Red Hat Enterprise Linux 7
7.2 Notas de Lançamento

Notas de Lançamento para o Red Hat Enterprise Linux 7.2

Red Hat Serviços de Conteúdo do Cliente

Red Hat Enterprise Linux 7 7.2 Notas de Lançamento

Notas de Lançamento para o Red Hat Enterprise Linux 7.2

Red Hat Serviços de Conteúdo do Cliente
rhel-notes@redhat.com

Nota Legal

Resumo

As Notas de Lançamento fornecem uma cobertura de alto nível das adições e aprimoramentos que foram implementados no Red Hat Enterprise Linux 7.2 e documenta os problemas conhecidos nesta versão. Para uma documentação detalhada sobre todas as alterações feitas no Red Hat Enterprise Linux para a atualização 7.2, consulte Errata no Portal do Cliente Red Hat.

Índice

Prefácio

Os lançamentos de manutenção do Red Hat Enterprise Linux agregam aprimoramentos individuais, erratas de segurança e correções de erros. As *Notas de Lançamento do Red Hat Enterprise Linux 7.2* documentam as maiores modificações feitas ao sistema operacional Red Hat Enterprise Linux 7 e aos seus aplicativos que acompanham este lançamento de manutenção, assim como aos problemas conhecidos e fornecem uma lista completa de todas as Apresentações Prévias de Tecnologia atualmente disponíveis.

Os recursos e os limites do Red Hat Enterprise Linux 7 comparados a outras versões do sistema estão disponíveis no artigo da base de dados de conhecimento da Red Hat em https://access.redhat.com/articles/rhel-limits.

Para mais informações sobre o ciclo de vida do Red Hat Enterprise Linux, por favor consulte https://access.redhat.com/support/policy/updates/errata/.

Capítulo 1. Arquiteturas

O Red Hat Enterprise Linux 7.2 está disponível em um kit único nas seguintes arquiteturas: [1]

- AMD 64 bits
- Intel 64 bits
- IBM POWER7+ e POWER8 (big endian) [2]
- IBM POWER8 (little endian) [3]
- IBM System z [4]

---

[1] Observe que a instalação do Red Hat Enterprise Linux 7.2 possui suporte somente em hardware de 64 bits. O Red Hat Enterprise Linux 7.2 é capaz de executar sistemas operacionais de 32 bits, incluindo versões prévias do Red Hat Enterprise Linux, como as máquinas virtuais.

[2] O Red Hat Enterprise Linux 7.2 (big endian) atualmente possui suporte somente em PowerVM.

[3] O Red Hat Enterprise Linux 7.2 (little endian) atualmente possui suporte em PowerVM e PowerHV (bare metal).

[4] Observe que o Red Hat Enterprise Linux 7.2 fornece suporte ao hardware IBM zEnterprise 196 ou a versões subsequentes; Os sistemas mainframe IBM System z10 não possuem mais suporte e não inicializarão o Red Hat Enterprise Linux 7.2.

Parte I. Novos Recursos

Esta seção descreve os novos recursos e os principais aprimoramentos introduzidos no Red Hat Enterprise Linux 7.2.

Capítulo 2. Atualizações Gerais

Melhorias nas dependências dos pacotes por todos os canais

Agora o yum solicita que o usuário final verifique os repositórios dos pacotes desabilitados no sistema, diante de um erro de dependência nos pacotes. Esta mudança permitirá que os usuários solucionem rapidamente os erros de dependência pesquisando, primeiro, em todos os canais conhecidos, pela dependência do pacote ausente.

Para habilitar esta funcionalidade, execute **`yum update yum subscription-manager`** antes de atualizar a sua máquina para o Red Hat Enterprise Linux 7.2.

Por favor, consulte o capítulo Gerenciamento do Sistema e Subscrições para mais detalhes sobre a implementação deste recurso.

A proteção RELRO agora é aplicada corretamente quando requisitada

Antigamente, os arquivos binários iniciados pelo carregador do sistema não dispunha, em alguns casos, da proteção de relocação em modo somente leitura (RELRO), apesar de ser solicitada explicitamente durante a compilação do aplicativo. Isto ocorria devido a uma má comunicação entre o linker estático e o carregador do sistema. O código fonte subjacente do linker foi ajustado para garantir a aplicação da proteção RELRO, recuperando, assim, o recurso de segurança para os aplicativos. Os aplicativos e todas as bibliotecas e os arquivos de objetos dependentes compilados com uma versão alpha e beta do *binutils* devem ser recompilados para a correção deste defeito. Esta atualização corrige o problema nas arquiteturas ARM 64-bit, PowerPC 64-bit, Intel 64 e AMD64.

Mais informações de diagnóstico e um plug-in renomeado para sosreport

A ferramenta sosreport foi aprimorada para coletar informações relacionadas aos processos de vários aplicativos, incluindo ptp, lastlog e ethtool. Como parte desta mudança, o plug-in **`startup`** foi renomeado para **`services`** para expressar melhor a sua função.

Habilitação da renomeação do dispositivo de rede virtio

Esta atualização adiciona um novo esquema de nomeação persistente ao driver virtio, que habilita a renomeação do dispositivo de rede virtio. Para habilitar este recurso no Red Hat Enterprise Linux 7.2, adicione o parâmetro do kernel **`net.ifnames=1`** durante inicialização.

Suporte a DIF/DIX (T10 PI) em hardware especificado

O SCSI T10 DIF/DIX possui suporte completo no Red Hat Enterprise Linux 7.2, desde que o fornecedor do hardware tenha qualificado-o e forneça suporte completo à configuração da matriz de armazenamento e ao HBA em particular. O DIF/DIX não possui suporte em outras configurações, não possui suporte para uso no dispositivo de inicialização e nem em máquinas virtuais.

Atualmente, os fornecedores que proporcionam este suporte são:

FUJITSU fornece suporte a DIF e DIX em:

- EMULEX 16G FC HBA:
  - EMULEX LPe16000/LPe16002, 10.2.254.0 BIOS, 10.4.255.23 FW com:
  - FUJITSU ETERNUS DX100 S3, DX200 S3, DX500 S3, DX600 S3, DX8100 S3, DX8700 S3, DX8900 S3, DX200F, DX60 S3

- QLOGIC 16G FC HBA:
  - QLOGIC QLE2670/QLE2672, 3.28 BIOS, 8.00.00 FW com:
  - FUJITSU ETERNUS DX100 S3, DX200 S3, DX500 S3, DX600 S3, DX8100 S3, DX8700 S3, DX8900 S3, DX200F, DX60 S3

Observe que o T10 DIX necessita de um banco de dados ou algum outro software que forneça geração e verificação das somas de verificação nos blocos de disco. Nenhum sistema de arquivo Linux atualmente com suporte possui este recurso.

EMC fornece suporte a DIF em:

- EMULEX 8G FC HBA:
  - LPe12000-E e LPe12002-E com firmware 2.01a10, ou posterior, com:
  - EMC VMAX3 Series com Enginuity 5977; EMC Symmetrix VMAX Series com Enginuity 5876.82.57 e posterior
- EMULEX 16G FC HBA:
  - LPe16000B-E e LPe16002B-E com firmware 10.0.803.25 ou posterior com:
  - EMC VMAX3 Series com Enginuity 5977; EMC Symmetrix VMAX Series com Enginuity 5876.82.57 e posterior
- QLOGIC 16G FC HBA:
  - QLE2670-E-SP e QLE2672-E-SP com:
  - EMC VMAX3 Series com Enginuity 5977; EMC Symmetrix VMAX Series com Enginuity 5876.82.57 e posterior

Por favor, consulte as informações de suporte do fornecedor do hardware para os status mais recentes.

O suporte ao DIF/DIX é mantido na Apresentação Prévia de Tecnologia para outros HBAs e matrizes de armazenamento.

Capítulo 3. Autenticação e Interoperabilidade

O Gerenciamento de Identidade estabelece uma relação de confiança unidirecional por padrão

O comando **`ipa trust-add`** agora configura uma relação de confiança unidirecional por padrão. As relações de confiança unidirecionais permitem que os usuários e grupos no Active Directory (AD) acessem os recursos no Gerenciamento de Identidade (IdM), mas não o contrário. Anteriormente, a configuração de relação de confiança padrão, ao executar **`ipa trust-add`**, era uma relação bidirecional.

O IdM ainda permite, no entanto, que o administrador configure uma relação de confiança bilateral adicionando a opção **`--two-way=true`** ao comando **`ipa trust-add`**.

Rebase do `openldap` para a versão 2.4.40

Os pacotes *openldap* foram atualizados para a versão upstream 2.4.40, a qual fornece várias correções de erros e um aprimoramento em relação à versão anterior. Em especial, a ORDENAÇÃO das regras de correspondência foi adicionada às descrições do tipo de atributo **`ppolicy`**. Entre os erros corrigidos estão: o servidor não é mais encerrado de forma inesperada, durante o processamento dos registros SRV, e as informações **`objectClass`** ausentes foram adicionadas, permitindo ao usuário modificar a configuração front-end por meios convencionais.

Autenticação de cache em SSSD

A autenticação ao cache sem uma tentativa de reconexão está disponível agora em SSSD, mesmo em modo online. A autenticação direta ao servidor de rede de forma repetida pode causar uma latência excessiva ao aplicativo, deixando o processo de login bastante lento.

SSSD habilita o mapeamento do UID e GID em clientes individuais

Agora é possível mapear os usuários a um UID e GID diferente em certos clientes Red Hat Enterprise Linux através da configuração do lado do cliente, usando SSSD. Essa possibilidade de substituição do lado do cliente pode resolver os problemas causados pela duplicação do UID e GID ou facilitar a transição de um sistema legado que usava anteriormente um mapeamento de ID diferente.

Observe que as substituições ficam armazenadas no cache SSSD e a remoção do cache também remove as substituições.

SSSD pode negar acesso SSH a contas bloqueadas

Anteriormente, quando SSSD usava OpenLDAP como o seu banco de dados de autenticação, os usuários podiam autenticar-se no sistema com uma chave SSH com êxito, mesmo após a conta do usuário ter sido bloqueada. Agora, o parâmetro **`ldap_access_order`** aceita o valor **`ppolicy`** , o qual pode negar acesso SSH ao usuário na situação descrita. Para mais informações sobre o uso de **`ppolicy`**, consulte a descrição **`ldap_access_order`** na página manual sssd-ldap(5).

O utilitário sudo é capaz de verificar o comando checksum (soma de verificação)

A configuração do utilitário sudo pode armazenar a soma de verificação de um comando ou script que está sendo permitido. Quando o comando ou script é executado novamente, a soma de verificação é comparada à soma de verificação armazenada para verificar se algo mudou. Se o comando ou binário for modificado, o utilitário sudo recusa a execução do comando ou registra um aviso. Esta funcionalidade possibilita transmitir

as responsabilidades e atividades para a solução de problemas de forma adequada, caso ocorra um incidente.

Suporte SSSD ao cartão inteligente

O SSSD oferece suporte agora a cartões inteligentes para autenticação local. Com este recurso, o usuário pode usar um cartão inteligente para fazer log on no sistema utilizando um console gráfico ou baseado em texto, assim como serviços locais, como o serviço sudo. O usuário deve colocar o cartão inteligente no leitor e fornecer o nome do usuário e o código PIN do cartão no aviso de login. Se o certificado no cartão inteligente for verificado, o usuário é autenticado com êxito.

Observe que o SSSD não permite, atualmente, que o usário adquira um tíquete Kerberos utilizando um cartão inteligente. Para obter um tíquete Kerberos, o usuário ainda é solicitado a fazer a autenticação usando o utilitário kinit.

Suporte para múltiplos perfis de certificado e certificados de usuário

O Gerenciamento de Identidades oferece suporte agora a múltiplos perfis para a emissão de servidores e outros certificados, ao invés de oferecer suporte apenas a um único perfil de certificado de servidor. Os perfis são armazenados no Servidor de Diretório e compartilhado entre as réplicas do IdM.

Além disto, o administrador pode agora emitir certificados a usuários individuais. Anteriormente, era possível emitir certificados a hosts e serviços apenas.

Senha Vault

Um novo recurso foi adicionado ao Gerenciamento de Identidades para permitir um armazenamento central seguro das informações privadas do usuário, como senhas e chaves.

Kerberos HTTPS proxy no Gerenciamento de Identidades

Uma função proxy do Centro de Distribuição de Chaves (KDC), interoperável com a implementação do Protocolo Proxy Kerberos KDC da Microsoft (MS-KKDCP), está disponível agora no Gerenciamento de Identidades e permite aos clientes acessar os serviços **`kpasswd`** e KDC usando HTTP. Os administradores de sistema podem expor o proxy na borda da rede através de um simples proxy reverso HTTP sem a necessidade de configurar e gerenciar um aplicativo em específico.

Atualização em segundo plano das entradas em cache

Agora, SSSD permite que as entradas em cache sejam atualizadas fora de banda em segundo plano. Antes desta atualização, quando a validade das entradas em cache expiravam, o SSSD analisava-as a partir do servidor remoto e armazenava-as no banco de dados outra vez, o que era um processo demorado. Com esta atualização, as entradas retornam instantaneamente, pois o back-end as mantém atualizadas todo o tempo. Observe que isto gera uma carga maior no servidor já que o SSSD baixa as entradas periodicamente e não apenas sob solicitação.

Cache para as operações `initgroups`

O cache de rápida memória SSSD agora oferece suporte às operações **`initgroups`**, o que aumenta a velocidade do processamento de initgroups e melhora o desempenho de alguns aplicativos como, por exemplo, GlusterFS e **`slapi-nis`**.

Negociação de autenticação otimizada com `mod_auth_gssapi`

O Gerenciamento de Identidades emprega agora o módulo **mod_auth_gssapi**, o qual usa chamadas GSSAPI ao invés de chamadas diretas Kerberos utilizadas pelo módulo **mod_auth_kerb** anteriormente empregado.

Recursos de gerenciamento do ciclo de vida do usuário

O gerenciamento do ciclo de vida do usuário fornece ao administrador um grande controle sobre a ativação e desativação das contas dos usuários. Agora, o administrador pode configurar novas contas de usuários adicionando-as a uma área de preparação que não as ativa por completo ou ativa as contas dos usuários inativas, deixando-as operacionais, ou ainda desativa as contas sem removê-las totalmente do banco de dados.

Os recursos de gerenciamento do ciclo de vida do usuário trazem importantes benefícios às implantações abrangentes do IdM. Observe que os usuários também podem ser adicionados à área de preparação diretamente de um cliente LDAP padrão, usando operações LDAP diretas. Anteriormente, o IdM oferecia suporte apenas ao gerenciamento de usuários utilizando as ferramentas da linha de comando do IdM ou da Interface do Usuário da web do IdM.

Suporte ao protocolo SCEP em `certmonger`

O serviço **certmonger** foi atualizado para trazer suporte ao Protocolo de Registro de Certificado Simples (SCEP). Agora é possível emitir um novo certificado e renovar ou substituir os certificados existentes sobre o SCEP.

Os módulos Apache para IdM passam a ter suporte completo

Os seguintes módulos Apache para o Gerenciamento de Identidade (IdM), adicionados como Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7.1, possuem, agora, suporte completo: **mod_authnz_pam**, **mod_lookup_identity** e **mod_intercept_form_submit**. Os módulos Apache podem ser usados por aplicativos externos para obter interações mais próximas com o IdM para além da simples autenticação.

NSS aumenta os valores mínimos aceitáveis de restrição de chave

A biblioteca dos Serviços de Segurança de Redes (NSS) no Red Hat Enterprise Linux 7.2 não aceita mais parâmteros de troca de chaves Diffie-Hellman (DH) menores que 768 bits, nem os certificados RSA e DSA com tamanhos de chave com menos de 1023 bits. O aumento dos valores mínimos aceitáveis de restrição de chave evita ataques que exploram as vulnerabilidades de segurança conhecidas, como Logjam (CVE-2015-4000) e FREAK (CVE-2015-0204).

Observe que as tentativas de conexão com um servidor usando chaves mais fracas do que os novos valores mínimos resultam, agora, em falha, mesmo que tais conexões funcionassem nas versões prévias do Red Hat Enterprise Linux.

NSS habilita as versões 1.1 e 1.2 do TLS por padrão

Os aplicativos usando as versões de protocolo que o NSS habilita por padrão agora também fornecem suporte às versões 1.1 e 1.2 dos protocolos TLS.

Certificados ECDSA passam a ter suporte

Os aplicativos que usam a lista de codificação do NSS padrão agora fornecem suporte às conexões com os servidores que usam os certificados Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA).

OpenLDAP escolhe automaticamente os conjuntos de codificação padrão do NSS

Os clientes OpenLDAP agora escolhem automaticamente os conjuntos de codificação padrão dos Serviços de Segurança de Rede (NSS) para a comunicação com o servidor. Não é mais necessário manter os conjuntos de codificação padrão manualmente no código fonte do OpenLDAP.

A configuração de um servidor IdM para ser um agente de confiança passa a ter suporte

O Gerenciamento de Identidade (IdM) distingue dois tipos de servidores IdM mestre: controladores de confiança e agentes de confiança. Os controladores de confiança executam todos os serviços necessários para o estabelecimento e a manutenção de uma relação de confiança; os agentes de confiança executam apenas os serviços necessários para o fornecimento de resoluções de usuários e grupos de florestas do Active Directory confiáveis para os clientes IdM inscritos nestes servidores IdM.

Por padrão, a execução do comando **`ipa-adtrust-install`** configura o servidor IdM como um controlador de confiança. Para configurar outro servidor IdM como um agente de confiança, acrescente a opção **`--add-agents`** ao comando **`ipa-adtrust-install`**.

A migração automatizada do WinSync para relações de confiança passa a ter suporte

O novo utilitário **`ipa-winsync-migrate`** possibilita uma migração harmoniosa da integração baseada em sicronização usando WinSync para a integração baseada em relações de confiança do Active Directory (AD). O utilitário migra automaticamente todos os usuários sincronizados usando WinSync de uma floresta do AD. Anteriormente, a migração de sincronização para a relação de confiança podia ser realizada apenas manualmente, usando as visualizações de ID.

Para mais informações sobre **`ipa-winsync-migrate`**, consulte a página manual ipa-winsync-migrate(1).

Solicitação de vários passos para as senhas de uso único e de longo prazo

Ao usar uma senha de uso único (token) junto com uma senha de longo prazo para a realização de login, o usuário recebe a solicitação para as duas senhas separadamente. Isto favorece o uso de senhas únicas assim como fornece uma extração da senha de longo prazo mais segura, permitindo que o cache da senha de longo prazo seja usado para autenticação offline.

Esquema LPK para OpenLDAP disponível no formato LDIF

LDIF é o novo formato padrão para o esquema de importação do OpenSDAP e o pacote *openssh-ldap* agora fornece o esquema de Chave Pública LDAP (LPK) no formato LDIF também. Assim, os administradores podem importar diretamente o esquema LDIF ao configurar a autenticação de chave pública baseada em LDAP.

Cyrus pode realizar a autenticação dos servidores IdM e AD novamente

Um lançamento upstream dos pacotes *cyrus-sasl* introduziu uma alteração não compatível com as versões anteriores que impedia o Cyrus de realizar a autenticação nas implementações SASL mais antigas. Como consequência, o Red Hat Enterprise Linux 7 não conseguia fazer a autenticação dos servidores AD e IdM do Red Hat Enterprise Linux 6. A alteração upstream foi revertida e o Cyrus agora é capaz de realizar a autenticação dos servidores AD e IdM como esperado.

SSSD fornece suporte à sobrescrição do site do AD descoberto automaticamente

O site do DNS do Active Directory (AD) com o qual o cliente conecta-se é descoberto automaticamente por

padrão. No entanto, a pesquisa automática padrão pode não descobrir o site do AD mais adequado em determinadas configurações. Em tais situações, você pode definir agora o site DNS manualmente, usando o parâmetro **`ad_site`** na seção **`[domain/NAME]`** do arquivo **`/etc/sssd/sssd.conf`**.

Suporte para SAML ECP

Os pacotes lasso foram rebaseados para a versão 2.5.0 e os pacotes mod_auth_mellon foram rebaseados para a versão 0.11.0 para adicionar suporte ao Security Assertion Markup Language (SAML) Enhanced Client or Proxy (ECP). O SAML ECP é um perfil SAML alternativo que permite Autenticações Únicas (SSO) não baseadas no navegador.

O serviço winbindd não lista mais as associações de grupos na sua configuração padrão

O serviço **`winbindd`** na versão 4.2.0, ou posterior, do Samba não lista mais as associações de grupos para fins de exibição. Em algumas situações, como em ambientes com domínios confiáveis, não era sempre possível fornecer esta informação com segurança. Para impedir o risco do fornecimento de informações incorretas, a configuração padrão **`winbindd`** foi alterada para **`winbind expand groups = 0`**, o que desabilita o comportamento anterior. Observe que, alguns comandos, como **`getent group`**, dependiam anteriormente desta funcionalidade e podem não comportar-se como antes.

Capítulo 4. Clusterização

systemd e pacemaker passam a ser coordenados corretamente durante o desligamento do sistema

Anteriormente, systemd e pacemaker não eram coordenados corretamente durante o desligamento do sistema, fazendo com que os recursos do pacemaker fossem encerrados inadequadamente. Com a atualização, o pacemaker é obrigado a interromper-se antes do dbus e outros serviços systemd iniciados por ele. Isto permite que tanto o pacemaker quanto os recursos que ele gerencia sejam encerrados corretamente.

Os comandos `pcs resource move` e `pcs resource ban` exibem uma mensagem de aviso esclarecendo o comportamento dos comandos

O comando **`pcs resource move`** e os comandos **`pcs resource ban`** criam restrições de local impedindo efetivamente a execução do recurso no nó atual até que a restrição seja removida ou até que o tempo de vida da restrição expire. Anteriormente, este comportamento não era muito claro para os usuários. Agora, esses comandos exibem uma mensagem de aviso explicando este comportamento e as telas de ajuda e documentações para esses comandos foram esclarecidas.

Novo comando para mover um recurso do pacemaker para seu nó preferencial

Depois que um recurso do pacemaker é movido, seja por falha ou porque o administrador moveu o nó manualmente, ele não volta necessariamente ao seu nó original, mesmo depois que as circunstâncias que causaram a falha forem corrigidas. Você pode usar agora o comando **`pcs resource relocate run`** para mover um recurso ao seu nó preferencial, como determinado pelo status atual do cluster, pelas restrições, pelo local dos recursos e por outras configurações. Você também pode usar o comando **`pcs resource relocate show`** para exibir os recursos migrados. Para mais informações sobre esses comandos, consulte High Availability Add-On Reference (Referência para Complementos de Alta Disponibilidade).

Método simplificado para a configuração de isolamento (fencing) para fornecimentos de energia redundante em um cluster

Ao configurar o isolamento para os fornecimentos de energia redundante, você deve certificar-se de que, quando os fornecimentos de energia são reinicializados, ambos sejam desligados antes que um deles seja ligado novamente. Se o nó nunca perde a energia por completo, ele pode não liberar seus recursos. Isto abre a possibilidade dos nós acessarem esses recursos simultaneamente e corrompê-los.

Antes do Red Hat Enterprise Linux 7.2, era preciso configurar explicitamente as diferentes versões dos dispositivos que usavam as ações 'ligado' (on) e 'desligado' (off). Com o Red Hat Enterprise Linux 7.2 adiante, é necessário apenas definir cada dispositivo uma vez e especificar que ambos são necessários para isolar o nó.

Para informações sobre a configuração de isolamento para o fornecimento de energia redundante, consulte o capítulo **`Fencing: Configuring STONITH`** do High Availability Add-On Reference Manual.

Nova opção --port-as-ip para agentes de isolamento (fencing)

Os agentes de isolamento usados apenas com dispositivos únicos exigiam uma configuração complexa no pacemaker. Agora é possível usar a opção **`--port-as-ip`** para inserir o endereço IP na opção **`port`**.

Capítulo 5. Compilador e Ferramentas

tail --follow funciona adequadamente nos arquivos no sistema de arquivos em cluster Veritas (VXFS)

O sistema de arquivos em cluster Veritas (VXFS) é um sistema de arquivos remoto, e em tais sistemas,**`tail`** não pode usar a funcionalidade **`inotify`** para o modo **`--follow`**. O sistema de arquivos em cluster Veritas foi adicionado à lista de sistemas de arquivos remotos, onde o modo polling é usado no lugar de **`inotify`**. Agora, **`tail --follow`** pode funcionar corretamente mesmo quando usado nos arquivos em VXFS.

O comando dd é capaz de exibir o progresso de transferência

O comando **`dd`**, que é usado para copiar arquivos por bytes, agora oferece a opção **`status=progress`** para exibir o progresso da transferência. Isto é bastante útil principalmente para as transferências de arquivos grandes, pois permite ao usuário estimar o tempo restante e detectar prováveis problemas com a transferência.

Melhor tempo de espera em libcurl

A biblioteca **`libcurl`** utilizava um longo e desnecessário atraso de bloqueio para as ações sem descriptores de arquivo ativos, mesmo para operações breves. Isto significava que algumas ações, tais como a resolução de um nome de host usando **`/etc/hosts`**, levavam muito tempo para serem completadas. O código de bloqueio em **`libcurl`** foi, agora, modificado para que o atraso inicial seja breve e aumente gradualmente até que um evento ocorra. As operações **`libcurl`** passam a ser completadas de forma mais rápida.

A biblioteca libcurl implementa uma comunicação SSL sem bloqueio

Anteriormente, a biblioteca **`libcurl`** não implementava uma comunicação SSL sem bloqueio, o que afetava negativamente o desempenho dos aplicativos baseados na API **`libcurl`** multi. Para resolver este problema, a comunicação SSL sem bloqueio foi implementada em **`libcurl`** e a API **`libcurl`** multi agora retorna imediatamente o controle para o aplicativo sempre que não pode ler ou gravar dados do ou para o soquete de rede subjacente.

O GDB no IBM Power Systems não apresenta mais falhas quando acessando a tabela de símbolos

Anteriormente, o GDB no IBM Power Systems de 64 bits desalocava incorretamente uma variável importante que retinha a tabela de símbolos para o binário sendo depurado, causando uma falha de segmentação quando o GDB tentava acessar aquela tabela de símbolos. Para resolver este problema, esta variável, em particular, foi definida como persistente e o GDB pode, agora, acessar as informações necessárias depois, durante a sessão de depuração, sem ler uma região de memória inválida.

nscd foi atualizado para carregar automaticamente os dados de configuração

Esta atualização do nscd (Name Server Caching Daemon) adiciona um sistema de monitoramento baseado em inotify e de monitoramento de backup baseado em estatísticas para os arquivos de configuração nscd, assim o nscd detecta corretamente as alterações às suas configurações e recarrega os dados. Isto impede que o nscd retorne dados obsoletos.

A função da biblioteca dlopen não colide mais com as chamadas recursivas

Anteriormente, um defeito na função da biblioteca **dlopen** podia fazer com que as chamadas recursivas nesta função abortassem ou colidissem com uma asserção da biblioteca. As chamadas recursivas são possíveis se uma implementação **malloc** fornecida pelo usuário chamar **dlopen**.

A implementação é agora reentrante e as chamadas recursivas não abortam ou colidem mais com uma asserção.

A ferramenta operf reconhece identificadores de páginas enormes e estáticas

Anteriormente, ao criar o perfil de desempenho de código Java compilado just-in-time (JIT) com páginas estáticas e enormes habilitadas, o comando operf do OProfile registrava um grande número de amostras de evento na memória anônima (em anon_hugepage), ao invés de fazer o registro no método Java apropriado. Com esta atualização, operf reconhece os identificadores de páginas estáticas e enormes e mapeia as amostras corretamente aos métodos Java, quando usando páginas enormes alocadas estatisticamente.

`rsync -X` funciona corretamente

Anteriormente, a ferramenta **rsync** alterava a propriedade do arquivo depois, e não antes, de configurar os atributos de segurança. Como consequência, os atributos de segurança no destino ficavam ausentes e a execução do comando **rsync -X** não funcionava adequadamente sob algumas circunstâncias. Com esta atualização, a ordem das operações foi trocada e o **rsync**, agora, altera as propriedades antes da configuração dos atributos de segurança. Como resultado, os atributos de segurança ficam presentes, como esperado, na situação descrita.

Executáveis do subversion são criados com dados RELRO completos

Os executáveis fornecidos com o pacote *subversion* são agora criados com dados de realocação em modo somente leitura (RELRO), o que oferece proteção contra alguns tipos de ataques à corrupção de memória. Como resultado, será mais difícil explorar Subversion, caso futuras vulnerabilidades sejam descobertas.

A extensão de thread na TCL funciona corretamente

Antigamente, o suporte a threads na Linguagem de Comandos de Ferramentas (TCL) não era implementado da maneira ideal. Se a chamada fork() fosse usada junto com a extensão de thread habilitada no intérprete de TCL, o processo poderia ficar sem resposta. Por causa disso, o intérprete de TCL e o aplicativo TK eram enviados junto com a extensão de thread desabilitada. Como consequência, os aplicativos de terceiros dependentes de TCL ou TK com thread não funcionavam corretamente. Agora, uma correção foi implementada a este erro e a TCL e o TK possuem a extensão de thread habilitada por padrão.

Os conjuntos de codificação AES podem ser habilitados ou desabilitados explicitamente para TLS

Com os pacotes curl atualizados, é possível habilitar ou desabilitar explicitamente os novos conjuntos de codificação do Padrão Avançado de Criptografia (AES) a ser usado para o protocolo TLS.

OpenJDK 7 fornece suporte a ECC

Com esta atualização, o OpenJDK 7 passa a fornecer suporte à ECC (Elliptic Curve Cryptography) e às codificações associadas para conexões TLS. A ECC é, na maioria das vezes, usada em preferência a soluções mais antigas de criptografia para a realização de conexões de rede seguras.

O ABRT é capaz de salvar arquivos core_backtrace em vez de todo um despejo de memória

O ABRT agora pode ser configurado para gerar um backtrace sem escrever um arquivo de despejo de memória no disco. Isto pode economizar tempo ao trabalhar com processos que alocam grandes blocos de memória. Este recurso pode ser habilitado configurando a opção **`CreateCoreBacktrace`** como **`yes`** e a opção **`SaveFullCore`** como **`no`** no arquivo **`/etc/abrt/plugins/CCpp.conf`**.

Recursos de segurança adicionados à biblioteca padrão Python

Vários aprimoramentos de segurança, descritos na Proposta de Aprimoramento do Python 446 (http://legacy.python.org/dev/peps/pep-0466/), foram transferidos da versão upstream mais atual para a biblioteca padrão do Python. Estes aprimoramentos incluem, por exemplo, novos recursos no módulo **`ssl`**, como o suporte para a Indicação de Nome de Servidor (SNI), assim como o suporte para novos protocolos TLSv1.x, novos algorítimos hash em **`hashlib module`**, entre outros.

Novas configurações globais para a verificação do certificado SSL/TLS na biblioteca padrão do Python

Foram adicionadas novas opções que permitem aos usuários habilitar ou desabilitar a verificação do certificado SSL/TLS nos clientes HTTP (como urllib, httplib ou xmlrpclib) da biblioteca padrão do Python. As opções estão descritas na Proposta de Aprimoramento do Python 493 (https://www.python.org/dev/peps/pep-0493/). O valor padrão não verifica os certificados. Para mais detalhes, consulte https://access.redhat.com/articles/2039753.

Capítulo 6. Área de trabalho (Desktop)

Rebase do GNOME para a versão 3.14

O **GNOME Desktop** foi atualizado para a versão upstream 3.14 (com algumas adições da versão 3.16), a qual inclui novos recursos e vários aprimoramentos, como:

O Red Hat Enterprise Linux 7.2 adiciona o **GNOME Software**, uma nova maneira de instalar e gerenciar software no sistema do usuário baseado em um yum backend. O GNOME PackageKit permanece como o atualizador padrão do GNOME (também instalado por padrão). Com o **GNOME Software**, o usuário gerencia um ambiente integrado com as tarefas relacionadas ao software, tais como navegação, instalação e remoção de aplicativos, e visualização e instalação de atualizações do software.

Na barra superior, os grupos recém-nomeados **System Status Menu** unem todos os indicadores e applets geralmente acessados individualmente - barra de brilho, modo avião aprimorado, conexão a redes Wi-Fi, Bluetooth, Volume, entre outros - a um menu compacto e coerente. Com relação ao Wi-Fi, o GNOME 3.14 fornece um suporte melhor aos hotspots Wi-Fi. Ao conectar-se a um portal Wi-Fi que exige autenticação, o GNOME agora exibe a página de login automaticamente, como parte do processo de conexão.

A combinação de chaves padrão para o bloqueio de tela foi alterada. O atalho padrão anterior **Ctrl+Alt+L** foi substituído pela combinação de chaves **Super key+L**.

O novo design do editor de texto **gedit** incorpora todos os recursos anteriores em uma interface mais compacta, a qual fornece mais espaço para trabalhar. O uso de popovers para a seleção do formato de documentos e da largura de abas está mais eficiente, comparado ao uso anterior das caixas de diálogo e menus. O controle da barra lateral também possibilita mais espaço, ao mesmo tempo que mantém a funcionalidade original. Outras melhorias importantes incluem novos atalhos para a abertura da última aba fechada, com **Ctrl+Shift+T**, e para a alteração de letras maiúsculas e minúsculas.

Nautilus, o gerenciador de arquivos do GNOME, agora utiliza a combinação de chaves **Shift+Ctrl+Z**, e não **Ctrl+Y**, para a operação **redo**. Além disto, uma barra de cabeçalho, em vez de uma barra de ferramentas, é usada agora.

O GNOME 3.14 inclui uma versão reformulada do aplicativo **Videos**. Com um estilo moderno, a nova versão permite que o usuário navegue por vídeos no computador, assim como por canais de vídeos online. O aplicativo **Videos** também inclui uma nova visualização de playback, fornecendo uma experiência ainda mais otimizada que a versão anterior: controles de playback flutuantes ocultos, quando o usuário não necessita deles, e a visualização de playback em tela cheia com uma aparência mais refinada.

Os recursos do **Evince** melhoraram a acessibilidade para a leitura de arquivos em PDF. A nova versão do visualizador de documentos utiliza uma barra de cabeçalho que fornece mais espaço para os seus documentos. Quando o **Evince** é lançado sem um documento especificado, ele exibe uma visão geral bastante útil dos seus documentos mais recentes. A última versão do **Evince** também inclui um **High Resolution Display Support** e uma melhor acessibilidade, com links, imagens e campos de formatos, todos disponíveis a partir de tecnologias assistivas.

A nova versão do aplicativo **Weather** do GNOME utiliza a nova estrutura de geolocalização do GNOME que exibe automaticamente as condições climáticas da sua atual localização e um novo layout que oferece uma maneira mais efetiva de ler as previsões do tempo.

Este lançamento também traz um suporte melhorado para os comentários no **LibreOffice** - importação e exportação de comentários aninhados em filtros RTF, DOCX, DOC e ODF, impressão de comentários nas margens e formatação de todos os comentários.

O aplicativo GNOME para máquinas remotas e virtuais, **Boxes**, introduz snapshots. Além disso, **Boxes** agora fornece download automático, executando múltiplas caixas em janelas diferentes, e aprimoramentos na interface do usuário, incluindo um melhor comportamento da tela cheia e de miniaturas.

O visualizador de documentação **Help** do GNOME foi reformulado para ficar consistente com outros 3 aplicativos do GNOME. Help agora usa uma barra de cabeçalho, possui uma função de pesquisa integrada e uma interface de marcação.

O **GTK+** 3.14 inclui várias correções de erros e aprimoramentos, tais como carregamento automático de menus de recursos, suporte a seleções múltiplas em **GtkListBox**, ligações de propriedades em arquivos **GtkBuilder**, suporte a desenhos fora de uma alocação do widget (gtk_widget_set_clip()), novos tipos de transição em GtkStack e carregamento e salvamento de arquivos com **GtkSourceView**. Além disso, **GTK+** agora fornece suporte à interação de gestos. Com a versão 3.14, a maioria dos gestos multitoque comuns está disponível para uso em aplicativos GTK+, como tocar, arrastar, passar, pinçar e girar. Os gestos podem ser adicionados aos aplicativos GTK+ existentes usando **GtkGesture**.

A Extensão do Gnome Shell, **Looking Glass Inspector**, recebeu vários recursos para os desenvolvedores: exibe todos os métodos, as classes e etc em um namespace mediante inspeção, expansão do histórico do inspetor de objetos ou copia os resultados do **Looking Glass** como sequências de caracteres e passa-os por eventos para o gnome-shell.

O recurso **High Resolution Display Support** foi estendido para incluir os principais aspectos da experiência GNOME 3, como a Visão Geral de Atividades, a animação na Visão Geral de Atividades junto com as animações de janela, a Barra Superior, o bloqueio de tela e a caixa de diálogos de sistemas.

No que diz respeito ao GNOME Extensions, este lançamento introduz suporte ao posicionamento alternativo do dock, incluindo a parte inferior da tela, em **Simple Dock**, um dock para o Gnome Shell.

O pacote ibus-gtk2 agora atualiza o arquivo immodules.cache

O script **update-gtk-immodules** costumava pesquisar por um diretório que não existe mais **/etc/gtk-2.0/$host**. Como consequência, o script de pós-instalação do pacote*ibus-gtk2* falhava e era finalizado sem a criação ou atualização do cache. O script de pós-instalação foi modificado agora para substituir **update-gtk-immodules** por **gtk-query-immodules-2.0-BITS** e o problema deixou de ocorrer.

Capítulo 7. Sistemas de Arquivos

Rebase do gfs2-utils para a versão 3.1.8

O pacote *gfs2-utils* foi rebaseado para a versão 3.1.8, a qual fornece importantes correções e diversos aprimoramentos:

* O desempenho dos utilitários **`fsck.gfs2`**, **`mkfs.gfs2`** e **`gfs2_edit`** foi aprimorado.

* O utilitário **`fsck.gfs2`** agora possui um desempenho melhor na verificação de diários, do jindex, dos números de série dos arquivos do sistema e dos valores 'meta' dos números de série.

* Os utilitários **`gfs2_jadd`** e **`gfs2_grow`** são agora programas separados, ao invés de symlinks para **`mkfs.gfs2`**.

* O conjunto de testes e as documentações relacionadas foram aprimoradas.

* O pacote não depende mais de Perl.

GFS2 impede os usuários de exceder as suas cotas

Anteriormente, o GFS2 verificava as violações de cotas somente após a conclusão das operações, o que podia resultar em usuários ou grupos excedendo as suas cotas alocadas. Este comportamento foi corrigido e o GFS2 agora prevê o número de blocos que uma operação alocaria e verifica se a alocação deles violaria as cotas. As operações que podem resultar em violações de cotas não são permitidas, assim os usuários nunca excedem as suas cotas alocadas.

Rebase do XFS para a versão 4.1

O XFS foi atualizado para a versão upstream 4.1, incluindo correções de erros secundários, refatoração, reformulação de certos mecanismos internos, tais como registro em log, contabilidade pcpu e novos bloqueios mmpa. Além das alterações upstream, esta atualização estende a função rename() para adicionar cross-rename (uma variante simétrica do rename()) e o manejo de whiteout.

Rebase do cifs para a versão 3.17

O módulo CIFS foi atualizado para a versão upstream 3.17, a qual fornece várias correções secundárias e novos recursos para o Bloco de Mensagens de Servidor (do inglês, Server Message Block) 2 e 3 (SMB2 e SMB3).

Alterações no NFS no Red Hat Enterprise Linux 7.2

O suporte ao fallocate permite a pré-alocação de arquivos no servidor. As extensões SEEK_HOLE e SEEK_DATA à função fseek() possibilitam localizar falhas e dados rapidamente e eficazmente. O Red Hat Enterprise Linux 7.2 também fornece suporte ao layout de arquivo flexível nos clientes NFSv4 descritos na seção de Apresentação Prévia de Tecnologia.

Capítulo 8. Habilitação do Hardware

Cartões OSA-Express5s com suporte em qethqoat

O suporte aos cartões OSA-Express5s foi adicionado à ferramenta qethqoat, parte do pacote s390utils, no Red Hat Enterprise Linux 7.1 como uma Apresentação Prévia de Tecnologia. Esta atualização de melhoria fornece suporte completo à operacionalidade estendida da rede e às configurações dos cartões OSA-Express5s.

Capítulo 9. Instalação e Inicialização

Configuração de rede corrigida em initrd, caso a configuração da rede seja fornecida em Kickstart

Anteriormente, o instalador falhava ao configurar ou reconfigurar as interfaces de rede em **`initrd`**, se essas interfaces fossem definidas nos arquivos Kickstart. Isto poderia provocar uma falha de instalação e entrada no modo de emergência, caso o acesso à rede fosse exigido por outros comandos no arquivo Kickstart.

Este problema está agora resolvido e Anaconda manipula a configuração de rede dos arquivos Kickstart em **`initrd`** adequadamente, no começo do processo de inicialização.

Anaconda agora oferece suporte à criação de volumes lógicos em cache

O instalador agora oferece suporte à criação de volumes lógicos LVM em cache e à instalação do sistema nesses volumes.

Atualmente, esta abordagem possui suporte somente no Kickstart. Para criar um volume lógico em cache, utilize as novas opções **`--cachepvs=`**, **`--cachesize=`** e **`--cachemode=`** do comando **`logvol`** do Kickstart.

Consulte o Guia de Instalação do Red Hat Enterprise Linux 7 para informações mais detalhadas sobre essas novas opções.

Melhor classificação do menu de inicialização do GRUB2

Os problemas com o mecanismo de classificação usado pelo comando **`grub2-mkconfig`** faziam com que o arquivo de configuração grub.cfg fosse gerado com os kernels disponíveis classificados de forma incorreta.

Agora, o GRUB2 utiliza o pacote *rpmdevtools* para classificar os kernels disponíveis e o arquivo de configuração está sendo gerado corretamente com a versão mais recente do kernel no topo da lista.

Anaconda reverte agora corretamente as ações de disco quando há alterações na seleção de disco

Anteriormente, Anaconda e Blivet não revertiam de forma correta as ações agendadas nos discos quando a seleção de disco era modificada, gerando vários problemas. Com esta atualização, Anaconda foi corrigido para criar um snapshot da configuração de armazenamento original e retornar a ele quando houver alterações na seleção de disco, revertendo completamente todas as ações agendadas para os discos.

Detecção aprimorada dos nomes de disco do device-mapper

Na versão anterior do Red Hat Enterprise Linux 7, o instalador costumava falhar quando instalando em discos que continham os volumes lógicos LVM e os metadados para esses volumes ainda estavam presentes. O instalador não podia reconhecer os nomes corretos do **`device-mapper`** e o processo de criação dos novos volumes lógicos LVM falhavam.

O método utilizado para obter os nomes do dispositivo **`device-mapper`** foi atualizado e a instalação nos discos que continham metadados LVM existentes está agora mais confiável.

Manipulação da Inicialização PReP corrigida durante particionamento

Em algumas situações, a partição **PReP Boot** no IBM Power Systems podia ser definida com um tamanho inválido durante a personalização do particionamento. Nesses casos, a remoção de qualquer partição causava falha no instalador.

Agora, as verificações são implementadas no *anaconda* garantindo que a partição tenha sempre o tamanho correto, entre **4096 KiB** e **10 MiB**. Além disto, não é mais necessário alterar o formato da partição**PReP Boot** para alterar o seu tamanho.

Partições EFI nos dispositivos RAID1

As Partições do Sistema EFI podem ser criadas agora em um dispositivo RAID1 para habilitar a recuperação do sistema, quando há falha em um disco de inicialização. No entanto, já que é garantido que o sistema descubra somente uma Partição do Sistema EFI, se o volume do ESP que é descoberto pelo firmware torna-se corrompido (mas, ainda aparenta ser um ESP válido) e ambos, **Boot####** e **BootOrder**, tornam-se corrompidos, então a ordem de inicialização não será recriada automaticamente. Neste caso, o sistema ainda deve ser inicializado manualmente a partir do segundo disco.

A instalação em modo texto não gera mais falhas durante a configuração de rede

Anteriormente, na tela de Configuração de Rede na instalação interativa em modo texto, o uso de um espaço na especificação de nameservers gerava falhas no instalador.

Agora, anaconda manipula os espaços nas definições de nameservers no modo texto de forma correta e não há mais falhas no processo de instalação, caso um espaço seja usado para separar os endereços de nameservers.

As telas do modo de resgate no IBM System z não são mais cortadas

Anteriormente, a segunda e a terceira tela no modo de resgate nos servidores do IBM System z estavam sendo exibidas inadequadamente e partes da interface estavam cortadas. O modo de resgate nesta arquitetura agora melhorou e todas as telas funcionam corretamente.

Complemento OpenSCAP em Anaconda

Agora é possível aplicar o conteúdo do Protocolo de Automação de Conteúdos de Segurança (em inglês, Security Content Automation Protocol - SCAP) durante o processo de instalação. Este novo complemento ao instalador possibilita a configuração fácil e confiável de políticas de segurança sem ter que depender de scripts personalizados.

Este complemento fornece uma nova seção Kickstart ("%addon org_fedora_oscap"), assim como uma nova tela na interface gráfica do usuário durante a instalação interativa. Todas as três partes estão documentadas no Guia de Instalação do Red Hat Enterprise Linux 7.

A aplicação de políticas de segurança durante uma instalação desempenhará várias alterações durante e imediatamente após a instalação, dependendo de qual política você ativar. Caso um perfil seja selecionado, o pacote *openscap-scanner* (uma ferramenta de verificação de conformidade com OpenSCAP) é adicionado à sua seleção de pacote e uma verificação de conformidade inicial é desempenhada após o fim da instalação. Os resultados desta verificação ficam salvos em **/root/openscap_data**.

Vários perfis são fornecidos na mídia de instalação pelo pacote *scap-security-guide*. Você também pode carregar outros conteúdos, tais como o processamento de fluxo de dados, arquivos ou um pacote RPM de um servidor HTTP, HTTPS ou FTP, se necessário.

Observe que não é necessária a aplicação de uma política de segurança em todos os sistemas. Este complemento deve ser usado somente quando as regras da sua organização ou as regulamentações governamentais determinam uma política específica, caso contrário o complemento pode ser deixado no seu

estado padrão, o qual não aplica nenhuma política de segurança.

Anaconda não atinge tempo limite mais quando esperando por um arquivo Kickstart em um CD ou DVD

Antigamente, se o Anaconda fosse configurado para carregar um arquivo Kickstart de uma mídia óptica usando o comando **`inst.ks=cdrom:/ks.cfg`**, e se o sistema fosse inicializado de um CD ou DVD também, o instalador aguardava por apenas 30 segundos para que o usuário trocasse o disco. Depois que este período de tempo passava, o sistema entrava em modo de emergência.

Com esta atualização, o Anaconda foi modificado para nunca mais atingir tempo limite ao aguardar pelo fornecimento de um arquivo Kickstart em um CD ou DVD pelo usuário. Se as opções de inicialização **`inst.ks=cdrom`** são usadas e o arquivo Kickstart não é detectado, o Anaconda agora exibe um aviso e aguarda até que o usuário forneça o arquivo ou reinicialize.

Capítulo 10. Kernel

Suporte para kpatch

O utilitário **kpatch** permite que os usuários gerenciem uma coleção de patches no kernel binário, o qual pode ser usado para aplicar patches no kernel dinamicamente, sem reinicialização. Anteriormente, o **kpatch** era incluído como uma Apresentação Prévia de Tecnologia e, agora, possui suporte completo ao ser usado sob a direção da equipe Red Hat Customer Experience and Engagement.

Para mais detalhes sobre o suporte à aplicação de patches no kernel, consulte https://access.redhat.com/solutions/2206511.

Os parâmetros SHMMAX e SHMALL do kernel retornaram para os valores padrão

Anteriormente, os valores dos parâmetros **`kernel.shmmax`** e **`kernel.shmall`**, que eram estabelecidos no arquivo **`/usr/lib/sysctl.d/00-system.conf`**, eram muito baixos. Como consequência, alguns aplicativos, como SAP, não funcionavam propriamente. As substituições inadequadas foram removidas e os padrões kernel, que são suficientemente altos, podem ser usados agora.

Páginas enormes e transparentes não corrompem mais a memória

As páginas enormes e transparentes não estavam sendo sincronizadas corretamente durante as operações de leitura e gravação. Em algumas circunstâncias, isto resultava em corrupção de memória, quando páginas enormes e transparentes eram habilitadas. Portanto, barreiras de memória foram adicionadas à manipulação das páginas enormes e transparentes para que a corrupção de memória não ocorra mais.

Rebase do SCSI LIO

O destino SCSI do kernel, LIO, foi rebaseado do Linux-4.0.stable, incluindo a correção de vários erros, principalmente para iSER, mas também incluindo a adição de suporte aos comandos XCOPY, WRITE SAME e ATS e suporte à integridade dos dados DIF.

makedumpfile passa a oferecer suporte ao novo formato sadump, representando mais de 16 TB de memória físca

O comando makedumpfile agora oferece suporte ao novo formato sadump, que pode representar mais de 16 TB de espaço de memória física. Isto permite aos usuários de makedumpfile ler arquivos de despejo com mais de 16 TB, gerados por sadump em certos modelos de servidor futuros.

A remoção ou atualização do kernel não exibe mais um aviso

O script weak-modules, que é usado pelo **`kmod`** para gerenciar os links simbólicos de módulos compatíveis com kABI (kABI-compatible), removia antigamente o diretório **`/lib/modules/<version>/weak-updates`** quando removendo os arquivos associados a um kernel. Este diretório pertence ao pacote *kernel* e a remoção dele gerava inconsistência entre o sistema de arquivo e o estado esperado pelo **`rpm`**. Isto também gerava um aviso que era exibido toda vez que um kernel era atualizado ou removido.

O script foi atualizado para remover os conteúdos do diretório **`weak-updates`**, mas manter o diretório em si, e não exibir mais os avisos.

Novo pacote: libevdev

Libevdev é uma biblioteca de baixo nível para a interface de dispositivos de eventos de entrada do kernel do

Linux. O pacote fornece interfaces seguras para a consulta dos recursos de dispositivos e o processamento dos eventos dos dispositivos. As versões atuais do xorg-x11-drv-evdev e xorg-x11-drv-synaptics necessitam desta biblioteca como uma dependência.

Tuned é executado no modo no-daemon

Anteriormente, Tuned podia executar somente como um daemon, o que podia afetar o desempenho dos sistemas pequenos por causa do volume de memória do Tuned daemon. Com esta atualização, o modo no-daemon (monoestável), que não exige memória residente alguma, foi adicionado ao Tuned. O modo no-daemon vem desabilitado por padrão porque muitas das funcionalidades do Tuned estão ausentes neste modo.

Novo pacote: tuned-profiles-realtime

O pacote *tuned-profiles-realtime* foi adicionado ao Red Hat Enterprise Linux Server e ao Red Hat Enterprise Linux for Real Time. Ele contém um perfil em tempo real usado pelo utilitário **`tuned`** para desempenhar isolamentos de CPU e ajustes de IRQ. Quando o perfil é ativado, ele lê sua seção variável, a qual especifica as CPUs a serem isoladas, e move todas as threads que podem ser tiradas desses núcleos da CPU.

As mensagens de erro de SCSI podem ser facilmente interpretadas

As alterações anteriormente introduzidas ao kernel referentes à função printk() resultavam nas mensagens de erro da Interface de Sistemas para Pequenos Computadores (SCSI) sendo registradas em múltiplas linhas. Como consequência disto, se múltiplos erros ocorressem em diferentes dispositivos, ficava difícil interpretar corretamente as mensagens de erro. Essa atualização muda agora o código de registro de erro da SCSI para um registro de mensagens de erro que usa a opção dev_printk(), a qual associa as mensagens de erro com o dispositivo que gerou o erro.

Drivers e subsistema libATA atualizados

Esta atualização fornece diversas correções de erros e aprimoramentos aos drivers e ao subsistema libATA.

FCoE e DC foram atualizados

Os componentes do kernel Fibre Channel sobre Ethernet (FCoE) e Data Center Bridging (DCB) foram atualizados para as versões upstream mais recentes, as quais fornecem várias correções de erros e aprimoramentos em relação às versões anteriores.

Rebase do `perf` para a versão 4.1

Os pacotes *perf* foram atualizados para a versão upstream 4.1, a qual fornece várias correções de estabilidade e desempenho e aprimoramentos em relação à versão anterior. Este rebase acrescenta, em especial, os recursos Intel Cache QoS Monitoring e AMD IBS Ops e fornece suporte ao Intel Xeon v4, para módulos do kernel compactados para eventos parametrizados, e suporte para a especificação da duração de pontos de interrupção. Além disso, diversas opções foram adicionadas à ferramenta **`perf`**, tais como **`--system-wide`**, **`top -z`**, **`top -w`**, **`trace --filter-pids`** e **`trace --event`**.

Suporte ao TPM 2.0

Esta atualização adiciona um suporte no âmbito de drivers para os dispositivos Trusted Platform Module (TPM) compatíveis com a versão 2.0.

`turbostat` agora fornece saída correta

Antigamente, a ferramenta **`turbostat`** detectava se o sistema oferecia suporte ao dispositivo MSR ao ler o arquivo /dev/cpu/0/msr como **`cpu0`** no lugar de **`cpu`**. Como consequência, a desabilitação de uma CPU removia as CPUs de saída do turbostat. Agora, este erro foi corrigido e a execução do comando **`turbostat ls`** retorna a saída correta.

`turbostat` fornece suporte aos processadores Intel Xeon v5

Este aprimoramento adiciona o suporte do processador Intel Xeon v5 à ferramenta **`turbostat`**.

A ferramenta `zswap` faz uso da API `zpool`

Anteriormente, a ferramenta **`zswap`** utilizava **`zbud`** diretamente, um pool de armazenamento que armazena páginas compactadas a uma proporção de 2:1 (quando cheio). Esta atualização introduz a API **`zpool`**, que fornece acesso ao pool **`zsmalloc`** ou ao pool **`zbud`**: **`zsmalloc`** armazena páginas compactadas a uma densidade provavelmente maior, resultando em mais memória recuperada para as páginas altamente compressíveis. Junto com esta atualização, **`zsmalloc`** foi promovido aos drivers /mm para que **`zpool`** funcione como esperado.

O tamanho do arquivo /proc/pid/cmdline passa a ser ilimitado

O limite de tamanho do arquivo /proc/pid/cmdline para o comando **`ps`** era, anteriormente, codificado no kernel para 4096 caracteres. Esta atualização assegura que o tamanho dos arquivos /proc/pid/cmdline seja ilimitado, o que é particularmente benéfico para os processos de listagem com argumentos de linha de comando longos.

dma_rmb e dma_wmb passam a receber suporte

Esta atualização introduz dois novos primitivos para a sincronização de leituras e gravações de memórias com coerência de cache, dma_wmb() e dma_rmb(). Este recurso estará disponível em drivers para uso adequado.

Conexão do driver qib HCA

Devido a uma incompatibilidade no ID de LOGIN do SRP, o destino do SRP obtinha erros antigamente ao conectar-se com o driver do dispositivo qib HCA. Esta atualização corrige este erro e a conexão agora pode ser estabelecida com êxito.

Aumento no limite de memória

A partir do Red Hat Enterprise Linux 7.2, o limite máximo de memória com suporte nos sistemas Intel 64 e AMD64 aumentou de 6 TB para 12 TB.

Novo pacote: *WALinuxAgent*

A versão 2.0.13 do Microsoft Azure Linux Agent (WALA) passou a ser incluída no canal Extras. Este agente fornece suporte ao provisionamento e à execução das Máquinas Virtuais Linux no Windows Azure cloud e deve ser instalado nas imagens Linux compiladas para executar no ambiente Windows Azure.

Capítulo 11. Sistema de Rede

SNMP agora obedece corretamente o diretivo clientaddr em relação ao IPv6

Anteriormente, a opção **clientaddr** em **snmp.conf** afetava somente as mensagens de saída enviadas via IPv4. Com este lançamento, as mensagens IPv6 de saída são corretamente enviadas da interface especificada por **clientaddr**.

tcpdump fornece suporte às opções -J, -j e --time-stamp-precision

Como o **kernel**, **glibc** e **libpcap** fornecem APIs agora para obter carimbos de data e hora de resoluções em nanossegundos, **tcpdump** foi atualizado para melhor proveito desta funcionalidade. Agora, os usuários podem consultar quais fontes de carimbo de data e hora estão disponíveis (-J), definir uma fonte específica de carimbo de data e hora (-j) e solicitar carimbos de data e hora com uma resolução específica (--time-stamp-precision).

Rebase do TCP/IP para a versão 3.18

A pilha TCP/IP foi atualizada para a versão upstream 3.18, a qual fornece várias correções de erros e aprimoramentos em relação à versão anterior. Esta atualização corrige, em especial, a extensão de abertura rápida do TCP, funcionando agora como esperado ao usar IPv6. Além disso, esta atualização fornece suporte para o autocorking TCP opcional e implementa DCTCP (em inglês, Data Center TCP).

Rebase do NetworkManager libreswan para a versão 1.0.6

Diversas correções de erros e aprimoramentos foram incorporados do upstream, como, por exemplo:

* O tratamento de senha passa a ser mais robusto

* O início e o término da conexão passam a ser mais robustos

* A rota padrão passa a ser autodetectada nas rotas enviadas

* Suporte adicionado às solicitações de senha interativas

* Anúncio errôneo da capacidade de exportação e importação corrigido

O NetworkManager fornece suporte à configuração do MTU de uma interface vinculada

Ambos, 'nmcli' e a interface GUI, agora permitem a configuração do MTU em uma interface vinculada.

O NetworkManager valida as opções do MTU de Anúncio de Roteador IPv6 antes de aplicá-las

Os nós maliciosos e configurados incorretamente poderiam enviar um MTU IPv6 que deixaria outras comunicações de rede problemáticas ou impossíveis, se aplicada. O NetworkManager trata de maneira adequada esses eventos e mantém a conectividade IPv6.

As extensões de Privacidade do IPv6 passam a ser habilitadas por padrão

Para determinar e definir as configurações de privacidade do IPv6 na ativação do dispositivo, o NetworkManager agora verifica a sua configuração de rede no NetworkManager.conf por padrão e retorna para **`/proc/sys/net/ipv6/conf/default/use_tempaddr`**, se necessário.

O Painel de Rede control-center passa a exibir recursos de dispositivos WiFi

As frequências operacionais de dispositivos WiFi com suporte agora são exibidas no painel de controle control-center.

O NetworkManager passa a tratar adequadamente os conflitos de rota quando múltiplas interfaces apontam para o mesmo gateway

O NetworkManager agora mantém registro das rotas configuradas e evita tentar configurar as rotas em conflito. Quando uma rota em conflito não está mais ativa, ela é removida.

Correção para blecaute de rede com conexões multihomed

O NetworkManager agora evita um blecaute de rede durante a ativação do segundo dispositivo em uma conexão multihomed.

Nova opção para impedir que o NetworkManager substitua `ip route add`

A nova opção 'never-default' foi adicionada à configuração IP de conexão. Esta opção impede o NetworkManager de configurar a própria rota padrão, permitindo que o administrador defina rotas padrão diferentes, conforme necessário.

Correção para os erros legados do network.service quando Carrier Down é detectado em alguns hardware

Quando um dispositivo não obtém nenhum carrier durante a inicialização, o NetworkManager aguarda pela detecção do carrier, em vez de fazer com que a ativação falhe imediatamente.

O NetworkManager fornece suporte a Wake On Lan

O utilitário nmcli agora permite que o **`Wake on Lan`** seja configurado conforme o dispositivo.

Suporte aprimorado para as zonas firewalld com conexões VPN

Ao configurar uma zona firewall para uma conexão VPN baseada em dispositivo, ela é configurada corretamente agora no firewalld.

Agendador de pacotes Fair Queue passa a ter suporte

O agendador de pacotes Fair Queue, conhecido como **`fq`**, foi adicionado ao Red Hat Enterprise Linux 7.2 e pode ser selecionado usando o utilitário **`tc`** (traffic controller).

Suporte adicionado à coalescência de transmissão

A extensão **`xmit_more`** foi implementada, melhorando o desempenho de transmissão do virtio-net e de outros drivers, principalmente quando o TSO (TCP Segmentation Offload) está desabilitado.

Desempenho aprimorado no recebimento de frames de rede

Ao refatorar o código para eliminar as operações de restauração e salvamento de IRQ na alocação de memória NAPI, reduziu-se a latência no recebimento dos frames de rede.

Desempenho altamente melhorado nas procuras de rotas

O código FIB do IPv4 (Forward Information Base) foi atualizado a partir do upstream para a melhora de seu desempenho.

Suporte ao Namespace da Rede para Interfaces Virtuais

A id netns passa a obter suporte em interfaces virtuais, possibilitando o controle confiável das interfaces de rede vinculadas por todos os limites do namespace da rede.

Os contêineres LXC e Docker agora podem ler net.ipv4.ip_local_port_range

O suporte ao namespace da rede para o net.ipv4.ip_local_port_range sysctl foi adicionado, melhorando o suporte ao contêiner para o software que necessita de acesso a esta informação.

Notificação melhorada das rotas IPv6 autoconfiguradas pela ferramenta 'ip'

A ferramenta **`ip`** não podia obter as informações de hoplimit e mtu de Anúncios de Rota e isto foi corrigido.

As opções de soquete de pilha dual agora são exportadas corretamente

Os soquetes AF_INET6 são exclusivos do IPv6, quando o IPV6_V6ONLY está configurado. Em todos os outros casos, o soquete também é compatível com o IPv4. Esta informação é adequadamente exportada e pode ser interrogada usando iproute2.

Data Center TCP passa a ter suporte

Este lançamento inclui uma implementação do DCTCP para melhorar o desempenho da rede nos ambientes Data Center. O parâmetro **`dctcp`** pode ser definido no **`sysctl`** ou conforme a rota com **`ip route`**.

Controle de Congestionamento por Rota

Para habilitar algorítimos diferentes de controle de congestionamento conforme a rota, o parâmetro **`congctl`** foi adicionado ao **`ip route`**.

Tratamento melhorado da Janela de Congestionamento para TCP Cubic e Reno ao usar GRO

O método para determinar o dimensionamento da largura de banda e da janela de congestionamento foi aprimorado, reduzindo o número de pacotes ACK necessários para a transmissão de grandes volumes de dados.

TCP Pacing passa a ter suporte

O parâmetro **`SO_MAX_PACING_RATE`** foi adicionado, possibilitando um maior controle da taxa de produtividade para ambientes onde ela é considerada.

Suporte para o cliente e servidor TFO

O recurso TCP Fast Open foi adicionado, usando o número de opção atribuído RFC 7413.

Mitigação dos loops TCP ACK

O tratamento dos TCP ACKs duplicados melhorou, impedindo alguns problemas ou middleboxes potencialmente maliciosos.

Suporte mínimo para os pontos de extremidade secundários com nf_conntrack_proto_sctp

Suporte básico à hospedagem múltipla (multihoming) foi adicionado ao SCTP.

Implementação AF_UNIX rebaseada

O código AF_UNIX (às vezes chamado de AF_LOCAL) foi atualizado para incluir vários erros e melhorias. Em particular, sendpage e splice (também conhecido como zerocopy) agora possuem suporte.

Suporte ao encapsulamento do kernel foi rebaseado para a versão upstream

Os drivers de encapsulamento do kernel foram atualizados do kernel 4, com várias correções e melhorias, principalmente para o VXLAN.

Suporte adicionado para o cruzamento de namespaces de rede (x-netns) nos túneis GRE

Tanto gre quanto ip6gre possuem suporte agora para x-netns.

Desempenho melhorado ao executar Tráfego da Máquina Virtual em VXLAN

O código de hash do fluxo de transmissão foi atualizado, resultando em um melhor desempenho quando o tráfego originário de uma máquina virtual é direcionado para um encapsulamento.

Descarregamento melhorado para os frames VLAN recebidos em um VXLAN ou a partir de encapsulamentos GRE

Várias alterações foram introduzidas para habilitar o suporte ao GRO e melhorar o desempenho sob encapsulamento VXLAN e NVGRE.

Desempenho aprimorado do encapsulamento Open vSwitch

O recurso do dispositivo **`tx-nocache-copy`** agora está desabilitado por padrão. O padrão anterior criava uma sobrecarga significante para muitos volumes de trabalho e, principalmente, para os encapsulamentos OVS em execução sob um VXLAN.

Tratamento IPsec aprimorado

O IPsec foi atualizado para fornecer várias correções e algumas melhorias. É importante notar que, este lançamento agora fornece a habilidade de corresponder a interfaces de saída.

Inclusão do suporte ao VT16 com capacidades netns

Interfaces de Encapsulamento Virtual para IPv6, incluindo capacidades netns, foram adicionadas ao kernel.

O valor padrão de nf_conntrack_buckets foi aumentado

Caso não seja especificado como parâmetro durante o carregamento de módulos, o número padrão de buckets é calculado através da divisão da memória total por 16384. A tabela de hash nunca terá menos que 32 e está limitada a 16384 buckets. Para sistemas com mais de 4GB de memória, no entanto, este limite será de 65536 buckets.

Melhorias no uso de memória para iptables em máquinas SMP com grande capacidade

Antigamente, grandes rulesets iptables podiam usar quantidades significantes de memória mesmo sem necessidade, já que o armazenamento de ruleset era realizado conforme a CPU (se possível). A sobrecarga de memória foi reduzida, alterando a forma como rulesets são armazenados.

Driver de vinculação de rede atualizado

Para melhorar a manutenção, o driver de vinculação de rede do kernel foi atualizado para alinhar-se com a fonte upstream.

Interfaces netlink do kernel para vinculação e 802.3ad (LACP)

Interfaces netlink adicionais para a leitura e configuração de parâmetros de vinculação em dispositivos LACP foram acrescentadas ao kernel.

Melhorias de desempenho para mactap e macvtap com VLANs

Algumas questões de baixa produtividade envolvendo problemas de segmentação foram tratadas:

* A comunicação com dispositivos e1000 para dispositivos virtio em mactap.

* A comunicação com um host externo ao usar VLANs no guest.

* A comunicação com o host KVM em um VLAN tanto no guest quanto no host.

Consulta de rede ethtool aprimorada

As capacidades network-querying do utilitário ethtool foram melhoradas em uma Apresentação Prévia de Tecnologia para o Red Hat Enterprise Linux 7.1 no IBM System z e possuem suporte completo a partir do Red Hat Enterprise Linux 7.2. Como consequência, ao usar hardware compatível com a consulta aprimorada, ethtool fornece melhores opções de monitoramento e exibe valores e configurações de placa de rede mais precisos.

Capítulo 12. Segurança

Algoritmos de troca de chaves GSSAPI podem ser desabilitados seletivamente

Em razão da vulnerabilidade de segurança Logjam, os métodos de troca de chaves **`gss-group1-sha1-*`** não são mais considerados seguros. Embora houvesse a possibilidade de desabilitar este método de troca de chaves por uma troca de chave normal, não era possível desabilitá-lo por uma troca de chave GSSAPI. Com esta atualização, o administrador pode desabilitar seletivamente este ou outros algoritmos usados pela troca de chaves GSSAPI.

Adição da política SELinux para o Red Hat Gluster Storage

Antigamente, a política SELinux para os componentes do Red Hat Gluster Storage (RHGS) estava ausente e o Gluster funcionava corretamente somente quando o SELinux estava em modo permissivo. Com esta atualização, as regras da política SELinux para os processos **`glusterd`** (Serviço de Gerenciamento glusterFS), **`glusterfsd`** (Servidor NFS), **`smbd`**, **`nfsd`**, **`rpcd`**, adn **`ctdbd`** foram atualizados fornecendo suporte SELinux ao Gluster.

Rebase do openscap para a versão 1.2.5

Os pacotes *openscap* receberam upgrade para a versão upstream 1.2.5, a qual fornece vários aprimoramentos e correções de erros em relação à versão anterior.

Aprimoramentos importantes:

* Suporte para OVAL versão 5.11, a qual traz melhorias múltiplas, tais como para as propriedades systemd

* Introdução de suporte nativo dos arquivos de entrada **`xml.bz2`**

* Introdução da ferramenta **`oscap-ssh`** para a avaliação de sistemas remotos

* Introdução da ferramenta **`oscap-docker`** para a avaliação de imagens/contêineres

Rebase do scap-security-guide para a versão 0.1.25

A ferramenta *scap-security-guide* recebeu upgrade para a versão upstream 0.1.25, a qual fornece vários aprimoramentos e correções de erros em relação à versão anterior.

Aprimoramentos importantes:

* Novos perfis de segurança para o Red Hat Enterprise Linux 7 Server: Common Profile for General-Purpose Systems, Draft PCI-DSS v3 Control Baseline, Standard System Security Profile e Draft STIG for Red Hat Enterprise Linux 7 Server.

* Novos parâmetros de referência de segurança para Firefox e os componentes do Java Runtime Environment (JRE) em execução no Red Hat Enterprise Linux 6 e 7.

* Novo subpacote **`scap-security-guide-doc`**, que possui documentos formatados em HTML contendo guias de segurança geradas de parâmetros de referência XCCDF (para cada perfil de segurança enviado nos parâmetros de segurança para o Red Hat Enterprise Linux 6 e 7, Firefox e JRE).

Capítulo 13. Servidores e Serviços

A diretiva ErrorPolicy está agora validada

A diretiva de configuração ErrorPolicy não estava validada mediante inicialização e uma política de erro padrão não intencional poderia ser usada sem aviso. A diretiva está validada agora mediante inicialização e restauração como padrão, caso o valor configurado esteja incorreto. A polícia proposta é usada ou uma mensagem de aviso é registrada.

CUPS desabilita a criptografia SSLv3 por padrão

Anteriormente, não era possível desabilitar a criptografia SSLv3 no agendador CUPS, deixando-o vulnerável a ataques contra SSLv3. Para resolver este problema, a palavra-chave **`cupsd.conf SSLOptions`** foi estendida para incluir duas novas opções, **`AllowRC4`** e **`AllowSSL3`**, ambas permitindo o recurso nomeado no arquivo **`cupsd`**. As novas opções também possuem suporte no arquivo **`/etc/cups/client.conf`**. A medida padrão agora é desabilitar tanto RC4 e SSL3 para **`cupsd`**.

`cups` permite sublinhado em nomes de impressora.

O serviço **`cups`** agora permite aos usuários incluir o caractere de sublinhado (_) nos nomes de impressora locais.

Dependências desnecessárias removidas do pacote tftp-server

Anteriormente, um pacote adicional era instalado por padrão durante a instalação do pacote *tftp-server*. Com esta atualização, a dependência do pacote supérfluo foi removida e o pacote desnecessário não é mais instalado por padrão durante a instalação do *tftp-server*.

O arquivo /etc/sysconfig/conman preterido foi removido

Antes de introduzir o gerenciador **`systemd`**, vários limites para os serviços podiam ser configurados no arquivo **`/etc/sysconfig/conman`**. Após migrar para **`systemd`**, **`/etc/sysconfig/conman`** passou a não ser mais usado e, portanto, foi removido. Para estabelecer limites e outros parâmetros daemon, tais como LimitCPU=, LimitDATA= ou LimitCORE=, edite o arquivo **`conman.service`**. Para mais informações, consulte a página manual systemd.exec(5). Além disso, uma nova variável LimitNOFILE=10000 foi adicionada ao arquivo **`systemd.service`** e está convertida em comentário por padrão. Observe que após fazer quaisquer alterações à configuração **`systemd`**, o comando **`systemctl daemon-reload`** precisa ser executado para que as alterações passem a funcionar.

Rebase do mod_nss para a versão 1.0.11

mod_nss packages foi atualizado para a versão upstream 1.0.11, a qual fornece várias correções de erros e aprimoramentos em relação à versão anterior. **`mod_nss`** agora habilita, em especial, TLSv1.2 e SSLv2 foi completamente removido. Além disto, foi adicionado suporte para codificações geralmente consideradas mais seguras.

O daemon vstfpd fornece suporte aos conjuntos de codificação DHE e ECDHE

O daemon **`vsftpd`** agora fornece suporte aos conjuntos de codificação baseados no protocolo de troca de chaves Diffie–Hellman Exchange (DHE) e Elliptic Curve Diffie–Hellman Exchange (ECDHE).

Permissões podem ser definidas para arquivos carregados com sftp

Os ambientes de usuários inconsistentes e as configurações **umask** estritas podiam resultar em arquivos inacessíveis durante o carregamento ao fazer uso do utilitário **sftp**. Com esta atualização, o administrador é capaz de forçar permissões exatas para os arquivos carregados usando **sftp**, evitando, assim, o problema descrito.

Consultas LDAP usadas por ssh-ldap-helper podem ser ajustadas

Nem todos os servidores LDAP utilizam um esquema padrão como esperado pela ferramenta **ssh-ldap-helper**. Esta atualização permite que o administrador ajuste a consulta LDAP usada por **ssh-ldap-helper** para obter chaves públicas de servidores usando um esquema diferente. A funcionalidade padrão mantém-se inalterada.

Nova diretiva `createolddir` no utilitário logrotate

Uma nova diretiva **createolddir** no logrotate foi adicionada para habilitar a criação automática do diretório **olddir**. Para mais informações, consulte a página manual logrotate(8).

As mensagens de erro do `/etc/cron.daily/logrotate` não são mais redirecionadas a `/dev/null`

As mensagens de erro geradas por cronjob diários do **logrotate** agora são enviadas ao usuário **root** em vez de serem descartadas silenciosamente. Além disto, o script **/etc/cron.daily/logrotate** é marcado como um arquivo de configuração no RPM.

Algoritmos baseados em SEED e IDEA estão restritos em `mod_ssl`

Os conjuntos de codificações habilitados por padrão no módulo **mod_ssl** do Apache HTTP Server foram restringidos para melhorar a segurança. Os algoritmos de criptografia baseada em SEED e IDEA não são mais habilitados na configuração padrão do **mod_ssl**.

Apache HTTP Server passa a fornecer suporte a UPN

Os nomes armazenados na porção **subject alternative name** dos certificados de cliente SSL/TLS, como o Microsoft User Principle Name, podem ser usados agora a partir da diretiva SSLUserName e estão disponíveis nas variáveis de ambiente **mod_ssl**. Os usuários podem agora ser autenticados com seus Common Access Card (CAC) ou certificados com um UPN dentro e ter seus UPN usados como informações de usuário autenticado - consumidos por ambos, o controle de acesso no Apache e usando a variável de ambiente **REMOTE_USER** ou um mecanismo semelhante nos aplicativos. Como resultado, os usuários podem agora definir **SSLUserName SSL_CLIENT_SAN_OTHER_msUPN_0** para autenticação usando UPN.

O banco de dados de bloqueio `mod_dav` está habilitado por padrão no módulo `mod_dav_fs`

O banco de dados de bloqueio **mod_dav** passa a ser habilitado por padrão agora, se o módulo **mod_dav_fs** do Apache HTTP estiver carregado. O local padrão **ServerRoot/davlockdb** pode ser substituído usando a diretiva de configuração **DAVLockDB**.

`mod_proxy_wstunnel` passa a fornecer suporte a WebSockets

O módulo **mod_proxy_wstunnel** do Apache HTTP agora está habilitado por padrão e inclui suporte a conexões SSL no esquema **wss://**. Além disto, é possível usar o esquema **ws://** nas diretivas **mod_rewrite**. Isto permite o uso de WebSockets como um destino para **mod_rewrite** e a habilitação de WebSockets no módulo proxy.

Capítulo 14. Armazenamento

Rebase do DM para a versão 4.2

O Device Mapper (DM) foi atualizado para a versão upstream 4.2, a qual fornece várias correções de erros e aprimoramentos em relação à versão anterior, incluindo uma importante atualização do desempenho DM crypt e uma atualização do núcleo DM para oferecer suporte ao Mecanismo de Enfileiramento (em inglês, Multi-Queue Block I/O Queueing Mechanism) (blk-mq).

Agendamento de múltiplas filas E/S com blk-mq

O Red Hat Enterprise Linux 7.2 inclui um novo mecanismo de agendamento de múltiplas filas E/S para dispositivos de blocos conhecidos como blk-mq. Ele melhora o desempenho permitindo que certos drivers de dispositivo mapeiem as solicitações E/S às múltiplas filas de software ou hardware. Esta melhora do desempenho vem através da redução da contenção de bloqueio presente quando múltiplas threads de execução desempenham E/S em um único dispositivo. Os dispositivos mais novos, como o Non-Volatile Memory Express (NVMe), ficam melhor posicionados para tirar proveito deste recurso, devido ao suporte nativo deles à múltipla submissão de hardware e às filas de conclusão, assim como às suas características de desempenho de baixa latência. Os ganhos com o desempenho, como sempre, dependerão do tipo exato de hardware e da carga de trabalho.

O recurso blk-mq está atualmente implementado e habilitado por padrão nos seguintes drivers: virtio-blk, mtip32xx, nvme e rbd.

O recurso relacionado, scsi-mq, permite que os drivers de dispositivo da Interface de Sistemas para Pequenos Computadores (do inglês, Small Computer System Interface - SCSI) utilizem a infraestrutura do blk-mq. O recurso scsi-mq é fornecido como uma apresentação prévia da tecnologia no Red Hat Enterprise Linux 7.2. Para habilitar o scsi-mq, especifique **`scsi_mod.use_blk_mq=y`** na linha de comando do kernel. O valor padrão é **n** (desabilitado).

O destino do device mapper (DM) multipath, o qual usa DM baseado em solicitação, também pode ser configurado para utilizar a infraestrutura do blk-mq, se a opção do kernel **`dm_mod.use_blk_mq=y`** estiver especificada. O valor padrão é **n** (desabilitado).

Pode ser proveitoso definir **`dm_mod.use_blk_mq=y`**, caso os dispositivos SCSI subjacentes também estejam usando blk-mq, já que reduz a sobrecarga de bloqueio na camada do DM.

Para determinar se o DM multipath está usando blk-mq em algum sistema, concatene o arquivo **`/sys/block/dm-X/dm/use_blk_mq`**, onde **`dm-X`** é substituído pelo dispositivo DM multipath de interesse. Este arquivo está em modo somente leitura e reflete o valor global no **`/sys/module/dm_mod/parameters/use_blk_mq`** no momento que o dispositivo DM multipath baseado em solicitação foi criado.

Novas opções delay_watch_checks e delay_wait_checks no arquivo multipath.conf

Mesmo quando um caminho não é confiável, como quando a conexão cai com frequência, o multipathd continua tentando usar este caminho. O tempo limite que o multipathd percebe que o caminho não é mais acessível é de 3000 segundos, o que pode dar a impressão de que o multipathd está paralisado.

Para corrigir isto, duas novas opções de configuração foram adicionadas: delay_watch_checks e delay_wait_checks. Configure delay_watch_checks para o número de ciclos de caminho que o multipathd deve assistir depois que ficar online. Caso o caminho falhe sob o valor atribuído, multipathd contará com a opção delay_wait_checks para informá-lo sobre o número de ciclos consecutivos que ele deve passar até que o caminho torne-se válido novamente. Isto previne que os caminhos inválidos sejam usados imediatamente depois que ficam online de novo.

Nova opção config_dir no arquivo multipath.conf

Os usuários não podiam dividir sua configuração entre /etc/multipath.conf e outros arquivos de configuração. Isso impedia que os usuários instalassem um arquivo de configuração principal para todas as suas máquinas e mantivessem informações de configuração específicas da máquina em arquivos de configuração separados para cada máquina.

Para resolver isso, uma nova opção config_dir foi adicionada ao arquivo multipath.config. Os usuários devem alterar a opção config_dir para uma cadeia de caracteres vazia ou um nome de caminho de diretório totalmente qualificado. Quando definido para qualquer outra coisa que não seja uma cadeia de caracteres vazia, o multipath irá ler todos os arquivos .conf em ordem alfabética. Ele irá, então, aplicar as configurações exatamente como se tivessem sido adicionadas ao /etc/multipath.conf. Se esta alteração não é feita, config_dir é padronizado em /etc/multipath/conf.d.

O novo comando dmstats exibe e gerencia as estatísticas de E/S para as regiões de dispositivos que usam o driver device-mapper.

O comando **`dmstats`** fornece suporte ao espaço de usuário para as estatísticas de E/S do device-mapper. Isto permite ao usuário criar, gerenciar e informar dados de histograma em latência, métricas e contadores de E/S para as regiões arbitrárias definidas pelos usuários de dispositivos device-mapper. Os campos de estatísticas estão, agora, disponíveis nos relatórios **`dmsetup`** e o comando **`dmstats`** adiciona novos modos de relatório especializados desenvolvidos para uso com informações estatísticas. Para mais informações sobre o comando **`dmstats`**, consulte a página manual dmstats(8).

LVM Cache

O LVM cache tem sido oferecido com suporte integral desde Red Hat Enterprise Linux 7.1. Este recurso permite aos usuários criar volumes lógicos (LVs) com um dispositivo pequeno e rápido desempenhando como um cache para dispositivos maiores e mais lentos. Consulte a página manual lvmcache(7) para informações sobre a criação de volumes lógicos cache.

Observe as seguintes restrições na utilização dos LVs cache:

* O LV cache deve ser um dispositivo de alto nível. Não pode ser usado como um LV thin-pool, uma imagem de um RAID LV ou qualquer outro tipo de sub-LV.

* Os sub-LVs do LV cache (LV de origem, LV de metadados e LV de dados) só podem ser do tipo linear, striped ou RAID.

* As propriedades do LV cache não podem ser modificadas após a criação. Para mudar as propriedades do cache, remova o cache conforme descrito em lvmcache(7) e recrie-o com as propriedades desejadas.

Nova política do LVM/DM cache

Uma nova política de dm-cache **`smq`** que reduz o consumo de memória e melhora o desempenho na maioria dos casos de utilização foi escrita. Esta é, agora, a política de cache padrão para os novos volumes lógicos de LVM cache. Os usuários que preferirem usar a política de cache **`mq`** legada ainda podem utilizá-la fornecendo o argumento **`–cachepolicy`** quando estiverem criando o volume lógico cache.

ID do sistema LVM

Os grupos de volume LVM agora podem ser atribuídos a um proprietário. O proprietário dos grupos de volume é a ID do sistema de um host. Somente o host com a ID de sistema dada pode usar o VG. Isto pode beneficiar os grupos de volume que existem em dispositivos compartilhados, visíveis a múltiplos hosts, os quais não são protegidos de outro modo do uso simultâneo de múltiplos hosts. Os grupos de volume LVM

em dispositivos compartilhados com uma ID do sistema atribuída são pertencentes a um host e protegidos de outros hosts.

Novo daemon `lvmpolld`

O daemon **`lvmpolld`** fornece um método polling para comandos LVM de execução longa. Quando habilitado, o controle dos comandos LVM de execução longa é transferido do comando LVM original para o daemon **`lvmpolld`**. Isto permite que a operação continue independente do comando LVM original. O daemon **`lvmpolld`** é habilitado por padrão.

Antes da introdução do daemon **`lvmpolld`**, qualquer processo de polling em segundo plano originário de um comando lvm2 iniciado dentro de um **`cgroup`** de um serviço systemd poderia ser interrompido, se o processo principal (o serviço principal) fosse encerrado no **`cgroup`**. Isto podia gerar o término prematuro do processo de polling do lvm2. Além disto, **`lvmpolld`** ajuda a evitar a geração de consultas de processos de polling do lvm2 para progresso na mesma tarefa múltiplas vezes, já que ele monitora o progresso para todas as tarefas de polling em andamento.

Para mais informações sobre o daemon **`lvmpolld`**, consulte o arquivo de configuração **`lvm.conf`**.

Melhorias nos critérios de seleção do LVM

O lançamento do Red Hat Enterprise Linux 7.2 fornece suporte a várias melhorias nos critérios de seleção do LVM. Anteriormente, era possível usar critérios de seleção somente para os comandos de notificação; agora, o LVM fornece suporte a critérios de seleção para diversos comandos de processamento de LVM também. Além disto, há chances de fornecer um suporte melhor neste lançamento para a seleção e campos de notificação de tempo.

Para mais informações sobre a implementação desses novos recursos, consulte o apêndice **`LVM Selection Criteria`** no manual Logical Volume Administration.

Aumento no número máximo padrão do SCSI LUNs

O valor padrão para o parâmetro **`max_report_luns`** aumentou de 511 para 16393. Este parâmetro especifica o número máximo de unidades lógicas que podem ser configuradas quando os sistemas escaneiam a interconexão SCSI usando o mecanismo Report LUNs.

Capítulo 15. Gerenciamento do Sistema e Subscrições

PowerTOP agora respeita os nomes de arquivo dos relatórios definidos pelos usuários

Anteriormente, os nomes de arquivo dos relatórios PowerTOP eram gerados de forma confusa e não documentada. Com esta atualização, a implementação melhorou e os nomes de arquivo gerados agora respeitam os nomes solicitados pelo usuário, aplicando-se tanto aos relatórios CSV quanto HTML.

Os comandos `yum-config-manager` foram corrigidos

Anteriormente, a execução do comando **`yum-config-manager --disable`** desabilitava todos os repositórios configurados, enquanto o comando **`yum-config-manager --enable`** não habilitava nenhum. Esta inconsistência foi corrigida. Agora, os comandos **`--disable`** e **`--enable`** exigem o uso de '*' na sintaxe e, assim, **`yum-config-manager --enable \*`** habilita os repositórios. A execução dos comandos sem o acréscimo de '*' imprime uma mensagem pedindo ao usuário a execução de **`yum-config-manager --disable \*`** ou **`yum-config-manager --enable \*`**, caso queiram desabilitar ou habilitar os repositórios.

Novo plug-in search-disabled-repos para yum

O plug-in search-disabled-repos para yum foi adicionado aos pacotes subscription-manager. Este plug-in permite que os usuários completem com êxito as operações yum que falham pelo fato do repositório fonte ser dependente de um repositório desabilitado. Quando o search-disabled-repos é instalado no cenário descrito acima, o yum exibe instruções para habilitar temporariamente os repositórios atualmente desabilitados e pesquisar por dependências ausentes.

Caso opte por seguir as instruções e desativar o comportamento padrão notify_only no arquivo/etc/yum/pluginconf.d/search-disabled-repos.conf, as operações yum futuras solicitarão que você habilite temporariamente ou permanentemente todos os repositórios desabilitados necessários para atender à transação yum.

Adquirindo dados de hipervisores em paralelo

Com esta atualização, virt-who é capaz de adquirir dados de múltiplos hipervisores em paralelo. Anteriormente, vir-who podia ler somente os dados de um único hipervisor por vez, e se um hipervisor em uma série não funcionasse, virt-who aguardava por sua resposta e, então, gerava falhas. A leitura dos hipervisores em paralelo contorna este problema e evita a falha descrita.

Filtragem de hipervisores notificados pelo virt-who

O serviço virt-who introduz um mecanismo de filtragem para os relatórios do Gerenciador de Subscrição. Como resultado, os usuários podem agora escolher quais hosts virt-who devem ser exibidos segundo os parâmetros especificados. Por exemplo, eles podem filtrar os hosts que não executam nenhuma máquina virtual Red Hat Enterprise Linux ou os hosts que executam máquinas virtuais de uma versão especificada do Red Hat Enterprise Linux.

Visualização melhorada da associação host-to-guest

A opção **`-p`** foi adicionada ao utilitário virt-who. Quando usada com **`-p`**, a saída do virt-who exibe um mapa codificado Javascript Object Notation (JSON) da associação host-guest. Além disto, a informação na associação host-guest autenticada no arquivo /var/log/rhsm/rhsm.log está formatada agora em JSON também.

Saída virt-who exibida como nomes de host

É possível configurar agora a consulta virt-who para que seus resultados sejam exibidos como nomes de host em vez de Identificadores Exclusivos Universais (UUIDs), quando visualizados no Red Hat Satellite e Portal do Cliente Red Hat. Para habilitar a função, adicione a opção **`hypervisor_id=hostname`** ao arquivo de configuração no diretório /etc/virt-who.d/. Idealmente, isto deve ser feito ao usar o virt-who pela primeira vez, caso contrário a configuração duplica o hipervisor.

Arquivo de configuração do virt-who pré-preenchido

Um arquivo de configuração para o virt-who foi colocado no diretório /etc/virt-who.d/. Ele contém um modelo e instruções para a configuração do virt-who. Isto substitui a configuração preterida que utiliza o arquivo /etc/sysconfig/virt-who.

Opções de conexão proxy aprimoradas

Com o Red Hat Enterprise Linux 7.2, o utilitário virt-who pode manipular as variáveis de ambiente HTTP_PROXY e HTTPS_PROXY e, assim, usar corretamente o servidor proxy, quando necessário. Isto permite que o virt-who conecte-se ao hipervisor Hyper-V e Red Hat Enterprise Virtualization Manager através do proxy.

O Gerenciador de Subscrição passa a fornecer suporte a syslog

A ferramenta *subscription-manager* pode usar agora o syslog como o formatador e manipulador de log, além de separar o log usado anteriormente. O formatador e o manipulador estão configurados no arquivo de configuração **`/etc/rhsm/logging.conf`**.

O Gerenciador de Subscrição passa a fazer parte do Initial Setup

O componente do Gerenciador de Subscrição do Firstboot (primeira inicialização) foi transportado para o utilitário Initial Setup (configuração inicial). Os usuários são capazes agora de registrar o sistema a partir do menu principal do Initial Setup, após instalação de um sistema Red Hat Enterprise Linux 7 e de sua primeira reinicialização.

O Gerenciador de Subscrição exibe o URL do servidor durante o registro em uma linha de comando.

Ao registrar um sistema usando o comando **`subscription-manager`** em uma linha de comando, a ferramenta também exibe agora o URL do servidor sendo usado para o registro ao perguntar pelo nome de usuário e senha. Isto ajuda o usuário a determinar quais credenciais usar.

A caixa de diálogo Gerenciar Repositórios no Gerenciador de Subscrição está mais ágil

A caixa de diálogo Gerenciar Repositórios na versão gráfica do Gerenciador de Subscrição (o pacote *subscription-manager-gui*) foi atualizada para não buscar informações em cada alteração na caixa de verificação. No lugar disto, o estado do sistema é sincronizado somente quando o botão novo **`save`** (salvar) é clicado. Isto remove os atrasos que os usuários experenciavam nas versões anteriores gerados pelo estado do sistema ser atualizado diante de toda ação da caixa de verificação. O gerenciamento de repositórios está bem mais ágil agora.

Capítulo 16. Virtualização

qemu-kvm oferece suporte a eventos de rastreamento de desligamento de máquinas virtuais

Os eventos de rastreamento qemu-kvm durante o processo de desligamento do sistema da máquina virtual agora estão disponíveis, o que permite aos usuários obter diagnósticos detalhados sobre as solicitações de desligamento de um sistema convidado emitidas pelo comando **`virsh shutdown`** ou pelo aplicativo virt-manager. Isso fornece aos usuários com recursos avançados o isolamento e a depuração de problemas de convidados KVM durante o desligamento.

Intel MPX exposto ao convidado

Com essa atualização, qemu-kvm permite o recurso de Extensões de Proteção de Memória Intel (em inglês, Intel Memory Protection Extensions - MPX) ser exposto ao convidado. Nos sistemas host Intel 64 que oferecem suporte ao recurso MPX, isto permite o uso de um conjunto de extensões que fornece suporte a hardware para proteção de vinculações em referências do ponteiro.

Extração de despejo da memória do convidado do núcleo qemu-kvm

O script dump-guest-memory.py foi introduzido ao QEMU, o que possibilita a análise do despejo da memória do convidado do núcleo qemu-kvm em caso de falha do kernel convidado. Para mais informações, consulte o texto de ajuda relacionado com o uso do comando **`help dump-guest-memory`**.

virt-v2v possui suporte completo

Com o Red Hat Enterprise Linux 7.2, a ferramenta de linha de comando virt-v2v passou a receber suporte completo. Esta ferramenta converte máquinas virtuais executando hipervisores estrangeiros para executar em KVM. Atualmente, virt-v2v pode converter convidados do Red Hat Enterprise Linux e Windows executando em Red Hat Enterprise Linux 5 Xen e VMware vCenter.

Virtualização em IBM Power Systems

O Red Hat Enterprise Linux com KVM possui suporte nos sistemas AMD64 e Intel 64, mas não em IBM Power Systems. Atualmente, a Red Hat fornece uma solução baseada em POWER8 com Red Hat Enterprise Virtualization para IBM Power Systems.

Mais informações sobre o suporte das versões e os procedimentos de instalação podem ser encontradas no seguinte artigo da base de dados de conhecimento: https://access.redhat.com/articles/1247773.

Suporte a TRIM no Hyper-V

Agora, é possível usar o disco rígido virtual Thin Provisioned Hyper-V (VHDX). A atualização acrescenta suporte para reduzir os arquivos VHDX básicos a tamanhos realmente utilizados pelas máquinas virtuais Microsoft Hyper-V.

Suporte KVM para tcmalloc

O KVM agora pode usar a biblioteca tcmalloc, a qual fornece uma melhora de desempenho significante nas operações de E/S por segundo.

Cópia de disco seletiva durante migração ao vivo de domínio

Ao migrar um domínio e seus discos ao vivo, o usuário pode agora selecionar quais discos serão copiados durante a migração. Isto permite uma migração ao vivo mais eficiente quando a cópia de alguns discos não é desejável, como quando eles já existem no destino ou quando eles não são mais úteis.

Os dispositivos que usam RMRRs estão excluídos dos domínios API IOMMU

De acordo com as alterações feitas no Red Hat Enterprise Linux 7.1, quando há uma tentativa de atribuir um dispositivo emaranhado por uma associação de Reserved Memory Region Reporting (RMRR), o kernel comunica o seguinte erro no log dmesg:

"Dispositivo não qualificado para anexação do domínio IOMMU devido às exigências RMRR da plataforma. Entre em contato com seu fornecedor de plataforma."

O fornecedor da plataforma tem a capacidade de solicitar ao subsistema VT-d IOMMU dentro do kernel a retenção de mapeamentos específicos para os dispositivos usando entradas na Configuração Avançada e na tabela Power Interface Direct Memory Access Remapping (ACPI DMAR), conhecida como estruturas RMRR. No entanto, QEMU-KVM e VFIO não têm visibilidade alguma para essas exigências de mapeamento e não há nenhuma API para desabilitar potenciais comunicações contínuas que possam ocorrer através destas regiões. Portanto, um dispositivo associado a uma estrutura RMRR poderia continuar a usar DMA através deste espaço de endereço mesmo depois do dispositivo ser atribuído a uma MV guest. Isto poderia fazer com que um dispositivo substituísse a memória da MV com dados DMA destinados para a memória descrita pela RMRR.

Para corrigir este erro, os dispositivos associados a RMRRs estão excluídos da participação na API IOMMU interna do kernel. Os usuários podem agora identificar tais dispositivos usando logs dmesg e também estão protegidos da atribuição de dispositivos fazendo uso de mapeamentos que têm a capacidade de gerar instabilidade nas máquinas virtuais convidadas.Os usuários impedidos de fazer uso da atribuição do dispositivo PCI, como resultado desta alteração, devem contactar os fornecedores de sua plataforma para uma atualização de BIOS para liberar o dispositivo de E/S da exigência RMRR imposta.

Para mais informações sobre essas alterações, consulte o seguinte artigo da base de dados de conhecimento:

https://access.redhat.com/articles/1434873

Capítulo 17. Atomic Host e Contêineres

Red Hat Enterprise Linux Atomic Host

O Red Hat Enterprise Linux Atomic Host é um sistema operacional seguro, leve e de mínimo impacto otimizado para executar os contêineres Linux.

Ele é pré-instalado com as seguintes ferramentas para o suporte dos contêineres Linux:

- Docker - um mecanismo open source que automatiza a implantação de qualquer aplicativo como um contêiner auto-suficiente, portátil e leve que é executado praticamente em qualquer ambiente
- atomic - define o ponto de entrada para os hosts Atomic
- kubernetes - fornece gerenciamento de cluster de contêineres
- etcd - fornece um armazenamento de valor de chave altamente disponível para configuração compartilhada
- flannel - contém um agente de gerenciamento de endereços baseado em etcd, que gerencia endereços IP de redes de sobreposição entre os sistemas executando contêineres que precisam de comunicar uns com os outros

O Red Hat Enterprise Linux Atomic Host usa as seguintes tecnologias:

- OSTree e rpm-OSTree - Estes projetos fornecem upgrades do atomic e capacidade de reversão
- systemd - um novo sistema init para o Linux que acelera o tempo de inicialização e facilita a orquestração
- SELinux - habilitado por padrão para fornecer uma segurança multilocatária completa

Além disto, o **`Cockpit`** também está disponível no Red Hat Enterprise Linux, como um pacote separado de Extras, e no Red Hat Enterprise Linux Atomic Host, como uma Imagem de Contêiner, **`cockpit-ws`**. O Cockpit é uma interface de administração do servidor que facilita a administração de servidores do Red Hat Enterprise Linux através de um navegador da web.

Red Hat Enterprise Linux Atomic Host 7.2.4

Pacotes atualizados:

- docker-1.9.1-40.el7
- kubernetes-1.2.0-0.11.git738b760.el7
- cockpit-0.103-1.el7
- cockpit-ostree-0.103-1.el7
- docker-distribution-2.4.0-2.el7 *
- runc-0.1.0-3.el7 *

Novos pacotes:

- atomic-devmode-0.3.3-3.el7
- docker-latest-1.10.3-22.el7

O asterisco (*****) refere-se aos pacotes que estão disponíveis somente para o Red Hat Enterprise Linux.

Imagens de contêiner atualizadas

Todas as imagens de contêiner oficiais da Red Hat estão disponíveis na página registry.access.redhat.com.

Red Hat Enterprise Linux 7.2.4 Container Image (rhel7/rhel)

Red Hat Enterprise Linux Atomic Tools Container Image (rhel7/rhel-tools)

Red Hat Enterprise Linux Atomic rsyslog Container Image (rhel7/rsyslog)

Red Hat Enterprise Linux Atomic sadc Container Image (rhel7/sadc)

Red Hat Enterprise Linux Atomic cockpit-ws Container Image (rhel7/cockpit-ws)

Red Hat Enterprise Linux Atomic etcd Container Image (rhel7/etcd)

Red Hat Enterprise Linux Atomic Kubernetes-controller Container Image (rhel7/kubernetes-controller-mgr)

Red Hat Enterprise Linux Atomic Kubernetes-apiserver Container Image (rhel7/kubernetes-apiserver)

Red Hat Enterprise Linux Atomic Kubernetes-scheduler Container Image (rhel7/kubernetes-scheduler)

Red Hat Enterprise Linux Atomic SSSD Container Image (rhel7/sssd) (Apresentação Prévia de Tecnologia)

Atualização OSTree

Nova Versão da Árvore: 7.2.4 (hash: b060975ce3d5abbf564ca720f64a909d1a4d332aae39cb4de581611526695a0c)

Alterações desde a Versão da Árvore 7.2.3-1 (hash: 644fcc603549e996f051b817ba75a746f23f392cfcc7e05ce00342dec6084ea8)

Para obter o OSTree mais recente, execute o comando **`atomic host upgrade`** no seu sistema Red Hat Enterprise Linux Atomic Host.

Começando com o lançamento Atomic Host 7.2.4, duas versões do serviço docker serão incluídas no sistema operacional: Docker 1.9 e Docker 1.10.

O artigo da base de dados de conhecimento a seguir contém todas as informações necessárias sobre como usar essas duas versões do Docker: https://access.redhat.com/articles/2317361

O conflito entre o docker 1.9 e as versões atomic-openshift 3.1 / versões de origem 1.1 foi removido

Anteriormente, devido a questões de estabilidade entre o docker 1.9 e as versões atomic-openshift 3.1/ versões de origem 1.1, o docker 1.9 era empacotado para entrar em conflito com as versões do atomic-openshift mais antigas que 3.2 e as versões de origem mais antigas que 1.2. Como consequência disso, a execução de **`yum update`** em um sistema OpenShift Enterprise 3.1 gerava falhas. Este erro foi corrigido e a execução de **`yum update`** agora não gera conflitos e, sim, resolve as dependências com êxito e instala o docker 1.9.

Novo pacote atomic-devmode disponível

O pacote atomic-devmode permite que os usuários experenciem facilmente a Red Hat Atomic Cloud Image. Ela adiciona um novo item de menu GRUB2, rotulado como **`Developer Mode`**, que possibilita aos usuários inicializar o sistema sem ter que configurar **`cloud-init`**. Quando no Modo de Desenvolvedor (Developer Mode), a senha root será gerada automaticamente e os usuários também entrarão automaticamente em uma

sessão interativa na qual o Cockpit é baixado e iniciado.

Pacotes kubernetes atualizados

Os pacotes kubernetes foram atualizados para ose v3.2.0.16, correspondendo ao kubernetes v1.2.0. Além disto, foi introduzido suporte para a exposição de chaves secretas nas variáveis de ambiente.

O Cockpit foi rebaseado para a versão 0.103

As alterações mais notáveis do *cockpit-0.103*:

- Quando o Cockpit não consegue se conectar a um host, o comando SSH relevante ou os detalhes do host agora são exibidos para auxiliar na resolução do problema.
- A política de reinicialização do Docker agora pode ser configurada durante a inicialização de um novo contêiner.
- A criação de volumes lógicos passou a ser reunida em uma única caixa de diálogo.
- A ingressao nos domínios IPA não oferece mais a opção **`Computer OU`**.
- Os dados binários do jornal agora são exibidos corretamente.
- Os tamanhos do sistema de arquivos ou disco são exibidos usando nomes IEC, tais como **`MiB`**.
- Os volumes lógicos não podem ser reduzidos mais e a caixa de diálogo da partição do sistema de arquivos impede os tamanhos negativos.
- Políticas de segurança de conteúdo estritas foram implementadas na maioria dos Cockpits para impedir ataques baseados no navegador.

Os pacotes também incluem várias correções de erros e melhorias na interface do administrador.

Red Hat Enterprise Linux Atomic Host 7.2.3

Pacotes atualizados:

- docker-1.9.1-25.el7
- etcd-2.2.5-1.el7
- python-docker-py-1.7.2-1.el7
- kubernetes-1.2.0-0.9.alpha1.gitb57e8bd.el7
- cockpit-0.96-2.el7
- atomic-1.9-4.gitff44c6a.el7
- docker-distribution-2.3.1-1.el7 *
- dpdk-2.2.0-2.el7 *

Novos pacotes:

- runc-0.0.8-1.git4155b68.el7 *
- atomic-pkglayer-2016.1.1.gfbf8dde-2.el7 *

O asterisco (*****) refere-se aos pacotes que estão disponíveis somente para o Red Hat Enterprise Linux.

`Imagens de Contêiner`

Todas as imagens de contêiner oficiais da Red Hat estão disponíveis na página registry.access.redhat.com.

Novo:

Red Hat Enterprise Linux Atomic SSSD Container Image (rhel7/sssd) (Apresentação Prévia de Tecnologia)

Atualizado:

Red Hat Enterprise Linux 7.2.3 Container Image (rhel7/rhel)

Red Hat Enterprise Linux Atomic Tools Container Image (rhel7/rhel-tools)

Red Hat Enterprise Linux Atomic rsyslog Container Image (rhel7/rsyslog)

Red Hat Enterprise Linux Atomic sadc Container Image (rhel7/sadc)

Red Hat Enterprise Linux Atomic cockpit-ws Container Image (rhel7/cockpit-ws)

Red Hat Enterprise Linux Atomic etcd Container Image (rhel7/etcd)

Red Hat Enterprise Linux Atomic Kubernetes-controller Container Image (rhel7/kubernetes-controller-mgr)

Red Hat Enterprise Linux Atomic Kubernetes-apiserver Container Image (rhel7/kubernetes-apiserver)

Red Hat Enterprise Linux Atomic Kubernetes-scheduler Container Image (rhel7/kubernetes-scheduler)

`Atualização OSTree`

Nova Versão da Árvore: 7.2.3 (hash: d620e841861c746b5a296337c1659e6625abfeff96844099d48540fc93717656)

Alterações desde a Versão da Árvore 7.2.2-2 (hash: 8b2cf24b420d659179dc866eab1bb341748839204ba56ed46a86218010789e91)

Para obter o OSTree mais recente, execute o comando **`atomic host upgrade`** no seu sistema Red Hat Enterprise Linux Atomic Host.

Pacotes do Cockpit rebaseados para a versão 0.96

Pacotes do Cockpit que fazem parte do Red Hat Enterprise Linux Atomic Host 7.2.3, incluem **`cockpit-bridge`**, **`cockpit-shell`**, **`cockpit-docker`** e **`cockpit-ostree`**. Outros programas relacionados ao Cockpit podem ser adicionados a um Red Hat Enterprise Linux Atomic Host via contêineres (como o rhel7/contêiner cockpit-ws).

O Cockpit 0.96 é compatível com o docker 1.10. Esta versão corrige erros anteriores com vazamentos de memória, na maioria das vezes relacionados a DBus, e vários problemas de conexão e navegação. Além disto, você pode agora limitar as autenticações simultâneas semelhantes ao ssshd usando a configuração **`MaxStartups`**.

Novo pacote runc agora disponível para o Red Hat Enterprise Linux

`runC` é uma implementação portátil, leve do Open Container Format (OCF) que fornece um tempo de execução do contêiner. A ferramenta de linha de comando runC pode ser usada para gerar e executar contêineres segundo a especificação do Open Container Project (OCP). Os contêineres são inicializados como um processo dependente do runC e podem ser incorporados em vários outros sistemas sem ter que

executar um daemon docker.

Novos subcomandos adicionados à CLI do atomic

A ferramenta de linha de comando do atomic para o gerenciamento dos contêineres e sistemas do Atomic agora inclui os sub-comandos **`top`**, **`diff`** e **`migrate`**. Para mais informações sobre seus usos e sintaxe, consulte https://access.redhat.com/documentation/en/red-hat-enterprise-linux-atomic-host/version-7/cli-reference/#cli_commands.

Suporte para a personalização do sistema host

Os novos pacotes atomic-pkglayer contêm uma ferramenta para a instalação dos pacotes de depuração nos sistemas Atomic. Elas devem ser usadas somente na imagem de contêiner do Red Hat Enterprise Linux Atomic Tools (rhel7/rhel-tools). Ela fornece um mecanismo para adicionar os pacotes RPM a um Atomic Host permitindo que você inclua-os nas camadas ostree locais no sistema existente. Consulte "Installing RPMs on an Atomic Host with atomic-pkglayer" (https://access.redhat.com/articles/2245351) para uma descrição da ferramenta atomic-pkglayer.

Red Hat Enterprise Linux Atomic Host 7.2.2

Pacotes atualizados:

- docker-1.8.2-10.el7
- etcd-2.2.2-5.el7
- flannel-0.5.3-9.el7
- docker-distribution-2.2.1-1.el7
- python-docker-py-1.6.0-1.el7
- kubernetes-1.2.0-0.6.alpha1.git8632732.el7
- cockpit-0.93-1.el7
- atomic-1.8-6.git1bc3814.el7

Imagens de contêineres atualizadas:

Red Hat Enterprise Linux 7.2.2 Container Image

Red Hat Enterprise Linux Atomic Tools Container Image

Red Hat Enterprise Linux Atomic rsyslog Container Image

Red Hat Enterprise Linux Atomic sadc Container Image

Red Hat Enterprise Linux Atomic cockpit-ws Container Image

Red Hat Enterprise Linux Atomic etcd Container Image

Red Hat Enterprise Linux Atomic Kubernetes-controller Container Image

Red Hat Enterprise Linux Atomic Kubernetes-apiserver Container Image

Red Hat Enterprise Linux Atomic Kubernetes-scheduler Container Image

Atualização do OSTree:

Nova Versão da Árvore: 7.2.2 (hash: a9036292783ddfd389459d9bab69df5a655a0d6bb4dc6239a0aeff0f5d356f2e)

A API v1beta3 não possui mais suporte nos kubernetes

O uso de v1beta3 nos arquivos de configuração não possui mais suporte. A criação de um objeto v1beta3 com o comando **`kubectl`** causará falhas com o seguinte erro:

```
error validating data: the server could not find the requested resource; if you choose to ignore these errors, turn validation off with --validate=false
```

O uso da opção **`--validate=false`** criará um objeto, no entanto ele aparecerá como um objeto v1.

Um subpacote cockpit-docker separado passa a ser enviado agora

Anteriormente, o suporte do docker Cockpit era enviado junto com o subpacote *cockpit-shell*. Agora, o subpacote *cockpit-docker* está disponível para ser instalado separadamente no Red Hat Enterprise Linux e está incluído no *ostree* disponível para o Red Hat Enterprise Linux Atomic Host.

As alterações mais notáveis no cockpit 0.93

- Distribuição de lincenças dos componentes incluídos no RPM de origem
- Reformulação dos certificados TLS para o Cockpit
- O Cockpit agora oferece a ativação de multipathd para discos multipath
- Interface do usário adicionada para upgrades OSTree e reversões
- Suporte ao login OAuth adicionado
- Relatório SOS adicionado à interface do usuário
- Suporte para a ferramenta de gerenciamento de energia Tuned

Red Hat Enterprise Linux Atomic Host 7.2

Pacotes atualizados:

- docker-1.8.2-8.el7
- flannel-0.5.3-8.el7
- cockpit-0.77-3.1.el7
- storaged-2.2.0-3.el7
- kubernetes-1.0.3-0.2.gitb9a88a7.el7
- atomic-1.6-6.gitca1e384.el7
- python-websocket-client-0.32.0-116.el7
- python-docker-py-1.4.0-118.el7

Novos pacotes:

- docker-distribution-2.1.1-3.el7

Imagens de contêineres atualizadas:

Red Hat Enterprise Linux 7.2 Container Image

Red Hat Enterprise Linux Atomic rsyslog Container Image

Red Hat Enterprise Linux Atomic sadc Container Image

Red Hat Enterprise Linux Atomic Tools Container Image

Red Hat Enterprise Linux Atomic cockpit-ws Container Image

Novas imagens de contêineres:

Red Hat Enterprise Linux Atomic etcd Container Image

Red Hat Enterprise Linux Atomic Kubernetes-controller Container Image

Red Hat Enterprise Linux Atomic Kubernetes-apiserver Container Image

Red Hat Enterprise Linux Atomic Kubernetes-scheduler Container Image

Atualização do OSTree: para a lista completa dos pacotes atualizados, consulte https://access.redhat.com/articles/2050783.

"docker-1.8.2-8.el7"

Os pacotes *docker* receberam upgrade para a versão upstream 1.8.2.

Além disto, *docker* também inclui as seguintes alterações:

- O `docker` agora exibe uma mensagem de aviso caso você esteja usando o dispositivo de loopback como uma opção de armazenamento backend.
- O comando **`docker info`** agora exibe a versão rpm

do servidor e cliente.

- A propagação de montagem padrão é **`Slave`** em vez de **`Private`**. Isto permite que as montagens de volume (associação) sejam alteradas no host e que as novas montagens apareçam dentro do contêiner.
- As opções **`--add-registry`** e **`--block-registry`** foram adicionadas. Isto permite que os registros adicionais sejam especificados além do **`docker.io`**.
- É possível agora inspecionar o conteúdo dos repositórios remotos e verificar as versões mais recentes. Esta funcionalidade está implementada no comando **`atomic verify`**.

"flannel-0.5.3-8.el7"

- O prefixo de rede do flannel foi alterado de **`coreos.com/network`** para **`atomic.io/network`**.
- O comportamento do flannel foi corrigido quando o primeiro pacote de ping foi perdido.
- **`flanneld.service`** agora é inicializado quando a rede está pronta.

"kubernetes-1.0.3-0.2.gitb9a88a7.el7"

- "kubectl version" agora exibe a versão correta.
- Ao executar **`kube-apiserver`** na porta 443 no modo de segurança, alguns recursos ficam ausentes. Como uma solução alternativa, o binário **`kube-apiserver`** deve ser modificado executando:

```
# chown root:root /usr/bin/kube-apiserver

# chmod 700 /usr/bin/kube-apiserver

# setcap CAP_NET_BIND_SERVICE=ep /usr/bin/kube-apiserver
```

"cockpit-0.77-3.1.el7"

- O Cockpit agora exibe o número limite de hosts com suporte ao adicionar servidores no painel.
- URLs marcáveis mais limpas/legíveis/claras
- Inclui funcionalidade básica da autenticação da chave SSH.
- As interações básicas com armazenamento multipath foram corrigidas.
- Quando a autorização de senha não é possível, o Cockpit exibe uma mensagem informativa.
- A autenticação agora funciona ao incorporar o Cockpit.

Ativação do soquete systemd removida

Por motivos de segurança, a ativação do soquete systemd, que possuía suporte nas versões mais antigas do Docker, foi removida. Agora, o uso do grupo docker como um mecanismo para conversar com o daemon docker, como um usuário não privilegiado, não é recomendável. Configure sudo no seu lugar para este tipo de acesso. Se o daemon docker não estiver em execução após o upgrade, crie o arquivo **`/etc/sysconfig/docker.rpmnew`**, adicione uma personalização local qualquer a ele e substitua **`/etc/sysconfig/docker`** por esta personalização. Além disto, remova a linha **`-H fd://`** de **`/etc/sysconfig/docker`**, caso esteja presente.

Capítulo 18. Red Hat Software Collections

O Red Hat Software Collections é um apanhado de conteúdos da Red Hat que fornece um conjunto de linguagens de programação dinâmicas, servidores de banco de dados e pacotes relacionados que você pode instalar e utilizar em todos os lançamentos com suporte do Red Hat Enterprise Linux 6 e Red Hat Enterprise Linux 7 nas arquiteturas AMD64 e Intel 64.

As linguagens dinâmicas, os servidores de banco de dados e as outras ferramentas distribuídas com o Red Hat Software Collections não substituem as ferramentas padrão do sistema fornecidas com o Red Hat Enterprise Linux, nem é dada preferência a estas ferramentas. O Red Hat Software Collections usa um mecanismo de empacotamento alternativo com base no utilitário **`scl`** para fornecer um conjunto paralelo de pacotes. Este conjunto permite o uso opcional de versões de pacotes alternativos no Red Hat Enterprise Linux. Ao usar o utilitário **`scl`**, os usuários podem escolher quais versões do pacote desejam executar, a qualquer momento.

O Red Hat Developer Toolset agora faz parte do Red Hat Software Collections e está incluído como um Software Collection separado. O Red Hat Developer Toolset foi criado para os desenvolvedores que trabalham na plataforma Red Hat Enterprise Linux. Ele fornece as versões atuais de GNU Compiler Collection, GNU Debugger, plataforma de desenvolvimento Eclipse, entre outras ferramentas de monitoramento de desempenho, desenvolvimento e depuração.

Importante

O Red Hat Software Collections tem um ciclo de vida e um período de suporte mais curto que o Red Hat Enterprise Linux. Para mais informações, consulte Red Hat Software Collections Product Life Cycle.

Consulte a documentação do Red Hat Software Collections para obter os componentes, requisitos do sistema, problemas conhecidos, usos e especificidades dos Software Collections individuais incluídos neste conjunto.

Consulte a documentação do Red Hat Developer Toolset para mais informações sobre os componentes incluídos neste Software Collection e sobre a instalação, o uso, os problemas conhecidos, entre outros.

Parte II. Apresentação Prévia de Tecnologia

Esta seção fornece uma visão geral da Apresentação Prévia de Tecnologia introduzida ou atualizada no Red Hat Enterprise Linux 7.2.

Para mais informações sobre o escopo do suporte aos recursos da Apresentação Prévia de Tecnologia da Red Hat, consulte https://access.redhat.com/support/offerings/techpreview/.

Capítulo 19. Autenticação e Interoperabilidade

Utilização dos provedores sudo AD e LDAP

O provedor Active Directory (AD) é um back-end usado para conectar-se a um servidor AD. No Red Hat Enterprise Linux 7.2, o uso do provedor sudo AD junto com o provedor LDAP possui suporte como uma Apresentação Prévia de Tecnologia. Para habilitar o provedor sudo AD, adicione a configuração **`sudo_provider=ad`** na seção [domínio] (em inglês domain) do arquivo **`sssd.conf`** .

DNSSEC disponível como uma Apresentação Prévia de Tecnologia no Gerenciamento de Identidade

Os servidores do Gerenciamento de Identidades com DNS integrados agoram oferecem suporte às Extensões de Segurança DNS (DNSSEC), um conjunto de extensões para o protocolo DNS que aumenta a segurança. As zonas DNS hospedadas nos servidores do Gerenciamento de Identidades podem ser automaticamente assinadas usando DNSSEC. As chaves criptográficas são geradas e rodadas automaticamente.

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

Práticas Operacionais de DNSSEC, Versão 2: http://tools.ietf.org/html/rfc6781#section-2

Guia de Implantação do Sistema de Nomes de Domínio (DNS) Seguro: http://dx.doi.org/10.6028/NIST.SP.800-81-2

Considerações sobre o Tempo de Substituição de Chave DNSSEC: http://tools.ietf.org/html/rfc7583

Observe que os servidores do Gerenciamento de Identidade com DNS integrado utilizam DNSSEC para validar as respostas DNS obtidas de outros servidores DNS. Isto pode afetar a disponibilidade das zonas DNS que não estão configuradas conforme as práticas de nomeação recomendadas e descritas no Red Hat Enterprise Linux Networking Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices.

Estrutura de eventos Nunc Stans disponível para o Servidor de Diretório

Uma nova estrutura de eventos Nunc Stans foi adicionada como Apresentação Prévia de Tecnologia para tratar de múltiplas conexões simultâneas. A estrutura possibilita o suporte de milhares de conexões ativas sem degradação do desempenho. Ela vem desabilitada por padrão.

Navegador para a API JSON-RPC disponível no IdM

Esta atualização implementa um navegador para a API JSON-RPC no Gerenciamento de Identidade. O navegador pode ser usado para visualizar a API. Observe que este recurso é experimental e a API ainda não possui suporte.

Novos pacotes: ipsilon

Os pacotes *ipsilon* fornecem o serviço de provedores de identidade Ipsilon para logon único (SSO) federado. Ipsilon conecta os provedores de autenticação e aplicativos ou utilitários permitindo SSO, incluindo um servidor e utilitários para configurar provedores de serviço baseados em Apache.

O kit de ferramentas e o servidor Ipsilon foi designado para configurar os Provedores de Serviços de identidade baseados no Apache. O servidor é um aplicativo **`mod_wsgi`** autocontido conectável que fornece

SSO federado aos aplicativos web.

O Ipsilon está sendo introduzido neste lançamento como uma Apresentação Prévia de Tecnologia. Não recomendamos a integração deste serviço em ambientes de produção neste momento.

Capítulo 20. Clusterização

Suporte para `clufter`, ferramenta usada para transformar e analisar os formatos de configuração dos clusters

O pacote *clufter*, disponível como uma Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7, fornece uma ferramenta que transforma e analisa os formatos de configuração dos clusters. Ele pode ser utilizado para auxiliar nas migrações de uma configuração de pilha mais antiga para uma configuração mais nova que otimiza o Pacemaker. Para mais informações sobre os recursos do **`clufter`**, consulte a página manual **`clufter(1)`** ou a saída do comando **`clufter -h`**.

Capítulo 21. Sistemas de Arquivos

OverlayFS

OverlayFS é um tipo de sistema de arquivo de união. Ele permite ao usuário sobrepor um sistema de arquivo sobre o outro. As alterações são registradas no sistema de arquivo mais recente, enquanto o sistema de arquivo mais antigo continua sem alteração. Isto permite que múltiplos usuários compartilhem uma imagem de sistema de arquivos, tais como um contêiner ou um DVD-ROM, onde a imagem base está disponível em mídia somente leitura. Consulte a documentação do arquivo do kernel Documentation/filesystems/overlayfs.txt para mais informações.

OverlayFS continua sendo uma Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7.2 na maior parte dos casos. Dessa forma, o kernel registra os avisos quando essa tecnologia é ativada.

OverlayFS possui suporte disponível quando usado com Docker sob as seguintes restrições:

* OverlayFS possui suporte somente para uso como um driver de gráfico Docker. A sua utilização oferece suporte somente para os conteúdos COW do contêiner e não para o armazenamento persistente. Qualquer armazenamento persistente deve ser colocado em volumes não OverlayFS para obterem suporte. Apenas a configuração Docker padrão pode ser usada; o que significa que um nível de sobreposição, um lowerdir e os níveis mais antigos e mais recentes estão no mesmo sistema de arquivos.

* Somente XFS possui suporte atualmente para uso como um sistema de arquivo mais antigo.

* SELinux deve estar habilitado e em modo de imposição na máquina física, mas deve estar desabilitado no contêiner ao desempenhar a separação do contêiner; o que significa que /etc/sysconfig/docker não deve conter --selinux-enabled. O suporte a SELinux para OverlayFS está sendo trabalhado em upstream e está previsto para uma versão de lançamento futura.

* O ABI do kernel do OverlayFS e o comportamento do espaço do usuário não são considerados estáveis e podem passar por modificações em atualizações futuras.

* Para fazer com que os utilitários yum e rpm funcionem adequadamente dentro do contêiner, o usuário deve usar os pacotes yum-plugin-ovl.

Observe que OverlayFS fornece um conjunto restrito dos padrões POSIX. Teste o seu aplicativo por completo antes de implantá-lo com OverlayFS.

Alguns problemas conhecidos também foram associados ao OverlayFS depois do lançamento do Red Hat Enterprise Linux 7.2. Para mais detalhes, consulte 'Non-standard behavior' no arquivo Documentation/filesystems/overlayfs.txt.

Suporte a clientes NFSv4 com layout de arquivo flexível

Red Hat Enterprise Linux 7.2 adiciona suporte para o layout de arquivo flexível em clientes NFSv4. Esta tecnologia habilita recursos avançados, tais como a mobilidade de arquivos sem interrupção e o espelhamento ao lado de clientes, fornecendo uma usabilidade aprimorada em áreas como bancos de dados, big data e virtualização.

Consulte https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/ para mais informações sobre layout de arquivo flexível NFS.

Sistema de arquivo Btrfs

O sistema de arquivo Btrfs (B-Tree) possui suporte agora como uma Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7.2. Este sistema de arquivo oferece gerenciamento avançado, confiabilidade e recursos de escalabilidade. Ele possibilita que usuários criem snapshots e permite a compactação e o

gerenciamento integrado de dispositivos.

Suporte a Layout em Bloco pNFS

Como uma Apresentação Prévia de Tecnologia, o código upstream foi transferido para o Red Hat Enterprise Linux client para fornecer suporte a layout em bloco pNFS.

Capítulo 22. Habilitação do Hardware

Instrumentação do Tempo de Execução para IBM System z

O suporte para o recurso de Instrumentação do Tempo de Execução está disponível como uma Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7.2 em IBM System z. A Instrumentação do Tempo de Execução habilita a execução e a análise avançada de vários aplicativos de espaço de usuário disponíveis com o sistema IBM zEnterprise EC12.

Adaptadores LSI Syncro CS HA-DAS

O Red Hat Enterprise Linux 7.1 inclui um código no driver megaraid_sas para habilitar os adaptadores LSI Syncro CS de armazenamento anexado direto de alta disponibilidade (HA-DAS). Embora o driver megaraid_sas possua suporte completo para os adaptadores habilitados anteriormente, o uso deste driver para Syncro CS está disponível como uma Apresentação Prévia de Tecnologia. O suporte para este adaptador é fornecido diretamente pelo LSI, seu integrador de sistemas, ou pelo fornecedor do sistema. Recomendamos que os usuários implantando Syncro CS no Red Hat Enterprise Linux 7.2 encaminhem seus comentários para a Red Hat e LSI. Para mais informações sobre as soluções LSI Syncro CS, por favor visite http://www.lsi.com/products/shared-das/pages/default.aspx.

Capítulo 23. Kernel

Suporte de múltiplas CPU em kdump nos sistemas AMD64 e Intel 64

Nos sistemas AMD64 e Intel 64, o mecanismo de despejo de travamento do kernel **kdump** agora pode ser inicializado com mais de uma CPU ativada. Isto soluciona um problema nos sistemas que, devido à alta entrada e saída durante a criação de um despejo de travameno do kernel, o Linux poderia falhar ao alocar interrupções para os dispositivos, quando apenas uma CPU era ativada usando como opções do kernel **maxcpus=1** ou **nr_cpus=1**.

Para habilitar múltiplas CPUs no kernel de travamento, forneça **nr_cpus=*X*** (onde *X* é o número de processadores) e as opções **disable_cpu_apicid=0** na linha de comando do kernel.

A ferramenta criu

O Red Hat Enterprise Linux 7.2 introduz a ferramenta **criu** como uma Apresentação Prévia de Tecnologia. Esta ferramenta implementa **Checkpoint/Restore in User-space**, o qual pode ser usado para congelar um aplicativo em execução e armazená-lo como uma coleção de arquivos. Depois, o aplicativo pode ser restaurado do seu estado congelado.

A ferramenta **criu** depende de **Protocol Buffers**, um mecanismo extensível de plataforma neutra e linguagem neutra para serializar os dados estruturados. Os pacotes *protobuf* e *protobuf-c*, os quais fornecem essa dependência, também são adicionados ao Red Hat Enterprise Linux 7.2 como uma Apresentação Prévia de Tecnologia.

Namespace do usuário

Este recurso fornece uma segurança suplementar aos servidores executando os contêineres Linux ao fornecer um melhor isolamento entre o host e os contêineres. Os administradores de um contêiner não são mais capazes de desempenhar operações administrativas no host, aumentando a segurança.

Monitoração LPAR para IBM System z

Um driver de monitoração aprimorado para IBM System z está disponível como uma Apresentação Prévia de Tecnologia. Este driver fornece suporte às partições lógicas Linux (LPAR), assim como aos convidados Linux no hipervisor z/VM e fornece reinicialização automática e recursos de despejo automático, caso um sistema Linux não responda.

i40evf manipula grandes reconfigurações

O tipo mais comum de restauração que a Função Virtual (em inglês, Virtual Function - VF) encontra é a restauração da Função Física (em inglês, Physical Function - PF) que cascatea para baixo em uma restauração VF para cada VF. No entanto, para as restaurações 'maiores', tais como a restauração Core ou EMP, quando o dispositivo é reinicializado, a VF não obtinha anteriormente o mesmo VSI, assim a VF era incapaz de recuperar-se, já que continuava solicitando recursos para o seu VSI original. Como uma apresentação prévia de tecnologia, essa atualização adiciona um estado extra à máquina do estado da fila de administração para que o driver possa solicitar novamente suas informações de configuração em tempo de execução. Durante a recuperação da reparação, essa parte é definida no campo aq_required e as informações de configuração são analisadas antes de tentarem reativar o driver.

Suporte para o driver do kernel OPA

O driver do kernel Intel Omni-Path Architecture (OPA), que possui suporte como uma Apresentação Prévia de Tecnologia, fornece hardware Host Fabric Interconnect (HFI) com inicialização e configuração para transferências de Dados de Alto Desempenho para outros nós de E/S e computação em um cluster de Computação de Alto Desempenho (HPC).

Para instruções sobre como obter documentações do Intel Omni-Path, consulte https://access.redhat.com/articles/2039623.

Suporte para Diag0c no IBM System z

O Red Hat Enterprise Linux 7.2 introduz suporte ao recurso Diag0c no IBM System z como uma Apresentação Prévia de Tecnologia. O suporte ao Diag0c possibilita a leitura das métricas de desempenho da CPU fornecidas pelo hipervisor z/VM e permite a obtenção do tempo de gerenciamento para cada CPU online de uma máquina virtual Linux onde a tarefa de diagnosticar é executada.

Recurso 10GbE RoCE Express para RDMA

O Red Hat Enterprise Linux 7.2 inclui o recurso 10GbE RDMA no lugar do Converged Ethernet (RoCE) Express, como uma Apresentação Prévia de Tecnologia. Isto possibilita o uso de Ethernet e do Acesso Remoto Direto à Memória (RDMA), assim como das APIs Direct Access Programming Library (DAPL) e OpenFabrics Enterprise Distribution (OFED), no IBM System z.

Antes de usar este recurso em um sistema IBM z13, certifique-se de que o serviço mínimo exigido seja aplicado: z/VM APAR UM34525 e HW ycode N98778.057 (bundle 14).

Compactação zEDC no IBM System z

O Red Hat Enterprise Linux 7.2 inclui o driver de dispositivo de mecanismo Generic Workqueue (GenWQE) como uma Apresentação Prévia de Tecnologia. A tarefa inicial do driver é desempenhar a compactação e descompactação zlib dos formatos RFC1950, RFC1951 e RFC1952, mas isto pode ser ajustado para acelerar várias outras tarefas.

Capítulo 24. Sistema de Rede

Rebase de i40e e i40evf para as versões 1.3.21-k e 1.3.13

Os drivers do kernel i40e e i40evf foram atualizados para as versões 1.3.21-k e 1.3.13. Esses drivers atualizados estão incluídos como uma Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7.2.

Antigamente, uma tentativa de executar comandos relacionados a iSCSI em portas i40e gerava a perda de conectividade de rede fora dessas portas. Esta atualização corrige este erro e o sistema agora permite que os comandos iSCSI prossigam.

Driver Cisco usNIC

Os servidores Cisco UCM (em inglês, Unified Communication Manager) possuem um recurso opcional para fornecer um Cisco proprietary User Space Network Interface Controller (usNIC), o qual permite o desempenho de operações do tipo de Acesso Remoto Direto à Memória (RDMA) para os aplicativos de espaço de usuários. O driver libusnic_verbs, que possui suporte como uma Apresentação Prévia de Tecnologia, possibilita a utilização de dispositivos usNIC via programação RDMA InfiniBand padrão baseada em API Verbs.

Driver do kernel Cisco VIC

O driver do kernel Cisco VIC, o qual possui suporte como uma Apresentação Prévia de Tecnologia, permite o uso da semântica do tipo de Acesso Remoto Direto à Memória (RDMA) nas arquiteturas Cisco.

Trusted Network Connect

Trusted Network Connect, com suporte como uma Apresentação Prévia de Tecnologia, é usado com soluções de controle de acesso à rede existentes (NAC), tais como TLS, 802.1X ou IPsec, para integrar avaliações de postura de pontos de extremidade; o que significa coletar informações do sistema dos pontos de extremidade (como parâmetros de configuração do sistema operacional, pacotes instalados e outros, denominados como medidas de integridade). Trusted Network Connect é usado para verificar essas medidas em relação às políticas de acesso à rede antes de permitir que os pontos de extremidade acessem a rede.

Funcionalidade SR-IOV no driver qlcnic

O suporte para a virtualização de E/S de raiz única (SR-IOV) foi adcionado ao driver qlcnic como uma Apresentação Prévia de Tecnologia. O suporte para esta funcionalidade será fornecido diretamente pelo QLogic e os clientes são incentivados a encaminhar comentários para QLogic e a Red Hat. As outras funcionalidades no driver qlnic permanecem com total suporte.

Capítulo 25. Armazenamento

Agendamento de E/S das filas múltiplas para SCSI

O Red Hat Enterprise Linux 7.2 inclui um novo mecanismo de agendamento de E/S de filas múltiplas para dispositivos de blocos conhecidos como blk-mq. O pacote scsi-mq permite ao subsistema da Interface de Sistemas para Pequenos Computadores (SCSI) utilizar esse novo mecanismo de fila. Essa funcionalidade é fornecida como uma Apresentação Prévia de Tecnologia e não é habilitada por padrão. Para habilitá-la, adicione **`scsi_mod.use_blk_mq=Y`** à linha de comando do kernel.

Infraestrutura de bloqueio LVM aprimorada

`lvmlockd` é uma infraestrutura de bloqueio de nova geração para LVM. Ela permite ao LVM gerenciar com segurança armazenamentos compartilhados de múltiplos hosts, usando os gerenciadores de bloqueio **`dlm`** ou **`sanlock`**. **`sanlock`** permite **`lvmlockd`** coordenar hosts através de bloqueios baseados em armazenamentos sem a necessidade de uma infraestrutura de cluster completa. Para mais informações, consulte a página manual **`lvmlockd`**(8).

Plug-in targetd da API libStorageMgmt

Desde o Red Hat Enterprise Linux 7.1, o gerenciamento da matriz de armazenamento com libStorageMgmt, uma API independente da matriz de armazenamento, tem recebido suporte completo. A API fornecida é consistente e estável e permite que os desenvolvedores gerenciem de forma esquematizada as diferentes matrizes de armazenamentos e utilizem os recursos acelerados por hardware fornecidos. Os administradores de sistema também podem usar libStorageMgmt para configurar manualmente e automatizar tarefas de gerenciamento de armazenamento com a interface de linha de comando incluída.

O plug-in Targetd não possui suporte completo e permanece uma Apresentação Prévia de Tecnologia.

DIF/DIX

O DIF/DIX é uma nova adição ao Padrão SCSI. Possui suporte completo no Red Hat Enterprise Linux 7.2 para HBAs e matrizes de armazenamento especificadas no capítulo Recursos, mas permanece na Apresentação Prévia de Tecnologia para todas as outras matrizes de armazenamento e HBAs.

O DIF/ DIX aumenta o tamanho do bloco de disco habitual de 512 bytes para 520 bytes, adicionando o Campo de Integridade de Dados (em inglês, Data Integrity Field - DIF). O DIF armazena um valor de soma de verificação para o bloco de dados que é calculado pelo Adaptador de Barramento de Host (HBA) quando ocorre uma gravação. O dispositivo de armazenamento, então, confirma a soma de verificação e armazena tanto os dados como a soma de verificação. Por outro lado, quando ocorre uma leitura, a soma de verificação pode ser verificada pelo dispositivo de armazenamento e pelo HBA receptor.

Capítulo 26. Virtualização

Virtualização aninhada

O Red Hat Enterprise Linux 7.2 oferece o recurso de virtualização aninhada, como uma Apresentação Prévia de Tecnologia. Este recurso permite que a KVM lance máquinas virtuais que possam atuar como hipervisores e criar suas próprias máquinas virtuais.

A ferramenta virt-p2v

O Red Hat Enterprise Linux 7.2 oferece a ferramenta virt-p2v como uma Apresentação Prévia de Tecnologia. Virt-p2v (físico para virtual) é uma imagem PXE, ISO ou CD-ROM que o usuário pode inicializar em uma máquina física e que cria uma máquina virtual KVM com conteúdos de disco idênticos aos da máquina física.

USB 3.0 suporte aos convidados KVM

A emulação do adaptador host USB 3.0 (xHCI) para convidados KVM permanece uma Apresentação Prévia de Tecnologia no Red Hat Enterprise Linux 7.2.

Suporte a VirtIO-1

Os drivers virtio foram atualizados para o kernel 4.1 para fornecer Suporte ao Dispositivo VirtIO 1.0.

Capítulo 27. Atomic Host e Contêineres

SSSD em contêiner

O SSSD em contêiner é fornecido como uma Apresentação Prévia de Tecnologia para permitir que o subsistema de autenticação do Red Hat Enterprise Linux Atomic Host seja conectado a provedores de identidade central, como o Red Hat Identity Management e Microsoft Active Directory.

Parte III. Drivers de Dispositivos

Este capítulo fornece uma lista detalhada de todos os drivers de dispositivos que foram atualizados no Red Hat Enterprise Linux 7.2.

Capítulo 28. Atualizações dos Drivers de Armazenamento

- O driver hpsa foi atualizado para a versão 3.4.4-1-RH4.
- O driver qla2xxx foi atualizado para a versão 8.07.00.18.07.2-k.
- O driver lpfc foi atualizado para a versão 10.7.0.1.
- O driver megaraid_sas foi atualizado para a versão 06.807.10.00.
- O driver fnic foi atualizado para a versão 1.6.0.17.
- O driver mpt2sas foi atualizado para a versão 20.100.00.00.
- O driver mpt3sas foi atualizado para a versão 9.100.00.00.
- O driver Emulex be2iscsi foi atualizado para a versão 10.6.0.0r.
- O driver aacraid foi atualizado para a versão 1.2.
- O driver bnx2i foi atualizado para a versão 2.7.10.1.
- O driver bnx2fc foi atualizado para a versão 2.4.2.

Capítulo 29. Atualizações dos Drivers de Rede

- O driver tg3 foi atualizado para a versão 3.137.
- O driver e1000 foi atualizado para a versão 7.3.21-k8-NAPI, a qual fornece suporte para o atraso da atualização txtd quando usando a variável booliana xmit_more.
- O driver e1000e foi atualizado para a versão 3.2.5-k.
- O driver igb foi atualizado para a versão 5.2.15-k.
- O driver igbvf foi atualizado para a versão 2.0.2-k.
- O driver ixgbevf foi atualizado para a versão 2.12.1-k.
- O driver ixgbe foi atualizado para a versão 4.0.1-k.
- Os drivers bna e firmware foram atualizados para a versão 3.2.23.0r.
- O driver bnx2 foi atualizado para a versão 2.2.6.
- O driver CNIC foi atualizado para a versão 2.5.21.
- O driver bnx2x foi atualizado para a versão 1.710.51-0, a qual também adiciona suporte a NPAR qlogic para os adaptadores qlogic-nx2.
- O driver be2net foi atualizado para a versão 10.6.0.3r.
- O driver qlcnic foi atualizado para a versão 5.3.62.
- O driver qlge foi atualizado para a versão 1.00.00.34, a qual corrige uma condição de corrida entre o registro e o cancelamento de registro da Nova API (NAPI) que levava, anteriormente, à falha do sistema. Esta condição ocorria quando certos parâmetros eram alterados enquanto o Cartão de Interface de Rede (NIC) estava 'desativado'.
- O driver r8169 foi atualizado para a versão 2.3LK-NAPI.
- O driver i40e foi atualizado para a versão 1.3.21-k.
- O driver i40evf foi atualizado para a versão 1.3.13.
- O driver netxen_nic foi atualizado para a versão 4.0.82.
- O driver sfc foi atualizado para a versão upstream mais recente.
- Esta atualização adiciona o driver fm10k da versão 0.15.2-k.
- Esta atualização adiciona suporte a VTI6 , incluindo recursos netns.
- O driver bonding foi atualizado para a versão 3.7.1.
- O driver iwlwifi foi atualizado para a versão upstream mais recente.
- O driver vxlan foi atualizado para a versão 0.1.

Capítulo 30. Atualizações dos Drivers de Gráficos e Drivers Diversos

- O driver HDA foi atualizado para a versão upstream mais recente para usar o novo método jack kctls.
- O driver HPI foi atualizado para a versão 4.14.
- O driver Realtek HD-audio codec foi atualizado para incluir a atualização dos códigos de inicialização EAPD.
- O driver IPMI foi atualizado para substituir o uso de timespec por timespec64.
- O driver i915 foi atualizado para incluir a rebase do driver ACPI Video Extensions no Red Hat Enterprise Linux 7.2.
- O driver ACPI Fan foi atualizado para a versão 0.25.
- O driver Update NVM-Express foi atualizado para a versão 3.19.
- O driver rtsx foi atualizado para a versão 4.0 para fornecer suporte aos chips rtl8402, rts524A, rts525A.
- O driver do dispositivo Generic WorkQueue Engine foi atualizado para a versão upstream mais recente.
- O driver PCI foi atualizado para a versão 3.16.
- O módulo kernel EDAC foi atualizado para fornecer suporte aos processadores Intel Xeon v4.
- O driver pstate foi atualizado para fornecer suporte à 6ª Geração dos processadores Intel Core.
- O driver intel_idle foi atualizado para fornecer suporte à 6ª Geração dos processadores Intel Core.

Parte IV. Funcionalidades Preteridas

Esta seção fornece uma visão geral das funcionalidades que foram preteridas em todos os lançamentos de manutenção até o Red Hat Enterprise Linux 7.2.

Capítulo 31. Funcionalidades Preteridas no Red Hat Enterprise Linux 7

As funcionalidades preteridas continuam a receber suporte até o fim do ciclo de vida do Red Hat Enterprise Linux 7. Elas não receberão suporte nos lançamentos principais futuros deste produto e não são recomendadas para as novas implantações.

Os componentes de *hardware* preteridos não são recomendados para as novas implantações nos lançamentos principais atuais ou futuros. As atualizações de drivers do hardware estão limitadas às correções críticas e de segurança apenas. A Red Hat recomenda a substituição do hardware assim que possível.

Um *pacote* pode ser preterido ou não recomendado para uso posterior. Sob tais circunstâncias, o pacote deve ser removido do produto. A documentação do produto identificará os pacotes mais recentes que oferecem funcionalidades semelhantes, idênticas ou mais avançadas do que aquela preterida e fornecerá outras recomendações.

Emulex Boards

Os Emulex Boards a seguir provavelmente não receberão suporte no próximo lançamento principal:

Tabela 31.1. Emulex Boards Preteridos

Dispositivos BladeEngine 2 (BE2)	
0x0704	TIGERSHARK FCOE
0x0700	TIGERSHARK NIC
0x0702	TIGERSHARK ISCSI
Dispositivos Fibre Channel (FC)	
0x1ae5	FIREFLY
0xe100	PROTEUS_VF
0xe131	BALIUS
0xe180	PROTEUS_PF
0xf095	RFLY
0xf098	PFLY
0xf0a1	LP101
0xf0a5	TFLY
0xf0d1	BSMB
0xf0d5	BMID
0xf0e1	ZSMB
0xf0e5	ZMID
0xf0f5	NEPTUNE
0xf0f6	NEPTUNE_SCSP
0xf0f7	NEPTUNE_DCSP
0xf180	FALCON
0xf700	SUPERFLY
0xf800	DRAGONFLY
0xf900	CENTAUR
0xf980	PEGASUS
0xfa00	THOR
0xfb00	VIPER

Dispositivos Fibre Channel (FC)	
0xfc00	LP10000S
0xfc10	LP11000S
0xfc20	LPE11000S
0xfc50	PROTEUS_S
0xfd00	HELIOS
0xfd11	HELIOS_SCSP
0xfd12	HELIOS_DCSP
0xfe00	ZEPHYR
0xfe05	HORNET
0xfe11	ZEPHYR_SCSP
0xfe12	ZEPHYR_DCSP

Para verificar as IDs do PCI do hardware no seu sistema, execute o comando **`lspci -nn`**.

Parte V. Problemas Conhecidos

Esta seção documenta os problemas conhecidos no Red Hat Enterprise Linux 7.2.

Capítulo 32. Atualizações Gerais

É possível que ocorram falhas no upgrade do Red Hat Enterprise Linux 6 em IBM Power Systems

Devido a um erro no carregador de inicialização **`yaboot`**, é possível que ocorram problemas no upgrade do Red Hat Enterprise Linux 6 para o Red Hat Enterprise Linux 7 nos servidores IBM Power Systems, com uma falha **`Unknown or corrupt filesystem`**.

Este problema é causado, geralmente, por um arquivo de configuração **`yaboot.conf`** posicionado incorretamente. Certifique-se de que este arquivo exista, seja válido e esteja posicionado em uma partição /boot (não-LVM) padrão.

O arquivo /etc/os-release contém informações desatualizadas depois do upgrade do sistema

O upgrade ao próximo lançamento de manutenção (por exemplo, do Red Hat Enterprise Linux 7.1 para o 7.2) não atualiza o arquivo **`/etc/os-release`** com o novo número do produto. No lugar disto, o arquivo continua a listar o número de lançamento anterior e um novo arquivo, nomeado **`os-release.rpmnew`**, é posicionado no diretório **`/etc`**.

Se você precisar do arquivo **`/etc/os-release`** atualizado, substitua-o por **`/etc/os-release.rpmnew`**.

Capítulo 33. Autenticação e Interoperabilidade

As solicitações do tíquete Kerberos são recusadas para tempo de vida curto

Devido a um erro no Active Directory, as solicitações do tíquete Kerberos para tempos de vida curtos (geralmente abaixo de três minutos) são recusadas. Para contornar este problema, solicite tíquetes com vidas mais longas (acima de cinco minutos).

A réplica de uma máquina Red Hat Enterprise Linux 7 em uma máquina Red Hat Enterprise Linux 6 gera falhas

Atualmente, os tipos de criptografia Kerberos Camellia (enctypes) são incluídos como possíveis enctypes padrão nos pacotes krb5, krb5-libs e krb5-server. Assim, a réplica de uma máquina Red Hat Enterprise Linux 7 em uma máquina Red Hat Enterprise Linux 6 gera falhas com uma mensagem de erro. Para contornar este problema, use os controles enctype padrão ou avise kadmin ou ipa-getkeytab quais tipos de criptografia usar.

Mensagem de erro inofensiva é registrada em log na inicialização do SSSD

Se o SSSD é conectado a um servidor IdM que não tem uma relação de confiança estabelecida com um servidor AD, a mensagem de erro inofensiva a seguir é impressa no registro de domínio na inicialização do SSSD:

Erro Interno (Erro de memória de buffer)

Para evitar que esta mensagem de erro inofensiva ocorra, defina **`subdomains_provider`** como **`none`** no arquivo sssd.conf, caso o ambiente não espere configurar nenhum domínio confiável.

As zonas DNS, com as chaves DNSSEC recentemente geradas, não estão sendo assinadas adequadamente

O IdM não assina adequadamente as zonas DNS com as chaves de Extensões de Segurança DNS (DNSSEC) geradas recentemente. O serviço named-pkcs11 registra o seguinte erro nesta situação:

O atributo não existe: 0x00000002

A falha é causada por um erro na condição de corrida no processo de distribuição e geração de chaves DNSSEC. A condição de corrida impede que named-pkcs11 acesse as novas chaves DNSSEC.

Para contornar este problema, reinicie named-pkcs11 no servidor afetado. Depois de reiniciado, a zona DNS é assinada adequadamente. Observe que, o erro pode reaparecer depois das chaves DNSSEC serem alteradas novamente.

A versão realmd antiga é iniciada durante a atualização do realmd enquanto em execução

O daemon **`realmd`** é iniciado apenas quando solicitado e, então, desempenha uma determinada ação e, após um momento, atinge tempo limite. Quando **`realmd`** é atualizado ainda em execução, a versão antiga do **`realmd`** é iniciada mediante uma próxima solicitação, pois **`realmd`** não é reiniciado após a atualização. Para contornar este problema, certifique-se de que **`reamld`** não esteja em execução antes de atualizá-lo.

As opções do ipa-server-install e ipa-replica-install são não validadas

Os utilitários **ipa-server-install** e **ipa-replica-install** não validam atualmente as opções fornecidas a eles. Caso o usuário passe os valores incorretos aos utilitários, ocorre falha na instalação. Para contornar o problema, certifique-se de fornecer os valores corretos e, então, execute os utilitários novamente.

Se a versão openssl necessária não é instalada, a atualização dos pacotes ipa gera falhas

Quando o usuário tenta realizar o upgrade dos pacotes **ipa**, o Gerenciamento de Identidade (IdM) não instala automaticamente a versão necessária dos pacotes **ipa**. Como consequência, se a versão 1.0.1e-42 do **openssl** não é instalada antes do usuário executar o comando **yum update ipa***, o upgrade falha durante a configuração do serviço DNSKeySync.

Para contornar este problema, atualize manualmente **openssl** para a versão 1.0.1e-42, ou mais recente, antes de atualizar **ipa**. Isto impede a falha do upgrade.

Capítulo 34. Compilador e Ferramentas

Múltiplos erros durante a inicialização a partir de SAN sobre FCoE

Os múltiplos erros surgiram da atual implementação de inicialização a partir da Storage Area Network (SAN) usando Fibre Channel sobre Ethernet (FCoE). A Red Hat está em busca de uma versão futura do Red Hat Enterprise Linux 7 que corrija esses erros. Para uma lista dos erros afetados e das soluções alternativas (quando disponíveis), por favor entre em contato com o seu representante da equipe de suporte da Red Hat.

Valgrind não pode executar programas compilados em relação à versão anterior do Open MPI

O Red Hat Enterprise Linux 7.2 oferece suporte somente à interface binária do aplicativo (ABI) Open MPI na versão 1.10, a qual é incompatível com a versão 1.6 do Open MPI ABI anteriormente distribuída. Como consequência, os programas compilados em relação à versão anterior do Open MPI não podem ser executados sob o Valgrind incluído no Red Hat Enterprise Linux 7.2. Para contornar este problema, utilize a versão do Valgrind do Red Hat Developer Toolset para programas ligados à versão 1.6 do Open MPI.

As funções sintéticas geradas pelo GCC confundem o System Tap

A otimização do GCC pode gerar funções sintéticas para as cópias parcialmente embutidas de outras funções. Essas funções sintéticas parecem funções de primeira classe e confundem as ferramentas, tais como System Tap e GDB, pois as investigações do System Tap podem ser substituídas nos pontos de entrada tanto de funções reais quanto sintéticas. Isto pode resultar em múltiplas ocorrências de investigação do System Tap por uma única chamada da função subjacente.

Para contornar este problema, um script do System Tap pode precisar adotar contramedidas, tais como a detecção de recursão e a supressão de investigações, relacionadas às funções parciais embutidas. Por exemplo, o scrip a seguir:

probe kernel.function("can_nice").call { }

conseguiu evitar o problema descrito abaixo:

global in_can_nice% probe kernel.function("can_nice").call { in_can_nice[tid()] ++; if (in_can_nice[tid()] > 1) { next } /* real probe handler here */ } probe kernel.function("can_nice").return { in_can_nice[tid()] --; }

Observe que este script não leva em consideração todos os cenários possíveis. Ele não funcionaria como esperado no caso de, por exemplo, kprobes ou kretprobes ausentes, ou da recursão genuína desejada.

AVC do SELinux gerado quando o ABRT coleciona backtraces

Se o novo e opcional recurso do ABRT, que permite a coleção de backtraces dos processos com falhas sem precisar de gravar um arquivo de despejo de memória no disco, estiver habilitado (usando a opção **`CreateCoreBacktrace`** no arquivo de configuração **`/etc/abrt/plugins/CCpp.conf`**), uma mensagem do AVC do SELinux é gerada quando a ferramenta **`abrt-hook-ccpp`** tenta usar o acesso **`sigchld`** em um processo com falhas para obter a lista de funções na pilha do processo.

GDB mantém watchpoints ativos mesmo depois de relatá-los como ocorrências

Em alguns casos, na arquitetura 64-bit ARM, o GDB pode manter watchpoints ativos incorretamente, mesmo após relatá-los como ocorrências. Isto faz com que os watchpoints sejam atingidos pela segunda vez, e somente desta vez a indicação do hardware não é mais reconhecida como um watchpoint e é impressa como um sinal SIGTRAP genérico. Existem várias formas de contornar este problema e interromper o

relatório SIGTRAP excessivo.

* Digite **`continue`** (continuar) ao ver um SIGTRAP depois de um watchpoint foi atingido.

* Instrua o GDB a ignorar o sinal SIGTRAP adicionando a seguinte linha ao seu arquivo de configuração **`~/.gdbinit`**:

handle SIGTRAP nostop noprint

* Utilize os watchpoints de software no lugar dos seus equivalentes de hardware. Observe que a depuração é bem mais lenta com os watchpoints de software e apenas o comando **`watch`** está disponível (e não **`rwatch`** ou **`awatch`**). Adicione a seguinte linha ao seu arquivo de configuração **`~/.gdbinit`**:

set can-use-hw-watchpoints 0

Ocorre falha na inicialização usando grubaa64.efi

Devido a problemas no pxeboot ou no arquivo de configuração PXE, a instalação do Red Hat Enterprise Linux 7.2 com o carregador de inicialização grubaa64.efi 7.2 falha ou experimenta grande atraso na inicialização do sistema operacional. Como uma solução alternativa, use o arquivo grubaa64.efi 7.1 no lugar do arquivo grubaa64.efi 7.2, ao instalar o Red Hat Enterprise Linux 7.2.

O recurso MPX no GCC exige a versão Red Hat Developer Toolset da biblioteca libmpx

A biblioteca libmpxwrappers não possui a versão gcc-libraries da biblioteca libmpx. Como resultado, o recurso Extensões de Proteção de Memória (MPX) pode não funcionar adequadamente no GCC e o aplicativo pode não vincular corretamente. Para contornar este problema, use a versão Red Hat Developer Toolset 4.0 da biblioteca libmpx.

Capítulo 35. Área de trabalho (Desktop)

As dependências quebradas do pacote pygobject3 impedem a atualização do Red Hat Enterprise Linux 7.1.

O pacote de 32 bits *pygobject3-devel.i686* foi removido do Red Hat Enterprise Linux 7.2 e substituído por uma versão multilib. Se você tiver a versão de 32 bits do pacote instalado no sistema Red Hat Enterprise Linux 7.1, você encontrará um erro **yum** ao tentar atualizar para o Red Hat Enterprise Linux 7.2.

Para contornar este problema, utilize o comando **yum remove pygobject3-devel.i686** como **root** para desinstalar a versão de 32 bits do pacote antes de atualizar o seu sistema.

Requisitos de compilação não foram definidos corretamente para Emacs

A versão anterior a 2.23.52.0.1-54 do pacote *binutils* gera uma falha de segmentação durante a compilação. Como consequência, não é possível compilar o editor de texto Emacs em IBM Power Systems. Para contornar este problema, instale o *binutils* mais recente.

Problemas de exibição externa ao combinar o encaixe/desencaixe e a suspensão do laptop

No ambiente desktop GNOME, em alguns laptops, as exibições externas conectadas a uma estação de encaixe podem não ser ativadas automaticamente durante a restauração de um laptop suspenso depois de desencaixá-lo e encaixá-lo novamente.

Para contornar este problema, abra o painel de configuração Exibições ou execute o comando **xrandr** em um terminal. Isto disponibiliza as exibições externas novamente.

Emacs é finalizado inesperadamente, às vezes, com o uso da seta pra cima em ARM

Na arquitetura ARM, o editor de texto **Emacs** é finalizado inesperadamente, algumas vezes, com uma falha de segmentação ao rolar para cima um buffer de arquivo. Isto acontece somente quando o realce de sintaxe está habilitado. Atualmente, não há uma solução alternativa para este problema.

Capítulo 36. Instalação e Inicialização

A instalação falha com um traceback durante a especificação de %packages --nobase --nocore em um arquivo Kickstart

O uso de um arquivo Kickstart, que contém a seção **%packages** e especifica as opções **--nobase** e **--nocore** ao mesmo tempo, provoca falha na instalação com uma mensagem de traceback por conta do pacote *yum-langpacks* ausente.

Para contornar este problema, adicione o pacote *yum-langpacks* na seção **%packages** ao usar **%packages --nobase --nocore** no seu arquivo Kickstart.

A instalação não pode proceder se uma senha root especificada no kickstart não passar pelos requisitos de política.

Se você usar um arquivo Kickstart que define uma senha root e a senha não satisfazer os requisitos para a política de segurança, você não será capaz de finalizar a instalação. O botão **Begin Installation** (Iniciar Instalação) ficará acinzentado e não será possível alterar a senha root manualmente antes de pressionar este botão.

Para contornar este problema, certifique-se de que seu arquivo Kickstart use uma senha suficientemente forte que passe nos requisitos definidos pela política de segurança selecionada.

Falha no modo de resgate ao detectar e montar o volume root em Btrfs

O modo de resgate do instalador (acessado a partir do menu de inicialização da mídia de instalação ou usando a opção de inicialização **inst.rescue**) não pode detectar um sistema existente com o diretório (root) **/** posicionado em um subvolume Btrfs. No lugar disto, uma mensagem de erro é exibida dizendo 'Você não possui nenhuma partição linux'.

Para contornar este problema, insira o shell e monte o volume root manualmente.

Título de janela errado na Configuração Inicial

A ferramenta Configuração Inicial, exibida automaticamente depois da primeira reinicialização pós-instalação e que permite que você defina as configurações, como conexões de rede, e registre seu sistema, exibe a cadeia de caracteres **__main__.py** no título da janela.

Trata-se, no entanto, de um problema superficial que não possui impacto negativo na usabilidade.

A reinstalação em um FBA DASD no IBM System z gera falhas no instalador

A reinstalação do Red Hat Enterprise Linux 7 no IBM System z com um Fixed Block Architecture (FBA) DASD, gera falhas no instalador devido ao suporte incompleto para estes dispositivos.

Para contornar este problema, certifique-se de que nenhum FBA DASD esteja presente durante a instalação, posicionando-os na lista de desconhecimento de dispositivos. Isto deve ser feito antes de iniciar o instalador. A partir de um shell root, use o comando **chccwdev** seguido do comando **cio_ignore** para manualmente mudar os dispositivos para offline e, então, adicioná-los à lista de desconhecimento de dispositivos.

Alternativamente, você pode remover todas as IDs do dispositivo FBA DASD do arquivo de configuração CMS ou do arquivo de parâmetros, em vez de usar esses comandos antes de iniciar a instalação.

Aliases HyperPAV não estão disponíveis depois da instalação no IBM System z

Um problema conhecido impede que os DASDs, configurados como aliases HyperPAV, sejam automaticamente anexados ao sistema após a finalização da instalação. Estes dispositivos de armazenamento estão disponíveis na tela Destino de Instalação durante a instalação, mas não são acessíveis imediatamente após o término da instalação e reinicialização.

Para resolver este problema temporariamente (até a próxima reinicializaçã), remova estes dispositivos da lista negra de dispositivos usando o comando **chccwdev**:

```
# chccwdev -e <devnumber>
```

Para disponibilizar os aliases HyperPAV de maneira persistente em todas as reinicializações, adicione seus números de dispositivos no arquivo de configuração **/etc/dasd.conf**.

Você pode usar o comando **lsdasd** para verificar se esses dispositivos estão disponíveis.

O arquivo anaconda-ks.cfg gerado no IBM System z não pode ser usado para a reinstalação do sistema

O arquivo **anaconda-ks.cfg**, um arquivo Kickstart gerado durante a instalação do sistema que contém todas as seleções feitas durante o processo de instalação, representa os tamanhos de disco como números decimais nos DASDs do IBM System z. Isto acontece porque os DASDs notificam um alinhamento de 4KiB, o que deixa os tamanhos dos discos calculados incorretamente, à medida que são registrados no arquivo Kickstart, pois somente os valores inteiros são aceitos. Portanto, não é possível reutilizar o arquivo Kickstart gerado para reproduzir a instalação.

O uso do arquivo **anaconda-ks.cfg** no IBM System z para a reinstalação do sistema exige que você altere manualmente todos os valores decimais dentro dos inteiros.

Possíveis mensagens de erro do NetworkManager durante instalação

Ao instalar o sistema, a seguinte mensagem de erro pode ser exibida e registrada em log:

ERR NetworkManager: <error> [devices/nm-device.c:2590] activation_source_schedule(): (eth0): estágio de ativação já agendado

A mensagem de erro não deve impedir a conclusão da instalação.

O pacote libocrdma está ausente do grupo do pacote InfiniBand Support

O pacote *libocrdma* não está incluído no conjunto de pacotes padrão do grupo InfiniBand Support. Consequentemente, quando os usuários selecionam o grupo InfiniBand Support e esperam que o RDMA over Converged Ethernet (RoCE) funcione nos adaptadores Emulex OneConnect, o driver necessário, *libocrdma*, não é instalado por padrão.

Na primeira inicialização, o usuário pode instalar manualmente o pacote ausente, emitindo o seguinte comando:

```
# yum install libocrdma
```

De maneira alternativa, adicione o pacote *libocrdma* à seção **%packages** do seu arquivo Kickstart.

Desta forma, o usuário será capaz de usar os dispositivos Emulex OneConnect no modo RoCE.

O tamanho insuficiente da partição /boot pode impedir o sistema de receber upgrade

A partição /boot, que contém kernels instalados e discos ram iniciais, pode ficar cheia, caso múltiplos kernels e pacotes adicionais, como *kernel-debug*, sejam instalados. Isto acontece pelo fato do tamanho padrão desta partição estar especificado para 500 MB durante a instalação, o que impede o sistema de receber upgrades.

Como uma solução alternativa, use **yum** para remover kernels mais antigos, caso você não precise deles. Se você estiver instalando um novo sistema, você também deve considerar esta possibilidade, e definir a partição /boot para um tamanho maior (por exemplo, 1 GB), em vez do padrão (500 MB).

A instalação nos dispositivos multipath falha se um ou mais discos não possuírem um rótulo

Durante a instalação nos dispositivos multipath, o instalador pode exibir uma caixa de diálogo de erro se ele não conseguir ler um ou mais discos que são membros do multipath. Este problema é gerado quando um ou mais discos não possuem um rótulo de disco e a instalação não pode prosseguir caso isto ocorra.

Para contornar este problema, crie rótulos de disco em todos os discos que fazem parte do dispositivo multipath que você está usando durante a instalação.

A configuração IPv4 estática no Kickstart é substituída se um nome de host estiver definido no script %pre

Ao definir um nome de host na seção **%pre** de um arquivo Kickstart, o comando **network** que estabelece somente nomes de host ("network --hostname=hn") é considerado como uma configuração do dispositivo com o valor padrão --bootproto ("dhcp") e o valor padrão **--device** ("link", significa o primeiro dispositivo com o link localizado). O Kickstart, então, comporta-se como se **network --hostname=hn --device=link** fosse usado.

Se o dispositivo considerado como padrão para a opção **--device** (o primeiro dispositivo com o link localizado) já tiver sido configurado para usar a configuração IPv4 estática (por exemplo, com o comando precedente **network**), a configuração é sobrescrita pelo IPv4 DHCP implícito pela opção **--hostname**.

Para contornar este problema, certifique-se de que o comando **network**, que define o nome do host, seja usado primeiro e o segundo comando **network**, que seria sobrescrito normalmente, seja usado depois.

Nos casos em que o comando **network** definindo um nome de host é o único comando deste tipo no arquivo Kickstart, adicione uma opção **--device** a ele com uma interface não existente (por exemplo, **network --hostname=hn --device=x**).

O uso do comando realm no Kickstart faz com que o instalador trave

Um problema conhecido impede que o comando **realm** seja usado nos arquivos Kickstart. A tentativa de ingressar em um domínio do Gerenciamento de Identidade e do Active Directory durante a instalação usando este comando faz com o instalador trave.

Para contornar este problema, você pode esperar até que a instalação termine e, depois, ingressar em um domínio manualmente ou você pode adicionar o comando **realm join <realm name>** à seção **%post** do arquivo Kickstart. Consulte a página manual **realm(8)** para informações sobre o ingresso em domínios usando a linha de comando.

A ajuda interna do instalador não é atualizada durante o upgrade do sistema

Ao realizar o upgrade do Red Hat Enterprise Linux 7.1 para a versão 7.2, a ajuda interna do instalador Anaconda (o pacote *anaconda-user-help*) não recebe upgrades devido a uma alteração significante no pacote.

Para contornar este problema, use **yum** para remover o pacote *anaconda-user-help* antes de desempenhar o upgrade e instale-o novamente depois de concluir o upgrade para o Red Hat Enterprise Linux 7.2.

Ordenação incorreta das entradas do menu de inicialização gerada por grubby

A ferramenta **grubby**, que é usada para modificar e atualizar os arquivos de configuração do carregador de inicialização GRUB2, pode adicionar as entradas do menu de inicialização de depuração no topo da lista ao gerar o arquivo de configuração do menu de inicialização. Portanto, essas entradas do menu de depuração fazem com que as entradas normais sejam empurradas para baixo, apesar de ainda estarem realçadas e selecionadas por padrão.

O uso de múltiplas imagens de atualização do driver ao mesmo tempo aplica-se somente à última imagem selecionada

Ao tentar desempenhar uma atualização de driver durante a instalação usando a opção de inicialização **inst.dd=/dd.img** e especificando-a mais de uma vez para carregar múltiplas imagens de atualização do driver, o Anaconda ignorará todas as instâncias do parâmetro, com exceção da última.

Para contornar este problema, você pode:

* Instalar drivers adicionais após a instalação, se possível

* Usar meios diferentes para especificar uma imagem de atualização de driver, como o comando Kickstart **driverdisk**

* Combinar múltiplas imagens de atualização de driver em uma única imagem

Ocorrem falhas no instalador quando ele detecta DASDs em formato LDL

Ocorrem falhas no instalador toda vez que ele detecta o formato LDL (Linux Disk Layout) em um ou mais DASDs no IBM System z. As falhas são causadas por uma condição de corrida na biblioteca **libparted** e acontecem mesmo quando esses DASDs não são selecionados como destinos de instalação. Outras arquiteturas não são afetadas por este problema.

Se os DASDs LDL tiverem que ser usados durante a instalação, os usuários devem reformatar manualmente cada DASD LDL como CDL (Compatible Disk Layout), usando o comando **dasdfmt** em um shell root antes de iniciar o instalador.

Caso os DASDs LDL estejam presentes em um sistema e o usuário não deseja utilizá-los durante a instalação, eles devem ser posicionados na lista de desconhecimento de dispositivos pela duração do processo de instalação. Isto deve ser feito antes de iniciar o instalador. A partir de um shell root, os usuários devem usar o comando **chccwdev** seguido do comando **cio_ignore** para manualmente mudar os dispositivos para offline e, então, adicioná-los à lista de desconhecimento de dispositivos.

Alternativamente, você pode remover todas as IDs do dispositivo DASD LDL do arquivo de configuração CMS ou do arquivo de parâmetros, em vez de usar esses comandos antes de iniciar a instalação.

Pânico do kernel na reinicialização após o upgrade dos pacotes redhat-release e do kernel

A instalação dos pacotes *kernel* e *redhat-release-server-7.2-9.el7* na mesma transação Yum faz com que uma linha **initrd** fique ausente na nova entrada de menu do kernel na configuração GRUB2. A tentativa de inicializar usando o último kernel instalado gera, então, um pânico do kernel devido ao initrd ausente. Este problema geralmente acontece ao realizar o upgrade do sistema de um lançamento de manutenção mais

antigo para o Red Hat Enterprise Linux 7.2 usando **`yum update`**.

Para contornar este problema, certifique-se de realizar o upgrade dos pacotes *redhat-release-server* e *kernel* em transações Yum separadas. Alternativamente, você pode localizar a nova entrada de menu do kernel no arquivo de configuração GRUB2 (**`/boot/grub2/grub.cfg`** em sistemas BIOS e **`/boot/efi/EFI/redhat/grub.cfg`** em sistemas UEFI) e adicionar o initrd manualmente.

A linha de configuração initrd será parecida com **`initrd /initramfs-3.10.0-327.el7.x86_64.img`**. Certifique-se de que o nome do arquivo corresponda ao kernel (vmlinuz) configurado na mesma entrada de menu e que o arquivo exista no diretório **`/boot`**. Use entradas de menu mais antigas para referência.

A configuração Inicial pode ser iniciada em modo texto mesmo que um ambiente gráfico esteja instalado

O utilitário Configuração Inicial, iniciado após a instalação ser concluída e o sistema instalado ser iniciado pela primeira vez, pode, em alguns casos, ser iniciado em modo texto nos sistemas mesmo onde um ambiente gráfico está disponível e a versão gráfica da Configuração Inicial deve ser iniciada. Isto é gerado pelos serviços tanto de modo texto quanto de modo gráfico sendo habilitados ao mesmo tempo para a Configuração Inicial.

Para contornar este problema, você pode usar um arquivo Kickstart durante a instalação e incluir uma seção **`%post`** para desabilitar a versão da Configuração Inicial que você não deseja executar.

Para garantir que a variante gráfica da Configuração Inicial seja executada após a instalação, use a seguinte seção **`%post`**:

```
%post
systemctl disable initial-setup-text.service
systemctl enable initial-setup-graphical.service
%end
```

Caso deseje habilitar a variante de modo texto da Configuração Inicial, troque os comandos **`enable`** e **`disable`** para desabilitar o serviço gráfico e habilitar o modo texto.

Capítulo 37. Kernel

Alguns sistemas de arquivo ext4 não podem ser redimensionados

Devido a um erro no código de ext4, atualmente é impossível redimensionar os sistemas de arquivo ext4 que têm um tamanho de bloco de 1 quilobyte e são menores que 32 megabytes.

Perdas repetidas de conexão com os destinos iSCSI habilitados para iSER

Ao usar o servidor como um destino iSCSI habilitado para iSER, perdas de conexão ocorrem repetidamente e o destino assim como o kernel podem parar de responder. Para contornar este problema, minimize as perdas de conexão do iSER ou reverta para o modo iSCSI sem iSER.

O instalador não detecta discos Fibre Channel sobre Ethernet em sistemas EDD

Nos sistemas EDD, os discos FCoE não são detectados automaticamente pelo Anaconda devido à ausência do driver **edd**. Isto deixa esses discos não usáveis durante a instalação.

Para contornar este problema, execute os seguintes passos:

* Adicione **fcoe=edd:nodcb** à linha de comando do kernel durante a instalação, os discos FCoE serão detectados pelo anaconda.

* Adicione **fcoe=edd:nodcb** à imagem de resgate e inicialize o sistema com ele.

* Adicione o módulo edd à imagem initrd executando os seguintes comandos:

```
#dracut --regenerate-all -f

#dracut --add-drivers edd /boot/initramfs-3.10.0-123.el7.x86_64.img
```

* Reinicialize o sistema com a entrada do menu de inicialização padrão

O balanceamento NUMA não funciona da maneira ideal em certas ciscunstâncias

O balanceamento do Acesso Não Uniforme à Memória (NUMA) do Kernel do Linux não funciona de forma ideal sob a seguinte condição no Red Hat Enterprise Linux 7: quando a opção **numa_balancing** é definida, algumas das memórias podem mover-se a um nó arbitrário sem destino antes de moverem-se a nós restritos e a memória no nó de destino também diminui sob algumas circunstâncias. No momento, não há nenhuma solução alternativa disponível.

PSM2 MTL está desabilitada para evitar conflitos entre PSM e PSM2 APIs

O novo pacote *libpsm2* fornece a PSM2 API para uso com os dispositivos Intel Omni-Path, sobrepondo a Performance Scaled Messaging (PSM) API instalada pelo pacote *infinipath-psm* para uso com os dispositivos Truescale. A sobreposição da API gera um comportamento indefinido quando um processo conecta-se a bibliotecas fornecidas por ambos pacotes. Este problema afeta **Open MPI**, caso o conjunto de seus módulos MCA habilitados inclua a Matching Transport Layer (MTL) **psm2** e um ou mais módulos que diretamente ou indiretamente dependem da biblioteca **libpsm_infinipath.so.1** do pacote *infinipath-psm*.

Para evitar o conflito entre PSM e PSM2 API, a MTL **psm2** do Open MPI foi desabilitada por padrão no arquivo de configuração **/etc/openmpi-*/openmpi-mca-params.conf**. Se você habilitá-la, você precisará desabilitar as MTLs **ofi** e **psm** e a Byte Transfer Layer (BTL) **usnic** que entra em conflito com ela (mais instruções são fornecidas nos comentários no arquivo de configuração).

Há também um conflito de pacote entre os pacotes *libpsm2-compat-devel* e *infinipath-psm-devel*, pois ambos contêm arquivos de cabeçalho PSM. Portanto, os dois pacotes não podem ser instalados ao mesmo tempo. Para instalar um, desinstale o outro.

Problema com o desempenho do utilitário perf

O comando **perf archive**, que cria arquivos com arquivos de objeto com IDs de compilação localizadas nos arquivos **perf.data**, leva bastante tempo para ser concluído no IBM System z. Atualmente, não existe uma solução alternativa. Outras arquiteturas não são afetadas.

Ocorrem falhas de dependência no qlcnic mediante vinculação

Alguns modos de vinculação definem um endereço MAC no dispositivo que o driver qlcnic não reconhece adequadamente. Isto impede o dispositivo de restaurar seu endereço MAC original quando ele é removido da vinculação.

Como uma solução alternativa, retire a dependência do driver qlcnic e reinicialize o seu sistema operacional.

Ocorrem falhas na instalação em alguns computadores 64-bit da Applied Micro

O Red Hat Enterprise Linux 7.2 falha durante a instalação em certos sistemas 64-bit ARM da Applied Micro com a seguinte mensagem de erro:

```
Unable to handle kernel NULL pointer dereference at virtual address 0000033f
```

Atualmente, não há uma solução alternativa para este problema.

O gerenciamento `libvirt` de dispositivos VFIO pode gerar falhas no host

O gerenciamento **libvirt** de dispositivos PCI do host, atribuído a máquinas virtuais usando o driver VFIO, pode fazer com que os drivers do kernel do host e o driver vfio-pci associem-se simultaneamente no mesmo grupo IOMMU. Trata-se de um estado inválido, que pode gerar o encerramento inesperado do host.

Por enquanto, a única solução alternativa é nunca desconectar automaticamente um dispositivo VFIO de uma máquina virtual, caso hajam outros dispositivos no mesmo grupo IOMMU.

Instalação usando interrupções de iSCSI e IPv6 por 15 minutos

Dracut atinge tempo limite depois de tentar conectar-se com o servidor iSCSI especificado por 15 minutos, se o IPv6 estiver habilitado. Evetualmente, Dracut consegue conectar-se e proceder como esperado; no entanto, para evitar o atraso, use **ip=eth0:auto6** na linha de comando do instalador.

Travamento de i40e NIC

Em firmware mais antigos, a placa de rede usando o driver i40e torna-se inutilizável por cerca de dez segundos depois de entrar no modo promíscuo. Para evitar este problema, atualize o firmware.

i40e emite WARN_ON

O driver i40e emite o macro WARN_ON durante as alterações do tamanho de anéis, já que o código clona o struct rx_ring, mas sem zerar os ponteiros antes de alocar nova memória. Observe que este aviso é inofensivo ao seu sistema.

netprio_cgroups não é montado durante inicialização

Atualmente, systemd monta o diretório /sys/fs/cgroup/ como somente leitura, o que impede a montagem padrão do diretório /sys/fs/cgroup/net_prio/. Como resultado, o módulo netprio_cgroups não é montado durante inicialização. Para contornar este problema, use o comando **`mount -o remount`**, seguido por **`rw -t cgroup nodev /sys/fs/cgroups`**. Isto possibilita a instalação manual do cgroups baseado em módulos.

Capítulo 38. Sistema de Rede

A política de tempo limite está desabilitada no kernel do Red Hat Enterprise Linux 7.2

O comando **`nfct timeout`** não possui suporte no Red Hat Enterprise Linux 7.2. Como uma solução alternativa, utilize os valores globais de tempo limite disponíveis em **`/proc/sys/net/netfilter/nf_conntrack_*_timeout_*`** para definir o valor do tempo limite.

Capítulo 39. Armazenamento

Nenhum suporte para o provisionamento dinâmico em cima do RAID em um cluster

Apesar dos volumes lógicos do RAID e dos volumes lógicos com provisionamento dinâmico poderem ser usados em um cluster quando ativados exclusivamente, não há atualmente nenhum suporte para o provisionamento dinâmico em cima do RAID em um cluster. Isto acontece mesmo quando a combinação é ativada exclusivamente. Atualmente, esta combinação possui suporte apenas no modo não clusterizado de uma única máquina do LVM.

Ao usar o provisionamento dinâmico, é possível perder gravações em buffer para o pool dinâmico, caso ele atinja a sua capacidade máxima

Caso um pool dinâmico atinja a sua capacidade, é possível que ele perda algumas gravações, mesmo que o pool esteja em crescimento naquele momento. Isto acontece porque uma operação de redimensionamento (mesmo uma automatizada) tenta descarregar E/S pendente no dispositivo de armazenamento antes do redimensionamento ser desempenhado. Já que não há espaço no pool dinâmico, as operações E/S devem obter erro primeiro para permitir que o crescimento seja bem sucedido. Depois que o pool dinâmico tiver crescido, os volumes lógicos associados ao pool dinâmico retornarão às operações normais.

Como uma solução alternativa para este problema, defina 'thin_pool_autoextend_threshold' e 'thin_pool_autoextend_percent' de acordo com suas necessidades no arquivo lvm.conf. Não deixe o limite muito alto ou a porcentagem muito baixa de modo que o seu pool dinâmico atinja a capacidade máxima rapidamente e não tenha tempo suficiente para estender-se automaticamente (ou para ser manulamente estendido, caso você prefira assim). Se você não estiver usando o provisionamento além do necessário (criando volumes lógicos maiores que o tamanho do pool dinâmico de apoio), prepare-se para remover os snapshots, conforme necessário, caso o pool dinâmico comece a atingir a sua capacidade.

Capítulo 40. Gerenciamento do Sistema e Subscrições

O botão `Voltar` (Back) não funciona no complemento para o Gerenciador de Subscrição na Configuração Inicial

O botão **`Voltar`** (Back) no primeiro painel do complemento para o Gerenciador de Subscrição no utilitário da Configuração Inicial não funciona. Para contornar este problema, clique em **`Concluído`** (Done) na parte superior da Configuração Inicial para sair do fluxo de trabalho de registro.

Falha no virt-who ao alterar a associação host-to-guest para o servidor Candlepin

Ao adicionar, remover, migrar um guest, o utilitário virt-who atualmente falha ao enviar o mapeamento host-to-guest e imprime um erro RateLimitExceededException no arquivo de log. Para contornar este problema, defina o parâmetro **`VIRTWHO_INTERVAL=`** no arquivo /etc/sysconfig/virt-who com um número maior, como 600. Isto permite que o mapeamento seja alterado corretamente, mas gera alterações no mapeamento host-to-guest que levam um tempo bem maior para serem processadas.

Capítulo 41. Virtualização

Problemas na navegação GRUB 2 com KVM

A utilização do console serial via KVM, pressionando uma tecla de direção por um longo período de tempo para navegar no menu GRUB 2, resulta em comportamentos erráticos. Para contornar este problema, evite a entrada rápida ao pressionar a tecla de direção por um tempo mais longo.

O redimensionamento dos discos da Tabela de Partição GUID (GPT) nas máquinas virtuais do Hyper-V gera erros na tabela de partição

O gerenciador Hyper-V oferece suporte à redução de um disco GPT particionado em uma máquina virtual se houver espaço livre após a última partição, permitindo ao usuário descartar a última parte não usada do disco. No entanto, esta operação removerá silenciosamente o cabeçalho GPT de backup no disco, o que pode provocar mensagens de erro quando a máquina virtual examinar a tabela de partição (por exemplo, com parted(8)). Esta é uma limitação conhecida do Hyper-V.

Para contornar este problema, é possível restaurar manualmente o cabeçalho GPT de backup com o comando expert do gdisk(8) **e**, após a redução do disco GPT. Isto também acontece com o uso da opção Expandir (Expand) do Hyper-V, mas também pode ser corrigido com a ferramenta parted(8).

Falha na criação de ponte com `virsh iface-bridge`

Ao instalar o Red Hat Enterprise Linux 7 a partir de outras fontes, e não da rede, os nomes dos dispositivos de rede não são especificados por padrão nos arquivos de configuração da interface (isto é feito com a linha **`DEVICE=`**). Como consequência, a criação de uma ponte de rede usando o comando**`virsh iface-bridge`** falha com uma mensagem de erro. Para contornar este problema, adicione as linhas **`DEVICE=`** nos arquivos /etc/sysconfig/network-scripts/ifcfg-*.

Cartões inteligentes CAC emulados com QEMU são incompatíveis com o software ActivClient

Atualmente, os cartões inteligentes Common Access Card (CAC) emulados com QEMU não são aceitos pelo software ActivClient. Para contornar este problema, desabilite o daemon pcscd, provisione uma máquina virtual KVM, pré-configure-a na ferramenta virt-viewer, selecione a opção de redirecionamento de USB, instale o software ActivClient e reinicialize a máquina virtual KVM. Com esta configuração, o ActivClient aceita o cartão CAC emulado.

Arquivos VFD no virtio-win não contêm drivers para o Windows 10

Devido às limitações no tamanho dos arquivos do disquete, os arquivos VFD (disquete virtual) nos pacotes virtio-win não contêm uma pasta do Windows 10. Se o usuário precisar instalar drivers para o Windows 10 de um VFD, ele pode utilizar os drivers para o Windows 8 ou Windows 8.1. Caso contrário, os drivers para o Windows 10 podem ser instalados do arquivo ISO no diretório /usr/share/virtio-win/.

As máquinas virtuais migradas não exibem o menu de inicialização no console serial

As máquinas virtuais (MVs) criadas no Red Hat Enterprise Linux 6 que não possuem placa gráfica (como as MVs criadas usando o utilitário virt-install com a opção **`--graphics none`**) não exibem o menu de inicialização no console serial mais, após a migração para os hosts Red Hat Enterprise Linux 7. Para contornar este problema, adicione a linha <bios useserial='yes'/> ao arquivo domain.xml, o que permitirá que o menu de inicilização seja exibido como esperado.

Observe que, se o arquivo XML é modificado como indicado, ele não deve ser usado no Red Hat Enterprise Linux 6.6 ou em versões mais antigas, já que não se beneficiam das alterações introduzidas para BZ#1162759.

Capítulo 42. Atomic Host e Contêineres

A instalação do Atomic Host oferece cryptsetup, embora não esteja disponível

Durante a instalação do Red Hat Enterprise Linux 7 Atomic Host, o instalador oferece a opção de criptografar partições usando **`cryptsetup`** na tela de Particionamento Manual, da mesma forma que oferece durante a instalação do Red Hat Enterprise Linux 7.2.

No entanto, as partições criptografadas não possuem suporte no Atomic Host. Se você criptografar qualquer partição durante a instalação, não conseguirá desbloqueá-la depois.

Para contornar este probema, não criptografe partições ou volumes lógicos durante a instalação do Red Hat Enterprise Linux Atomic Host, mesmo que o instalador apresente esta opção.

O instalador pode adicionar o armazenamento avançado apenas na primeira vez que o usuário entrar na tela de configuração do armazenamento

Durante uma instalação interativa que utiliza a interface gráfica do Anaconda, a adição do armazenamento avançado (iSCSI, zFCP, FCoE) à sua seleção de disco não funcionará se você já tiver entrado e saído da tela de configuração do armazenamento. Para contornar este problema, certifique-se, se necessário, de que a rede esteja ativa e, depois, entre na tela de configuração do armazenamento e adicione todos os dispositivos de armazenamento avançado.

A instalação do Atomic Host oferece BTRFS, mas não possui suporte

O instalador do Red Hat Enterprise Linux Atomic Host oferece BTRFS como uma opção de partição, mas a árvore não inclui btrfs-progs. Como consequência, um sistema Atomic Host com particionamento BTRFS não funcionará, mesmo que a opção esteja presente no instalador. Não selecione esta opção no instalador. O BTRFS não possui suporte para o Atomic Host.

ostreesetup nos arquivos Kickstart fornece suporte apenas a HTTP e HTTPS

O comando **`ostreesetup`** no Kickstart do Atomic Host fornece suporte apenas a Identificadores de Recursos Uniformes (URIs) HTTP e HTTPS. O fornecimento de uma opção diferente, como, por exemplo, **`ftp://`**, pode gerar falhas no instalador. Use somente HTTP e HTTPS.

O Red Hat Enterprise Linux Atomic Hostfornece suporte somente à localidade en_US.UTF-8

Durante a instalação, se você selecionar um idioma diferente do Inglês Americano, como o tipo de teclado padrão, esta escolha não refletirá no sistema instalado depois. A localidade ainda estará definida como **`en_US`** e as mensagens de erro sobre as localidades ausentes serão exibidas. Isto pode ser problemático para programas que requerem outras localidades ou, por exemplo, quando se tem uma senha em outro idioma e o sistema não a reconhece.

Quando a partição root está sem espaço livre

O Red Hat Enterprise Linux Atomic Host aloca 3GB de armazenamento para a partição root, incluindo os volumes do docker (unidades de armazenamento que um contêiner em execução pode solicitar do sistema host). Isto acaba gerando a falta de espaço de armazenamento na partição root. Para obter suporte para mais espaço de volume, mais armazenamento físico deve ser adicionado ao sistema ou o Volume Lógico root deve ser estendido.

Por padrão, 40% do outro volume fica reservado para o armazenamento de imagens de contêiner. Os outros 60% podem ser usados para estender a partição root. Para instruções mais detalhadas, consulte https://access.redhat.com/documentation/en/red-hat-enterprise-linux-atomic-host/version-7/getting-started-with-containers/#changing_the_size_of_the_root_partition_after_installation.

O modo de resgate não funciona no Red Hat Enterprise Linux Atomic Host

O instalador do Anaconda não é capaz de localizar um sistema Atomic Host instalado previamente quando em modo de resgate. Portanto, o modo de resgate não funciona e não deve ser usado.

O daemon docker é incapaz de criar um despejo de memória

No Red Hat Enterprise Linux Atomic Host, o padrão principal é definido como **`core`**. Isto impede a gravação de despejos de memória para daemons como o docker, cujo diretório é **`root`** (**`/`**), já que é somente para leitura. Para contornar o problema, especifique um padrão de nome de arquivo principal que aponte para uma localização gravável:

```
echo /var/lib/core > /proc/sys/kernel/core_pattern
```

Com esta solução alternativa, os despejos de memória serão salvos sob **`/var/lib`**.

O serviço `brandbot.path` pode fazer com que o subscription-manager altere o arquivo /etc/os-release nas instalações 7.1

O arquivo **`/etc/os-release`** ainda pode especificar a versão 7.1, mesmo depois que o Atomic Host tenha recebido upgrade para 7.2, usando o comando **`atomic host upgrade`**. Isto acontece porque a ferramenta ostree subjacente preserva os arquivos modificados em **`/etc`**. Como uma solução alternativa, depois do upgrade para a versão 7.2, execute o seguinte comando: **`cp /usr/etc/os-release /etc`**. Desta maneira, o arquivo **`/etc/os-release`** retornará em um estado não modificado e, já que *brandbot.path* é mascarado em 7.2.0, ele não será modificado no futuro pelo subscription-manager e os upgrades futuros exibirão a versão correta.

Apêndice A. Versões dos Componentes

Este apêndice contém uma lista dos componentes e suas versões no lançamento do Red Hat Enterprise Linux 7.2

Tabela A.1. Versões dos Componentes

Componente	Versão
Kernel	3.10.0-327
Driver QLogic **`qla2xxx`**	8.07.00.08.07.2-k
Driver QLogic **`qla4xxx`**	5.04.00.00.07.02-k0
Driver Emulex **`lpfc`**	0:10.7.0.1
Utilitários do iniciador iSCSI	*iscsi-initiator-utils-6.2.0.873-32*
DM-Multipath	*device-mapper-multipath-0.4.9-85*
LVM	*lvm2-2.02.130-5*

Apêndice B. Histórico de Revisões

Revisão 0.0-1.37.2 **Wed Jul 13 2016** **maria suppes de andrada**

pt-BR translation completed

Revisão 0.0-1.37.1 **Wed Jul 13 2016** **maria suppes de andrada**

Tradução de arquivos sincronizados com a versão 0.0-1.37 de fontes do XML

Revisão 0.0-1.37 **Thu May 12 2016** **Lenka Špačková**

Atualização do capítulo Atomic Host e Contêineres com o lançamento do Red Hat Enterprise Linux Atomic Host 7.2.4; duas versões do serviço docker estão agora disponíveis.

Revisão 0.0-1.36 **Thu Apr 21 2016** **Lenka Špačková**

Atualização do capítulo Atomic Host e Contêineres; nomes de contêineres adicionados.

Revisão 0.0-1.35 **Wed Apr 13 2016** **Lenka Špačková**

Mudança do utilitário **kpatch** das Apresentações Prévias de Tecnologia para Novos Recursos com suporte consulte os detalhes em Capítulo 10, *Kernel*.

Revisão 0.0-1.34 **Thu Mar 31 2016** **Lenka Špačková**

Atualização do capítulo Atomic Host e Contêineres com o lançamento do Red Hat Enterprise Linux Atomic Host 7.2.3.

Revisão 0.0-1.33 **Mon Mar 28 2016** **Lenka Špačková**

Atualização de Funcionalidades Preteridas, Apresentação Prévia de Tecnologia (clufter) e Novos Recursos (winbindd).

Revisão 0.0-1.32 **Mon Feb 29 2016** **Lenka Špačková**

Informação removida sobre o subcomando **`atomic host deploy`** que ainda não está disponível.

Revisão 0.0-1.31 **Tue Feb 23 2016** **Lenka Špačková**

Atualização do capítulo Atomic Host e Contêineres com informações sobre a retirada do suporte para a API v1beta3.

Revisão 0.0-1.30 **Tue Feb 16 2016** **Lenka Špačková**

Atualização do capítulo Atomic Host e Contêineres com o lançamento do Red Hat Enterprise Linux Atomic Host 7.2.2.

Revisão 0.0-1.29 **Thu Feb 11 2016** **Lenka Špačková**

Correção da descrição do recurso RoCE Express para a Apresentação de Tecnologia RDMA.

Revisão 0.0-1.28 **Tue Jan 26 2016** **Lenka Špačková**

Informação incorreta sobre o aplicativo **Photos** removida de Novos Recursos (Desktop).

Revisão 0.0-1.27 **Tue Jan 19 2016** **Lenka Špačková**

Adição de problema conhecido (Instalação e Inicialização).

Revisão 0.0-1.26 **Wed Jan 13 2016** **Lenka Špačková**

Adição de correção de erro em relação a RMRR (Virtualização).

Revisão 0.0-1.25 **Thu Dec 10 2015** **Lenka Špačková**

Adição de problema conhecido (Instalação e Inicialização).

Revisão 0.0-1.22 **Wed Dec 02 2015** **Lenka Špačková**

Adição de vários problemas conhecidos (Virtualização, Autenticação).

Revisão 0.0-1.21 **Thu Nov 19 2015** **Lenka Špačková**

Lançamento das Notas de Lançamento do Red Hat Enterprise Linux 7.2.

Revisão 0.0-1.4 **Mon Aug 31 2015** **Laura Bailey**

Lançamento das Notas de Lançamento Red Hat Enterprise Linux 7.2 Beta.