaterais de MPI. Como conseqüência, isto pode desencadear erros de execução. Para contornar este problema:

- Execute o comando **mpirun** usando os seguintes parâmetros:

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

onde,

- O parâmetro **-mca btl openib** desactiva **o openib BT** L
- O parâmetro **-mca pml ucx** configura o MPI ABERTO para usar **o ucx** PML.
- O parâmetro **x UCX_NET_DEVICES=** restringe o UCX a usar os dispositivos especificados

O MPI ABERTO, quando executado sobre um cluster **heterogeneous** (configuração diferente de hardware e software), ele usa o UCX como o PML padrão. Como consequência, isto pode fazer com que os trabalhos MPI ABERTO funcionem com desempenho errático, comportamento não responsivo ou falhas de crash. Para contornar este problema, defina a prioridade do UCX como:

- Execute o comando **mpirun** usando os seguintes parâmetros:

```
-mca pml_ucx_priority 5
```

Como resultado, a biblioteca OPEN MPI é capaz de escolher uma camada alternativa de transporte disponível sobre a UCX.

(BZ#186666402)

6.5.7. 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)

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 nomear um volume lógico **writecache** ao usar comandos **pvmove**.
- Não é possível utilizar volumes lógicos com **writecache** em combinação com piscinas finas ou VDO.

A seguinte limitação também se aplica ao método de **cache**:

- Não é possível redimensionar um volume lógico enquanto o **cache** ou o **writecache** estiver anexado a ele.

(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)

6.5.8. 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)

Conflitos de símbolos entre bibliotecas OpenLDAP podem causar falhas no httpd

Quando ambas as bibliotecas **libldap** e **libldap_r** fornecidas pelo OpenLDAP são carregadas e usadas dentro de um único processo, podem ocorrer conflitos de símbolos entre essas bibliotecas. Conseqüentemente, os processos infantis do Apache **httpd** usando a extensão **ldap** do PHP podem terminar inesperadamente se os módulos **mod_security** ou **mod_auth_openidc** também forem carregados pela configuração **httpd**.

Com esta atualização da biblioteca Apache Portable Runtime (APR), você pode contornar o problema definindo a variável de ambiente **APR_DEEPBIND**, que permite o uso da opção de linker dinâmico **RTLD_DEEPBIND** ao carregar módulos **httpd**. Quando a variável de ambiente **APR_DEEPBIND** é habilitada, não ocorrem mais falhas nas configurações **httpd** que carregam bibliotecas conflitantes.

(BZ#1819607)

6.5.9. Gestão da Identidade

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)

Usando o utilitário cert-fix com a opção --agent-uid pkidbuser break Certificate System

O uso do utilitário **cert-fix** com a opção **--agent-uid pkidbuser** corrompe a configuração LDAP do Sistema de Certificado. Como conseqüência, o Sistema de Certificado pode se tornar instável e são necessários passos manuais para recuperar o sistema.

(BZ#1729215)

Os certificados emitidos pela PKI ACME Responder ligado à PKI CA podem falhar a validação OCSP

O perfil padrão do certificado ACME fornecido pela PKI CA contém uma amostra de URL OCSP que não aponta para um serviço OCSP real. Como conseqüência, se o Respondente PKI ACME estiver configurado para usar um emissor PKI CA, os certificados emitidos pelo Respondente podem falhar na validação do OCSP.

Para contornar este problema, você precisa definir a propriedade **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0** para um valor em branco no arquivo de configuração **/usr/share/pki/ca/profiles/ca/acmeServerCert.cfg:**

1. No arquivo de configuração do ACME Responder, altere a linha **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=http://ocsp.example.com** para **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=**.

2. Reinicie o serviço e regenere o certificado.

Como resultado, a PKI CA gerará certificados ACME com um URL OCSP autogerado que aponta para um serviço OCSP real.

(BZ#1868233)

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)

6.5.10. Desktop

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)

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)

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)

6.5.11. Infra-estruturas gráficas

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, desabilite **o radeon** 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 em falha na ativação. Isto é devido ao sistema pensar erroneamente que não há largura de banda suficiente no hub para suportar todos os monitores.

(BZ#1812577)

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)

O VNC Viewer exibe cores erradas com a profundidade de cor de 16 bits no IBM Z

O aplicativo VNC Viewer exibe cores erradas quando você se conecta a uma sessão VNC em um servidor IBM Z com a profundidade de cor de 16 bits.

Para contornar o problema, configure a profundidade de cor de 24 bits no servidor VNC. Com o servidor **Xvnc**, substitua a opção **-depth 16** por **-depth 24** na configuração do **Xvnc**.

Como resultado, os clientes VNC exibem as cores corretas, mas utilizam mais largura de banda de rede com o servidor.

(BZ#1886147)

A aceleração de hardware não é suportada na ARM

Os drivers gráficos incorporados não suportam a aceleração de hardware ou o Vulkan API na arquitetura ARM de 64 bits.

Para permitir a aceleração de hardware ou Vulkan no ARM, instale o driver proprietário Nvidia.

(JIRA:RHELPLAN-57914)

6.5.12. 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)

6.5.13. Funções do Sistema Red Hat Enterprise Linux

as funções de entrada e saída de **procura elástica** não são suportadas no registro de funções do sistema

A entrada de **oVirt** e a saída de **procura elástica** não são suportadas no registro de funções do sistema, embora sejam mencionadas no arquivo README. Não há nenhuma solução de trabalho disponível no momento.

(BZ#1889468)

6.5.14. Virtualização

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 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)

Máquinas virtuais usando Cooperlake não podem inicializar quando o TSX é desativado no host

Máquinas virtuais (VMs) que utilizam o modelo de CPU **Cooperlake** atualmente não inicializam quando a bandeira da CPU **TSX** é diabólica no host. Ao invés disso, o host exibe a seguinte mensagem de erro:

```
a CPU é incompatível com a CPU do host: A CPU hospedeira não fornece as características necessárias: hle, rtm
```

Para tornar as VMs com **Cooperlake** utilizáveis em tal host, desative as bandeiras HLE, RTM e TAA_NO na configuração da VM na configuração XML da VM:

```
<feature policy='disable' name='hle'/>
<feature policy='disable' name='rtm'/>
<feature policy='disable' name='taa-no'/>
```

(BZ#1860743)

Máquinas virtuais às vezes não podem inicializar em máquinas Witherspoon

Máquinas virtuais (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 XML da VM da seguinte forma:

```
<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)

6.5.15. RHEL em ambientes de nuvens

Problemas de GPU em instâncias do Azure NV6

Ao executar o RHEL 8 como um sistema operacional convidado em uma instância do Microsoft Azure NV6, retomar a máquina virtual (VM) a partir da hibernação às vezes faz com que a GPU da VM funcione incorretamente. Quando isto ocorre, o kernel registra a seguinte mensagem:

```
hv_irq_unmask() falhou: 0x5
```

(BZ#1846838)

kdump às vezes não começa com Azure e Hyper-V

Nos sistemas operacionais convidados RHEL 8 hospedados nos hipervisores Microsoft Azure ou Hyper-V, iniciar o **kdump** kernel em alguns casos falha quando os notificadores pós-exec são habilitados.

Para contornar este problema, desabilite os notificadores de crash kexec post notifiers:

```
# echo N
```

(BZ#1865745)

O ajuste de IP estático em uma máquina virtual RHEL 8 em um host VMWare não funciona

Atualmente, ao utilizar o RHEL 8 como um sistema operacional convidado de uma máquina virtual (VM) em um host VMWare, a função DatasourceOVF não funciona corretamente. Como conseqüência, se você usar o utilitário de **nuvem** para configurar a rede da VM para IP estático e depois reiniciar a VM, a rede da VM será alterada para DHCP.

(BZ#1750862)

As máquinas virtuais RHEL 8 com certos DNIs para uma máquina remota no Azure levam mais tempo do que o esperado

Atualmente, o uso do utilitário **kdump** para salvar o arquivo dump principal de uma máquina virtual RHEL 8 (VM) em um hipervisor Microsoft Azure para uma máquina remota não funciona corretamente quando a VM está usando um NIC com rede acelerada habilitada. Como conseqüência, o arquivo dump é salvo após aproximadamente 200 segundos, em vez de imediatamente. Além disso, a seguinte mensagem de erro é logada no console antes que o arquivo dump seja salvo.

```
dispositivo (eth0): linklocal6: DAD falhou para um endereço EUI-64
```

(BZ#1854037)

Os contadores de pacotesTX/RX não aumentam após a retomada das máquinas virtuais da hibernação

Os contadores de pacotes **TX**/**RX** param de aumentar quando uma máquina virtual RHEL 8 (VM), com um CX4 VF NIC, retoma da hibernação no Microsoft Azure. Para manter os balcões funcionando, reinicie a VM. Note que, ao fazer isso, os contadores serão reiniciados.

(BZ#1876527)

As máquinas virtuais RHEL 8 falham em retomar a hibernação no Azure

O GUIA da função virtual (VF), **dispositivo vmbus**, muda quando uma máquina virtual RHEL 8 (VM),

com **SR-IOV** habilitado, é hibernada e desalocada no Microsoft Azure . Como resultado, quando a VM é reiniciada, ela não é retomada e trava. Como uma solução de trabalho, a VM é reinicializada usando o console serial do Azure.

(BZ#1876519)

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)

6.5.16. 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)

6.5.17. 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)

aconexão do sistema podman add não define automaticamente a conexão padrão

O comando de **adição de conexão do sistema podman** não define automaticamente a primeira conexão como sendo a conexão padrão. Para definir a conexão padrão, você deve executar manualmente o comando **podman padrão de conexão**do sistema

(BZ#1881894)

6.6. INTERNACIONALIZAÇÃO

6.6.1. 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, libhangul

6.6.2. 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.
- Vários locais da **glibc** foram sincronizados com o Unicode 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#1816862, BZ#1638875, BZ#1728943
NetworkManager	BZ#1814746, BZ#1626348
anaconda	BZ#1665428, BZ#1775975, BZ#1630299, BZ#1823578, BZ#1672405, BZ#1644662, BZ#1745064, BZ#1821192, BZ#1822880, BZ#1862116, BZ#1890261, BZ#1891827,BZ#1691319
abr	BZ#1819607
authselect	BZ#1654018
bcc	BZ#183737906
bind	BZ#1818785
buildah-container	BZ#1627898
buildah	BZ#1806044
clevis	BZ#1716040, BZ#1818780, BZ#1436735, BZ#1819767
cloud-init	BZ#1750862
parte de crescimento de nuvens-utils-growpart	BZ#1846246
gravação da sessão de cockpit	BZ#1826516
cockpit	BZ#1710731, BZ#1666722
corosync-qdevice	BZ#1784200
crun	BZ#1841438
crypto-policies	BZ#1832743, BZ#1660839
cyrus-sasl	BZ#1817054

Componente	Ingressos
distribuição	BZ#1815402, BZ#1657927
dnf	BZ#1793298, BZ#1832869, BZ#1842285
elfutils	BZ#1804321
fapolicyd	BZ#1897090, BZ#1817413, BZ#1714529
agentes de vedação	BZ#1830776, BZ#1775847
firewalld	BZ#1790948, BZ#1682913, BZ#1809225, BZ#1817205, BZ#1809636
freeradius	BZ#1672285, BZ#1859527, BZ#1723362
gcc-toolset-10-gdb	BZ#1838777
gcc	BZ#1784758
gdb	BZ#1659535
git	BZ#1825114
glibc	BZ#1812756, BZ#1743445, BZ#1783303, BZ#1642150, BZ#1810146, BZ#1748197, BZ#1774115, BZ#1807824, BZ#1757354, BZ#1836867, BZ#1780204, BZ#1821531, BZ#1784525
gnome-session	BZ#1739556
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1724302
gnome-software	BZ#1668760
gnutls	BZ#1677754, BZ#1789392, BZ#1849079, BZ#1855803
go-toolset	BZ#1820596
gpgme	BZ#1829822
grafana-container	BZ#1823834

Componente	Ingressos
grafana-pcp	BZ#1807099
grafana	BZ#1807323
grub2	BZ#1583445
httpd	BZ#1209162
inicial-setup	BZ#1676439
ipa-healthcheck	BZ#1852244
ipa	BZ#181616784, BZ#1810154, BZ#913799, BZ#1651577, BZ#1851139, BZ#1664719, BZ#1664718
iperf3	BZ#1665142, BZ#1700497
jss	BZ#1821851
kernel-rt	BZ#1818138
kernel	BZ#1758323, BZ#1812666, BZ#1793389, BZ#1694705, BZ#1748451, BZ#1654962, BZ#1792125, BZ#1708456, BZ#1812577, BZ#1757933, BZ#1847837, BZ#1791664, BZ#1666538, BZ#1602962, BZ#1609288, BZ#1730502, BZ#1806882, BZ#1660290, BZ#1846838, BZ#1865745, BZ#1868526, BZ#1884857, BZ#1854037, BZ#1876527, BZ#1876519, BZ#1823764, BZ#1822085, BZ#1735611, BZ#1281843, BZ#1828642, BZ#1825414, BZ#1761928, BZ#1791041, BZ#1796565, BZ#1834769, BZ#1785660, BZ#1683394, BZ#1817752, BZ#1782831, BZ#1821646, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#150363672, BZ#1570255, BZ#1696451, BZ#1348508, BZ#1778762, BZ#1839311, BZ#1783396, BZ#1665295, BZ#1658840, BZ#1660627, BZ#1569610
krb5	BZ#1791062, BZ#1784655, BZ#1820311, BZ#1802334, BZ#1877991
libbpf	BZ#1759154
libcap	BZ#1487388

Componente	Ingressos
libdb	BZ#1670768
libffi	BZ#1723951
libgnome-keyring	BZ#1607766
libkcapi	BZ#1683123
libmaxminddb	BZ#1642001
libpcap	BZ#1806422
libreswan	BZ#1544463, BZ#1820206
libseccomp	BZ#1770693
libselinux-python-2,8-módulo	BZ#1666328
libssh	BZ#1804797
libvirt	BZ#1664592, BZ#1528684
lldb	BZ#1841073
llvm-toolset	BZ#1820587
llvm	BZ#1820319
lshw	BZ#1794049
lvm2	BZ#1496229, BZ#1768536, BZ#1598199, BZ#1541165, JIRA:RHELPLAN-39320
memcached	BZ#1809536
mesa	BZ#1886147
microdnf	BZ#1781126
mod_http2	BZ#1814236
nfs-utils	BZ#1817756, BZ#1592011
nginx	BZ#1668717, BZ#1826632

Componente	Ingressos
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1817533, BZ#1645153
opencryptoki	BZ#1780293
openmpi	BZ#1866402
opensc	BZ#1810660
openscap	BZ#1803116, BZ#1870087, BZ#1795563, BZ#1824152, BZ#1829761
openssh	BZ#1744108
openssl	BZ#1685470, BZ#1810911
oscap-anaconda-addon	BZ#1816199, BZ#1665082, BZ#1674001, BZ#1691305, BZ#1787156, BZ#1843932, BZ#1834716
marcapasso	BZ#1828488, BZ#1784601, BZ#1837747, BZ#1718324
papi	BZ#1807346, BZ#1664056, BZ#1726070
pcp-container	BZ#1497296
pcp	BZ#1792971
pcs	BZ#1817547, BZ#1684676, BZ#1839637, BZ#1619620
porl-5,30-módulo	BZ#1713592
perl-IO-Socket-SSL	BZ#1824222
perl-libwww-perl	BZ#1781177
php	BZ#1797661
pki-core	BZ#1729215, BZ#1868233, BZ#1770322, BZ#1824948

Componente	Ingressos
podman	BZ#1804193, BZ#1881894, BZ#1627899
powertop	BZ#1783110
pykickstart	BZ#1637872
python38	BZ#1847416
qemu-kvm	BZ#1719687, BZ#1860743, JIRA:RHELPLAN-45901, BZ#1651994
traseiro	BZ#1843809, BZ#1729502, BZ#1743303
redhat-support-tool	BZ#1802026
agentes de recursos	BZ#1814896
rhel-system-roles-sap	BZ#1844190, BZ#1660832
rhel-system-roles	BZ#1889468, BZ#1822158, BZ#1677739
rpm	BZ#1688849
rsyslog	BZ#1659383, JIRA:RHELPLAN-10431, BZ#1679512, BZ#1713427
rubi-2,7-módulo	BZ#1817135
rubi	BZ#1846113
conjunto ferrugem	BZ#1820593
samba	BZ#1817557, JIRA:RHELPLAN-13195
scap-security-guide	BZ#1843913, BZ#1858866, BZ#1750755, BZ#1760734, BZ#1832760, BZ#1815007
scap-workbench	BZ#1640715
selinux-policy	BZ#1826788, BZ#1746398, BZ#1776873, BZ#1772852, BZ#1641631, BZ#1860443
setools	BZ#1820079
skopeo-container	BZ#1627900

Componente	Ingressos
smartmontools	BZ#1671154
tempero	BZ#1849563
lula	BZ#1829467
sssd	BZ#1827615, BZ#1793727
stratis-cli	BZ#1734496
túnel	BZ#1808365
gerenciador de assinaturas	BZ#1674337
sudo	BZ#1786990
systemtap	BZ#1804319
tang	BZ#1716039
tcpdump	BZ#1804063
tigervnc	BZ#1806992
tpm2-ferramentas	BZ#1789682
sintonizado	BZ#1792264, BZ#1840689, BZ#1746957
udica	BZ#1763210
usbguard	BZ#1738590, BZ#1667395, BZ#1683567
valgrind	BZ#1804324
wayland	BZ#1673073
xdp-tools	BZ#1880268, BZ#1820670
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1698565
yum	BZ#1788154

Componente	Ingressos
outros	JIRA:RHELPLAN-45950, JIRA:RHELPLAN-57572, BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1790635, BZ#1823398, BZ#1757877, JIRA:RHELPLAN-25571, BZ#1777138, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, BZ#1897383, BZ#1900019, BZ#1839151, BZ#1780124, JIRA:RHELPLAN-42395, BZ#1889736, BZ#1842656, JIRA:RHELPLAN-45959, JIRA:RHELPLAN-45958, JIRA:RHELPLAN-45957, JIRA:RHELPLAN-45956, JIRA:RHELPLAN-45952, JIRA:RHELPLAN-45945, JIRA:RHELPLAN-45939, JIRA:RHELPLAN-45937, JIRA:RHELPLAN-45936, JIRA:RHELPLAN-45930, JIRA:RHELPLAN-45926, JIRA:RHELPLAN-45922, JIRA:RHELPLAN-45920, JIRA:RHELPLAN-45918, JIRA:RHELPLAN-45916, JIRA:RHELPLAN-45915, JIRA:RHELPLAN-45911, JIRA:RHELPLAN-45910, JIRA:RHELPLAN-45909, JIRA:RHELPLAN-45908, JIRA:RHELPLAN-45906, JIRA:RHELPLAN-45904, JIRA:RHELPLAN-45900, JIRA:RHELPLAN-45899, JIRA:RHELPLAN-45884, JIRA:RHELPLAN-37573, JIRA:RHELPLAN-37570, JIRA:RHELPLAN-49954, JIRA:RHELPLAN-50002, JIRA:RHELPLAN-43531, JIRA:RHELPLAN-48838, BZ#1873567, BZ#1866695, JIRA:RHELPLAN-14068, JIRA:RHELPLAN-7788, JIRA:RHELPLAN-40469, JIRA:RHELPLAN-42617, JIRA:RHELPLAN-30878, JIRA:RHELPLAN-37517, JIRA:RHELPLAN-55009, JIRA:RHELPLAN-42396, BZ#1836211, JIRA:RHELPLAN-57564, JIRA:RHELPLAN-57567, BZ#1890499, JIRA:RHELPLAN-40234, JIRA:RHELPLAN-56676, JIRA:RHELPLAN-14754, JIRA:RHELPLAN-51289, BZ#1893174, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1889737, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-41549, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057, BZ#1748980, BZ#1827628, BZ#1871025, BZ#1871953, BZ#1874892, BZ#1893767, JIRA:RHELPLAN-60226

APÊNDICE B. HISTÓRICO DE REVISÃO

0-1-3

Ter 16 de fevereiro de 2021, Lenka Špačková(lspackova@redhat.com)

- Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 8.3.1.
- Seção de atualização no local em Visão Geral com o lançamento da assessoria RHBA-2021:0569.

0-1-2

Sex Fev 12 2021, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou duas questões conhecidas (Segurança, Instalador).

0-1-1

Qua Fev 10 2021, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentada uma questão conhecida (Virtualização).

0-1-0

Qua Fev 03 2021, Lenka Špačková(lspackova@redhat.com)

- Acrescentou uma nota sobre a consolidação da configuração da rede na linha de comando do kernel sob o parâmetro **ip** (Networking).
- Adicionado **mercurial** aos pacotes depreciados.
- Acrescentada uma questão conhecida relacionada aos anfitriões Witherspoon (Virtualização).

0-0-9

Sex 29 de janeiro de 2021, Lucie Maňásková(lmanasko@redhat.com)

- Adicionada nova descrição de correção de erros (Segurança).
- Acrescentou uma nota sobre a desvalorização do pacote do **carteiro** (Gerenciamento de software).
- Atualizada a seção Novos recursos (Segurança, Gerenciamento de Identidade).
- Acrescentei uma nota de pré-visualização tecnológica sobre o serviço **resolvido pelo sistema**.
- Outras pequenas atualizações.

0.0-8

Seg 14 Dez 2020, Lucie Maňásková(lmanasko@redhat.com)

- Atualizou a seção de problemas conhecidos e a seção de correção de erros.

0.0-7

Sex 27 de novembro de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Acrescentou uma correção de erros para emissão com **fapolicyd** (Segurança).
- Mais atualizações para a seção de correção de erros.
- Acrescentou uma nota sobre a desvalorização do REST API V1 (Containers) baseado no Podman varlink.
- Atualizada a seção Novos recursos.
- Acrescentada a nova edição conhecida sobre a replicação de plantas do back end **lorax-composer** para o novo back end **osbuild-composer** (Image Builder).

0.0-6

Sex 20 de novembro de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Adicionada uma descrição de correção de bugs OpenSCAP (Segurança).
- Atualizada a seção Novos recursos (Gerenciamento de software).

0.0-5

Quarta-feira 18 de novembro de 2020, Lenka Špačková(lspackova@redhat.com)

- Adicionadas informações sobre conversão de Oracle Linux ou CentOS para RHEL (Visão geral).

0.0-4

Thu Nov 12 2020, Lenka Špačková(lspackova@redhat.com)

- Informações adicionais sobre o **Node.js 14.15.0** divulgadas com a assessoria RHEA-2020:5101.

0.0-3

Qua 11 Nov 2020, Lucie Maňásková(lmanasko@redhat.com)

- Descrição adicional sobre o suporte ao software hospedeiro Omni-Path Architecture (OPA) para Novos recursos.

0.0-2

Seg 09 Nov 2020, Lenka Špačková(lspackova@redhat.com)

- Acrescentei os gráficos Intel Tiger Lake como uma prévia tecnológica (infra-estruturas gráficas).

0.0-1

Quar 04 Nov 2020, Lucie Maňásková(lmanasko@redhat.com)

- Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 8.3.

0.0-0

Ter 28 de julho de 2020, Lucie Maňásková(lmanasko@redhat.com)

- Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 8.3 Beta.