Red Hat Enterprise Linux 8

8.1 릴리스 노트

Red Hat Enterprise Linux 8.1 릴리스 정보

Last Updated: 2024-04-06

Red Hat Enterprise Linux 8 8.1 릴리스 노트

Red Hat Enterprise Linux 8.1 릴리스 정보

법적 공지

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

초록

릴리스 노트에서는 Red Hat Enterprise Linux 8.1에서 구현된 개선 사항 및 추가 사항에 대해 개략적으로 설명하고 이 릴리스의 알려진 문제점과 주요 버그 수정, 기술 프리뷰, 사용되지 않는 기능 및 기타 세부 정보를 문서화합니다.

차례

RED HAT 문서에 관한 피드백 제공 3

1장. 개요 4
- 설치 프로그램 및 이미지 생성 4
- Red Hat Enterprise Linux 시스템 역할 4
- 인프라 서비스 4
- 보안 4
- 커널 4
- 파일 시스템 및 스토리지 4
- 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버 5
- 컴파일러 툴 세트 5
- IdM (Identity Management) 5
- 데스크탑 5
- RHEL 7에서 RHEL 8으로의 즉각적 업그레이드 5
- 추가 리소스 6

2장. 아키텍처 7

3장. 외부 커널 매개 변수로의 중요한 변경 8
- 새 커널 매개변수 8
- 업데이트된 커널 매개변수 10
- 새로운 /proc/sys/kernel 매개변수 11
- 새로운 /proc/sys/net 매개변수 11
- 업데이트된 /proc/sys/fs 매개변수 11
- 업데이트된 /proc/sys/kernel 매개변수 11

4장. RHEL 8의 콘텐츠 배포 13
- 4.1. 설치 13
- 4.2. 리포지토리 13
- 4.3. APPLICATION STREAMS 13
- 4.4. YUM/DNF를 사용한 패키지 관리 14

5장. RHEL 8.1.1 릴리스 15
- 5.1. 새로운 기능 15

6장. RHEL 8.1.0 릴리스 18
- 6.1. 새로운 기능 18
- 6.2. 새 드라이버 51
- 6.3. 업데이트된 드라이버 54
- 6.4. 버그 수정 56
- 6.5. 기술 프리뷰 74
- 6.6. 사용되지 않는 기능 91
- 6.7. 확인된 문제 99

7장. 컨테이너 관련 주요 변경 사항 131

8장. 국제화 133
- 8.1. RED HAT ENTERPRISE LINUX 8 국제 언어 133
- 8.2. RHEL 8 국제화의 주요 변경 사항 134

부록 A. 구성 요소별 티켓 목록 135

부록 B. 개정 내역 141

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. 문서를 개선하는 방법을 알려주십시오. 이를 위해 다음을 수행합니다.

Jira를 통해 피드백 제출 (등록 필요)

1. Jira 웹 사이트에 로그인합니다.
2. 상단 탐색 모음에서 **생성** 을 클릭합니다.
3. **요약** 필드에 설명 제목을 입력합니다.
4. **설명** 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

1장. 개요

설치 프로그램 및 이미지 생성

이제 사용자는 Kickstart 설치 중에 모듈을 비활성화할 수 있습니다.

자세한 내용은 6.1.1절. "설치 프로그램 및 이미지 생성"을 참조하십시오.

Red Hat Enterprise Linux 시스템 역할

새 **스토리지** 역할이 RHEL 시스템 역할에 추가되었습니다.

자세한 내용은 6.1.17절. "Red Hat Enterprise Linux 시스템 역할" 을 참조하십시오.

인프라 서비스

RHEL 8.1에는 이전 버전의 RHEL에서 사용된 **Quagga** 를 대체하는 새로운 라우팅 프로토콜 스택 GA가 도입되었습니다. **pvcR** 은 여러 IPv4 및 IPv6 라우팅 프로토콜을 지원하는 TCP/IP 기반 라우팅 서비스를 제공합니다.

Tuned 시스템 튜닝 툴은 버전 2.12로 업데이트되어 CPU 목록 부정에 대한 지원이 추가되었습니다.

chrony 제품군은 버전 3.5로 다시 기반하여 RHEL 8.1 커널의 하드웨어 타임스탬프를 사용하여 시스템 클럭의 보다 정확한 동기화를 지원합니다.

자세한 내용은 6.1.4절. "인프라 서비스"의 내용을 참조하십시오.

보안

RHEL 8.1에는 컨테이너에 대한 SELinux 정책을 생성하는 새로운 도구가 도입되었습니다. **udica**. 오디 **카를 사용하면** 컨테이너에서 스토리지, 장치 및 네트워크와 같은 호스트 시스템 리소스에 액세스하는 방법을 보다 효과적으로 제어하기 위한 맞춤형 보안 정책을 만들 수 있습니다. 이를 통해 보안 위반에 대해 컨테이너 배포를 강화할 수 있으며 규정 준수의 달성 및 유지를 단순화할 수 있습니다.

fapolicyd 소프트웨어 프레임워크에는 사용자 정의 정책에 따라 애플리케이션 화이트리스트 및 블랙리스트 형식이 도입되었습니다. RHEL 8.1 애플리케이션 화이트리스트 기능은 시스템에서 신뢰할 수 없고 악의적인 애플리케이션 실행을 방지하는 가장 효율적인 방법 중 하나를 제공합니다.

보안 규정 준수 제품군인 **OpenSCAP** 은 이제 SCAP 1.3 데이터 스트림을 지원하고 향상된 보고서를 제공합니다.

자세한 내용은 6.1.5절. "보안"를 참조하십시오.

커널

커널 **kpatch** 에 대한 실시간 패치를 사용할 수 있으므로 시스템을 재부팅할 필요 없이 심각 및 중요한 CVE 수정을 사용할 수 있습니다.

eBPF(Extended Berkeley Packet Filter)는 커널 공간에서 코드를 실행할 수 있는 커널 내 가상 시스템입니다. **eBPF** 는 RHEL의 여러 구성 요소에서 사용합니다. RHEL 8.1에서는 **BCC(BPF Compiler Collection)** 툴 패키지가 AMD 및 Intel 64비트 아키텍처에서 완전히 지원되며 다른 아키텍처에서 기술 프리뷰로 사용할 수 있습니다. 또한 **bpftrace** 추적 언어 및 **eXpress Data Path(XDP)** 기능은 기술 프리뷰로 사용할 수 있습니다.

자세한 내용은 6.1.7절. "커널" 및 6.5.2절. "커널"을 참조하십시오.

파일 시스템 및 스토리지

LUKS 버전 2(**LUKS2) 형식은**이제 장치가 사용 중인 동안 블록 장치를 재암호화하는 기능을 지원합니다.

자세한 내용은 6.1.9절. "파일 시스템 및 스토리지"를 참조하십시오.

동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

다음 구성 요소의 최신 버전을 새 모듈 스트림으로 사용할 수 있습니다.

- **PHP 7.3**
- **Ruby 2.6**
- **Node.js 12**
- **nginx 1.16**

자세한 내용은 6.1.11절. "동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버" 을 참조하십시오.

컴파일러 툴 세트

RHEL 8.1에는 최신 버전의 개발 툴을 제공하는 Software Collection으로 패키징된 애플리케이션 스트림인 **GCC Toolset 9** 라는 새로운 컴파일러 툴셋이 도입되었습니다.

또한 다음과 같은 컴파일러 툴 세트가 업그레이드되었습니다.

- **LLVM 8.0.1**
- **히스토리 툴 세트 1.37**
- **Go Toolset 1.12.8**

자세한 내용은 6.1.12절. "컴파일러 및 개발 도구"를 참조하십시오.

IdM (Identity Management)

ID 관리에는 새로운 명령줄 도구인 **Healthcheck** 가 도입되었습니다. **Healthcheck** 는 사용자가 IdM 환경의 환경에 영향을 줄 수 있는 문제를 찾는 데 도움이 됩니다.

자세한 내용은 6.1.13절. "IdM (Identity Management)" 을 참조하십시오.

Identity Management에서는 설치 및 관리를 위한 Ansible 역할 및 모듈을 지원합니다. 이번 업데이트를 통해 IdM 기반 솔루션을 쉽게 설치하고 구성할 수 있습니다.

자세한 내용은 6.1.13절. "IdM (Identity Management)" 를 참조하십시오.

데스크탑

GNOME Classic 환경의 작업 공간 전환기가 수정되었습니다. 스위터는 이제 아래쪽 막대의 오른쪽 부분에 위치하며 수평면 패널로 설계되었습니다. 필요한 축소판 이미지를 클릭하면 작업 영역 간 전환이 가능합니다. 자세한 내용은 6.1.14절. "데스크탑" 을 참조하십시오.

DRM (**Direct Rendering Manager**) 커널 그래픽 하위 시스템은 업스트림 Linux 커널 버전 5.1로 업데이트되었습니다. 이 버전은 새 GPU 및 APU에 대한 지원과 다양한 드라이버 업데이트를 포함하여 이전 버전에 비해 여러 가지 개선 사항을 제공합니다. 자세한 내용은 6.1.14절. "데스크탑"을 참조하십시오.

RHEL 7에서 RHEL 8으로의 즉각적 업그레이드

다음과 같은 주요 개선 사항이 도입되었습니다.

- 다음 아키텍처에 대한 즉각적 업그레이드 지원이 추가되었습니다. 64비트 ARM, IBM POWER(Lttle endian), IBM Z.
- 이제 웹 콘솔에서 사전 업그레이드 시스템 평가를 수행하고 새 **cockpit-leapp** 플러그인을 사용하여 자동화된 수정을 적용할 수 있습니다.
- **/var** 또는 **/usr** 디렉토리를 별도의 파티션에 마운트할 수 있습니다.

- UEFI가 지원됩니다.
- **LeApp은** 이제 보조 리포지토리에서 패키지를 업그레이드합니다.

지원되는 업그레이드 경로에 대한 자세한 내용은 Red Hat Enterprise Linux에 대한 지원 내부 업그레이드 경로를 참조하십시오. 즉각적 업그레이드를 수행하는 방법에 대한 지침은 RHEL 7에서 RHEL 8로 업그레이드를 참조하십시오.

CentOS Linux 7 또는 Oracle Linux 7을 사용하는 경우 RHEL 8로 업그레이드하기 전에 **convert2rhel** 유틸리티를 사용하여 운영 체제를 RHEL 7로 변환할 수 있습니다. 자세한 내용은 RPM 기반 Linux 배포판에서 RHEL로 변환을 참조하십시오.

추가 리소스

- Red Hat Enterprise Linux 8의 **기능 및 제한사항** 과 다른 시스템 버전과의 비교는 지식베이스 문서 Red Hat Enterprise Linux 기술 기능 및 제한사항 에서 확인할 수 있습니다.
- Red Hat Enterprise Linux **라이프사이클에** 대한 정보는 Red Hat Enterprise Linux 라이프 사이클 문서를 참조하십시오.
- 패키지 매니페스트 문서는 RHEL 8의 **패키지 목록을** 제공합니다.
- **RHEL 7과 RHEL 8의 주요 차이점은 RHEL 8** 채택을 고려한 것으로 설명되어 있습니다.
- RHEL 7 **에서 RHEL 8로 즉각적 업그레이드를 수행하는 방법에 대한 지침은 RHEL 7**에서 RHEL 8로 업그레이드 문서에서 제공합니다.
- 알려진 기술 문제를 사전에 식별, 검사 및 해결할 수 있는 **Red Hat Insights** 서비스는 이제 모든 RHEL 서브스크립션을 통해 사용할 수 있습니다. Red Hat Insights 클라이언트를 설치하고 시스템을 서비스에 등록하는 방법에 대한 지침은 Red Hat Insights 시작하기 페이지를 참조하십시오.

Red Hat Customer Portal 랩

Red Hat 고객 포털 랩은 고객 포털의 섹션에서 https://access.redhat.com/labs/ 사용할 수 있는 일련의 툴입니다. Red Hat 고객 포털 랩의 애플리케이션은 성능을 개선하고 문제를 신속하게 해결하며 보안 문제를 식별하며 복잡한 애플리케이션을 신속하게 배포하고 구성할 수 있도록 지원합니다. 가장 많이 사용되는 애플리케이션 중 일부는 다음과 같습니다.

- 등록 도우미
- 제품 라이프 사이클 검사기
- 킥스타트 생성기
- Red Hat Satellite Upgrade Helper
- Red Hat 코드 브라우저
- JVM 옵션 구성 도구
- Red Hat CVE 검사기
- Red Hat 제품 인증서
- 로드 밸런서 설정 도구
- yum 리포지토리 설정 도우미

2장. 아키텍처

Red Hat Enterprise Linux 8.1은 다음 아키텍처를 지원하는 커널 버전 4.18.0-147과 함께 배포됩니다.

- AMD 및 Intel 64비트 아키텍처
- 64비트 ARM 아키텍처
- IBM Power Systems, Little Endian
- 64-bit IBM Z

각 아키텍처에 적합한 서브스크립션을 구매해야 합니다. 자세한 내용은 Red Hat Enterprise Linux - 추가 아키텍처 시작하기 를 참조하십시오. 사용 가능한 서브스크립션 목록은 고객 포털의 서브스크립션 사용률 을 참조하십시오.

3장. 외부 커널 매개 변수로의 중요한 변경

이 장에서는 시스템 관리자에게 Red Hat Enterprise Linux 8.1과 함께 제공되는 커널의 중요한 변경 사항을 요약해서 설명합니다. 이러한 변경 사항에는 **proc** 항목, **sysctl** 및 **sysfs** 기본값, 부팅 매개 변수, 커널 구성 옵션 또는 눈에 보이는 동작 변경이 포함됩니다.

새 커널 매개변수

perf_v4_pmi = [X86,INTEL]

이 매개 변수는 Intel PMU 카운터 정지 기능을 비활성화합니다.
이 기능은 Arch Perfmon v4(Skylake 이상)부터 시작됩니다.

형식: <bool>

hv_nopvspin [X86,HYPER_V]

이 매개변수는 반가상 스핀락 최적화를 비활성화하여 하이퍼바이저가 잠금 경합 시 게스트를 'idle'할 수 있도록 합니다.

ipcmni_extend [KNL]

이 매개 변수는 고유한 System V IPC 식별자의 최대 수를 32,768에서 16,777,216으로 확장합니다.

kpti = [ARM64]

이 매개 변수는 사용자 및 커널 주소 공간의 페이지 테이블 격리를 제어합니다.
옵션은 다음과 같습니다.

- **default**: 완화가 필요한 코어에서 활성화됩니다.
- **0**: 강제 비활성화
- **1**: 강제로 활성화

mds = [X86,INTEL]

이 매개변수는 MDS(Micro-architectural Data Sampling) 취약점에 대한 완화 기능을 제어합니다.
특정 CPU는 특정 조건에서 공개 가젯으로 정보를 전달할 수 있는 CPU 내부 버퍼에 대한 위협에 취약합니다. 취약한 프로세서에서 예측 가능한 전달된 데이터를 캐시 사이드 채널 공격에 사용하여 공격자가 직접 액세스할 수 없는 데이터에 액세스할 수 있습니다.

옵션은 다음과 같습니다.

- **full** - 취약한 CPU에서 MDS 완화를 활성화합니다.
- **full, nosmt** - MDS 완화를 활성화하고 취약한 CPU에서 SMT(Simultaneous Multi Threading)를 비활성화합니다.
- **off** - MDS 완화를 무조건 비활성화합니다.
  이 매개 변수를 지정하지 않는 것은 **mds=full** 과 동일합니다.

  자세한 내용은 업스트림 커널 설명서를 참조하십시오.

완화 = [X86,PPC, S390,ARM64]

이 매개변수는 CPU 취약점에 대한 선택적 완화 조치를 제어합니다. 이는 각각 기존 아카이브별 옵션의 집계인 선별된 아치 독립적인 옵션 집합입니다.
옵션은 다음과 같습니다.

- **off** - 모든 선택적 CPU 완화를 비활성화합니다. 이로 인해 시스템 성능이 향상되지만 여러 CPU 취약점에 사용자가 노출될 수도 있습니다.
  다음과 같습니다.
  - **nopti [X86,PPC]**
  - **kpti=0 [ARM64]**
  - **nospectre_v1 [X86,PPC]**
  - **nobp=0 [S390]**
  - **nospectre_v2 [X86,PPC,S390,ARM64]**
  - **spectre_v2_user=off [X86]**
  - **spec_store_bypass_disable=off [X86,PPC]**
  - **ssbd=force-off [ARM64]**
  - **l1tf=off [X86]**
  - **mds=off [X86]**
- **auto** (기본값) - 모든 CPU 취약점을 완화하지만 보안 취약점이 취약하더라도 SMT(Simultaneous Multi Threading)를 사용하도록 둡니다. 이 옵션은 SMT가 커널 업그레이드에서 비활성화되거나 SMT 기반 공격을 방지할 수 있는 다른 방법을 가지고 있기 때문에 놀랄 필요가 없는 사용자를 위한 것입니다.
  다음과 같습니다.
  - (기본 동작)
- **auto,nosmt** - 모든 CPU 취약점을 완화하여 필요한 경우 SMT(동시 멀티 스레드)를 비활성화합니다. 이 옵션은 SMT를 손실하는 것을 의미하더라도 항상 완전히 완화하려는 사용자를 위한 것입니다.
  다음과 같습니다.
  - **l1tf=flush,nosmt [X86]**
  - **mds=full,nosmt [X86]**

novmcoredd [KNL,KDUMP]

이 매개 변수는 장치 덤프를 비활성화합니다.
장치 덤프를 사용하면 드라이버가 vmcore에 덤프 데이터를 추가할 수 있으므로 드라이버가 지정된 디버그 정보를 수집할 수 있습니다. 드라이버는 제한 없이 데이터를 추가할 수 있으며 이 데이터는 메모리에 저장되므로 메모리에 상당한 메모리 부하가 발생할 수 있습니다.

장치 덤프를 비활성화하면 메모리를 절약하는 데 도움이 될 수 있지만 드라이버 디버그 데이터를 더 이상 사용할 수 없습니다.

이 매개변수는 **CONFIG_PROC_VMCORE_DEVICE_DUMP** 커널 구성이 설정된 경우에만 사용할 수 있습니다.

nospectre_v1 [X86]

이 매개변수는 Spectre Variant 1의 완화 기능을 비활성화합니다(바운드 확인 바이패스).
이 옵션을 사용하면 시스템에서 데이터 유출이 가능합니다.

psi = [KNL]

이 매개 변수는 누수 정보 추적을 활성화하거나 비활성화합니다.
형식: <bool>

random.trust_cpu={on,off} [KNL]

이 매개변수는 CPU의 임의 번호 생성기(사용 가능한 경우) 사용을 신뢰하여 커널의 CRNG(Cryptdom Random Number Generation)을 완전히 시드할 수 있도록 활성화하거나 비활성화합니다. 기본값은 **CONFIG_RANDOM_TRUST_CPU 커널 구성에서** 제어합니다.

vm_debug[=options] [KNL]

CONFIG_DEBUG_VM=y 와 함께 사용할 수 있습니다.
이 매개 변수를 활성화하면 특히 메모리 양이 많은 시스템에서 시스템 부팅 속도가 느려질 수 있습니다.

모든 옵션은 기본적으로 활성화되며, 이 인터페이스는 특정 가상 메모리 디버깅 기능을 선택적으로 활성화하거나 비활성화할 수 있도록 합니다.

옵션은 다음과 같습니다.

- p **-** 페이지 구조 init 시간 침입을 활성화합니다.
- **-** (대시) - 위의 모든 옵션을 비활성화합니다.

업데이트된 커널 매개변수

cgroup_no_v1 = [KNL]

이 매개변수는 버전 1(v1)에서 cgroup 컨트롤러 및 명명된 계층 구조를 비활성화합니다.
매개 변수는 **cgroup_disable** 커널 매개 변수와 같지만 cgroup v1에만 적용됩니다. 블랙리스트로 지정된 컨트롤러는 cgroup2에서 계속 사용할 수 있습니다. "all" 옵션은 모든 컨트롤러를 블랙리스트로 지정하고 "named" 옵션은 명명된 마운트를 비활성화합니다. "all"과 "named"를 모두 지정하면 v1 계층 구조가 모두 비활성화됩니다.

형식: { { controller | "all" | "named" } [,{ controller | "all" | "named" }...] }

crashkernel = size[KMG][@offset[KMG]][KNL]

kexec 시스템 호출을 통해 Linux는 패닉 시 'crash kernel'으로 전환할 수 있습니다. 이 매개 변수는 해당 커널 이미지에 대해 [offset, offset + size] 물리적 메모리 영역을 예약합니다. **@offset** 을 생략하면 적합한 오프셋이 자동으로 선택됩니다.
[KNL, x86_64] 먼저 4G 아래의 지역을 선택하고 **@offset** 이 지정되지 않은 경우 4G 위의 지역을 예약하도록 대체합니다.

자세한 내용은 업스트림 kdump 문서를 참조하십시오.

l1tf = [X86]

이 매개변수는 영향을 받는 CPU에서 L1 Terminal Fault(L1TF) 취약점의 완화를 제어합니다.
옵션은 다음과 같습니다.

- **off** - 하이퍼바이저 완화 기능을 비활성화하고 경고를 보내지 않습니다. 또한 하이퍼바이저와 베어 메탈에 대해 스왑 크기 및 사용 가능한 RAM 제한 제한도 줄입니다.
- **flush** - 기본값입니다.
  자세한 내용은 업스트림 커널 설명서를 참조하십시오.

nospectre_v2 [X86,PPC_FSL_BOOK3E,ARM64]

이 매개변수는 Spectre variant 2 (indirect branch predict) 취약점에 대한 모든 완화 기능을 비활성화합니다.
시스템에서 이 매개 변수를 사용하여 데이터 누수를 허용할 수 있습니다.

pci=option[,option...] [PCI]

다양한 PCI 하위 시스템 옵션.
옵션은 다음과 같습니다.

- **force_floating** [S390] - 유동 인터럽트의 강제 사용.
- **nomio** [S390] - 메모리 입/출력(MIO) 명령을 사용하지 마십시오.

새로운 /proc/sys/kernel 매개변수

hyperv_record_panic_msg

이 매개변수는 패닉 커널 메시지(kmsg) 데이터가 Hyper-V에 보고되는지 여부를 제어합니다.
값은 다음과 같습니다.

- **0** - 패닉 kmsg 데이터를 보고하지 마십시오.
- **1** - 패닉 kmsg 데이터를 보고합니다. 기본 동작입니다.

새로운 /proc/sys/net 매개변수

bpf_jit_limit

이 매개변수는 BPF JIT(Berkeley Packet Filter Just-in-Time) 컴파일러에 대한 메모리 할당에 대한 글로벌 제한을 적용하여 권한이 없는 JIT 요청을 초과하면 해당 요청을 거부합니다.
bpf_jit_limit 매개 변수에는 전역 제한 값(바이트)이 포함되어 있습니다.

업데이트된 /proc/sys/fs 매개변수

dentry-state

dentries는 동적으로 할당되고 할당됩니다.
사용자는 **/proc/sys/fs/dentry-state** 파일을 읽고 다음 값을 검색할 수 있습니다.

- **nr_dentry** - 할당된 총 들여쓰기 수(활성 + 사용되지 않음)를 표시합니다.
- **nr_unused** - 현재 사용되지 않지만 향후 재사용을 위해 최근 Least(Least) 목록에 저장되는 dentries 수를 표시합니다.
- **age_limit** - 메모리가 짧으면 **dcache** 항목을 회수할 수 있는 시간(초)을 표시합니다.
- **want_pages** - **shrink_dcache_pages()** 함수가 호출되고 **dcache** 가 아직 정리되지 않은 경우 0이 아닙니다.
- **nr_negative** - 파일에 매핑되지 않는 음수 들여쓰기인 사용하지 않은 들여쓰기 수를 표시합니다. 대신 사용자가 제공하는 존재하지 않는 파일을 신속하게 거부할 수 있습니다.

업데이트된 /proc/sys/kernel 매개변수

msg_next_id, sem_next_id, and shm_next_id

참고:

1. 커널은 새 오브젝트에 원하는 ID를 보장하지 않습니다. 이는 사용자 공간, "잘못" ID로 오브젝트를 처리하는 방법까지입니다.

2. IPC(Inter-process Communication) 개체 할당 후 커널에서 기본값이 아닌 값으로 전환합니다. IPC 오브젝트 할당 syscall에 실패하면 값이 수정되지 않았거나 -1로 재설정되는 경우 정의되지 않습니다.

4장. RHEL 8의 콘텐츠 배포

4.1. 설치

Red Hat Enterprise Linux 8은 ISO 이미지를 사용하여 설치합니다. AMD64, Intel 64비트, 64비트 ARM, IBM Power Systems, IBM Z 아키텍처에서는 두 가지 유형의 ISO 이미지를 사용할 수 있습니다.

- 바이너리 DVD ISO: BaseOS 및 AppStream 리포지토리가 포함된 전체 설치 이미지를 사용하여 추가 리포지토리 없이 설치를 완료할 수 있습니다.

  참고

  바이너리 DVD ISO 이미지는 4.7GB보다 크므로 단일 계층 DVD에 적합하지 않을 수 있습니다. 부팅 가능한 설치 미디어를 생성하려면 바이너리 DVD ISO 이미지를 사용하는 경우 듀얼 계층 DVD 또는 USB 키를 사용하는 것이 좋습니다. Image Builder 툴을 사용하여 사용자 지정 RHEL 이미지를 만들 수도 있습니다. 이미지 빌더에 대한 자세한 내용은 *사용자 지정된 RHEL 시스템 이미지 구성* 문서를 참조하십시오.

- 부팅 ISO: 설치 프로그램으로 부팅하는 데 사용되는 최소 부팅 ISO 이미지입니다. 설치 프로그램으로 부팅하는 데 사용하는 최소 부트 ISO 이미지입니다. 이 옵션을 사용하여 소프트웨어 패키지를 설치하려면 BaseOS와 AppStream 리포지토리에 액세스해야 합니다.리포지토리는 바이너리 DVD ISO 이미지의 일부입니다.

ISO 이미지 다운로드, 설치 미디어 생성 및 RHEL 설치 완료 방법은 표준 RHEL 8 설치 문서를 참조하십시오. 자동화된 Kickstart 설치 및 기타 고급 주제는 고급 RHEL 8 설치 문서를 참조하십시오.

4.2. 리포지토리

Red Hat Enterprise Linux 8은 다음 두 가지 주요 리포지토리를 통해 배포됩니다.

- BaseOS
- AppStream

두 리포지토리 모두 기본 RHEL 설치에 필요하며 모든 RHEL 서브스크립션을 통해 사용할 수 있습니다.

BaseOS 리포지토리의 콘텐츠는 모든 설치의 기반이 되는 기본 OS 기능의 코어 세트를 제공하는 데 사용됩니다. 이 콘텐츠는 RPM 형식으로 사용 가능하며 이전 RHEL 릴리스와 비슷한 지원 조건이 적용됩니다. BaseOS를 통해 배포되는 패키지 목록은 패키지 매니페스트를 참조하십시오.

Application Stream 리포지토리의 콘텐츠에는 다양한 워크로드와 사용 사례를 지원하는 추가 사용자 공간 애플리케이션, 런타임 언어 및 데이터베이스가 포함되어 있습니다. 애플리케이션 스트림은 친숙한 RPM 형식, *모듈* 이라는 RPM 형식 또는 소프트웨어 컬렉션으로 사용할 수 있습니다. AppStream에서 사용 가능한 패키지 목록은 패키지 매니페스트를 참조하십시오.

또한 CodeReady Linux Builder 리포지토리는 모든 RHEL 서브스크립션을 통해 사용할 수 있습니다. 이는 개발자가 사용할 수 있는 추가 패키지를 제공합니다. CodeReady Linux Builder 리포지토리에 포함된 패키지는 지원되지 않습니다.

RHEL 8 리포지토리에 관한 자세한 내용은 패키지 매니페스트를 참조하십시오.

4.3. APPLICATION STREAMS

Red Hat Enterprise Linux 8에는 Application Streams의 개념이 도입되어 있습니다. 이제 여러 버전의 사용자 공간 구성 요소가 핵심 운영 체제 패키지보다 더 자주 제공되고 업데이트됩니다. 이는 플랫폼 또는 특정 배포의 기본 안정성에 영향을 주지 않고 Red Hat Enterprise Linux를 사용자 지정할 수 있는 유연성을 향상시킵니다.

Application Stream으로 사용 가능한 구성 요소는 모듈 또는 RPM 패키지로 패키징할 수 있으며 RHEL 8의 AppStream 리포지토리를 통해 제공합니다. 각 Application Stream 구성 요소에는 RHEL 8과 동일하거나 짧은 라이프사이클이 있습니다. 자세한 내용은 Red Hat Enterprise Linux 라이프사이클 을 참조하십시오.

모듈은 논리 단위, 애플리케이션, 언어 스택, 데이터베이스 또는 툴 세트를 나타내는 패키지 컬렉션입니다. 이러한 패키지는 함께 빌드, 테스트, 릴리스됩니다.

모듈 스트림은 Application Stream 구성 요소의 버전을 나타냅니다. 예를 들어 PostgreSQL 데이터베이스 서버의 여러 스트림(버전)을 기본 postgresql **:10** 스트림이 있는 **postgresql** 모듈에서 사용할 수 있습니다. 시스템에는 하나의 모듈 스트림만 설치할 수 있습니다. 개별 컨테이너에서 서로 다른 버전을 사용할 수 있습니다.

자세한 모듈 명령은 사용자 공간 구성 요소 설치, 관리 및 제거 문서에서 설명합니다. AppStream에서 사용 가능한 모듈 목록은 패키지 매니페스트를 참조하십시오.

4.4. YUM/DNF를 사용한 패키지 관리

Red Hat Enterprise Linux 8에서는 **DNF** 기술을 기반으로 하는 **YUM** 툴을 통해 소프트웨어를 설치합니다. 당사는 이전 RHEL 주 버전과의 일관성을 위해 **yum** 용어 사용을 의도적으로 준수합니다. 그러나 **yum** 이 호환성을 위해 **dnf** 에 대한 별칭이므로 **yum**이 **yum** 대신 **dnf** 를 입력하는 경우 명령이 예상대로 작동합니다.

자세한 내용은 다음 설명서를 참조하십시오.

- 사용자 공간 구성 요소 설치, 관리 및 제거
- RHEL 8 채택 고려 사항

5장. RHEL 8.1.1 릴리스

Red Hat은 마이너 릴리스 (8.Y)마다 분기별로 Red Hat Enterprise Linux 8 컨텐츠를 제공합니다. 분기 별 릴리스는 세 번째 숫자 (8.Y.1)로 번호가 매겨집니다. RHEL 8.1.1 릴리스의 새로운 기능은 아래에 설명되어 있습니다.

5.1. 새로운 기능

새 모듈 스트림: postgresql:12

RHEL 8.1.1 릴리스에는 **PostgreSQL 12** 가 도입되어 버전 10에 비해 여러 가지 새로운 기능과 개선 사항이 추가되었습니다. 주요 변경 사항은 다음과 같습니다.

- 표준 PostgreSQL 로깅 기능을 통해 자세한 세션 및 오브젝트 감사 로깅을 제공하는 PostgreSQL Audit Extension, **pgaudit**
- 파티셔닝 기능 개선 (예: 해시 파티셔닝 지원)
- 쿼리 병렬 처리 기능 개선
- 저장된 SQL 프로시저를 트랜잭션 관리 가능
- 다양한 성능 향상
- 관리 기능 개선
- SQL/JSON 경로 언어 지원
- 생성된 열 저장
- 결정적이지 않은 협력
- GSSAPI 인증 또는 다단계 인증을 사용할 때 TCP/IP 연결 암호화를 포함한 새로운 인증 기능.

PostgreSQL 11 이후 업스트림에서 사용할 수 있는 JIT(Just-In-Time) 컴파일 지원은 **postgresql:12** 모듈 스트림에서 제공되지 않습니다.

postgresql:12 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install postgresql:12
```

RHEL 8에서 이전 **postgresql** 스트림을 업그레이드하려면 전환에서 이후 스트림으로 설명한 절차를 수행한 다음 RHEL 8 버전의 **PostgreSQL** 버전으로 마이그레이션하는 데 설명된 대로 PostgreSQL 데이터를 마이그레이션합니다.

(JIRA:RHELPLAN-26926)

jboss Toolset을 버전 1.39로 다시 설정

satellite Toolset이 1.39 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- **async** - **.await** 구문이 stable에 추가되었습니다. 이제 **비동기** 함수와 블록을 정의하고 **.await** 기능을 정의할 수 있습니다.
- 향상된 파이프라인 컴파일로 빌드 시간을 10-20% 향상하여 최적화되고 정리된 일부 crate 그래프를 빌드할 수 있습니다.

- **by-move** 바인딩이 **일치** 표현식의 기본 패턴에 있는 **경우** 이제 가 이러한 바인딩을 참조할 수 있는 경우입니다.
- 컴파일 시 메모리 보안 버그를 감지해야 하지만 이전의 검사기에는 제한 사항이 있으며 정의되지 않은 동작과 메모리가 안전하지 않았습니다. 새로운 NLL 차용 검사기는 이러한 문제를 찾을 수 있으며 마이그레이션 단계로 이에 대한 경고를 높였습니다. 이제 이러한 경고가 하드 오류입니다.
- **이제 mem::{uninitialized, zeroed}** 함수에서 lint를 제공하여 **&T 및 Box<T>** 와 같이 일부 유형을 초기화하는 데 사용됩니다.
- 다음 함수는 표준 **라이브러리에서 fn** 을 설정합니다. **Vec::new**,**String::new**,**LinkedList::new**,**str::len**,**[T]::len**,**str::as_bytes**,**abs**,**wrapping_abs** 및 **overflowing_abs**.

pvc Toolset 모듈 스트림을 설치하려면 root로 다음 명령을 실행합니다.

```
# yum module install rust-toolset
```

사용법에 대한 자세한 지침은 Rust Toolset 사용을 참조하십시오.

(BZ#1680096)

새 모듈: jmc:rhel8

RHEL 8.1.1에서는 HotSpot JVM을 위한 강력한 프로파일러인 JDK Mission Control(JMC)을 새로운 **jmc** 모듈로 도입했습니다. JMC는 JDK¢ Recorder에서 수집한 광범위한 데이터의 효율적이고 자세한 분석을 위한 고급 툴 세트를 제공합니다. 툴 체인을 사용하면 개발자와 관리자가 로컬로 실행되거나 프로덕션 환경에서 배포되는 Java 애플리케이션에서 데이터를 수집 및 분석할 수 있습니다. JMC를 실행하려면 JDK 버전 8 이상이 필요합니다. JMC가 JDK¢ Recorder 기능에 액세스할 수 있도록 목표 Java 애플리케이션은 OpenJDK 버전 11에서 실행해야 합니다.

jmc:rhel8 모듈 스트림에는 두 개의 프로필이 있습니다.

- 전체 JMC 애플리케이션을 설치하는 **common** 프로필
- 코어 Java 라이브러리만 설치하는 **core** 프로필(jm**c-core**)

jmc:rhel8 모듈 스트림의 **공통** 프로필을 설치하려면 다음을 사용합니다.

```
# yum module install jmc:rhel8/common
```

프로필 이름을 **core** 로 변경하여 **jmc-core** 패키지만 설치합니다.

(BZ#1716452)

RHEL 8에서 NET Core 3.1 사용 가능

이번 업데이트에서는 .NET Core 3.1 Software Development Kit (SDK) 및 .NET Core 3.1 Runtime을 RHEL 8에 추가합니다. 또한 웹 애플리케이션 및 서비스 구축을 위한 ASP.NET Core 3.1 프레임워크를 사용할 수 있습니다.

(BZ#1711405)

virtio-win 드라이버용 새 설치 프로그램

virtio-win 패키지에 대화형 Windows 설치 프로그램이 추가되었습니다. 따라서 Microsoft Windows를 게스트 운영 체제로 사용하는 가상 머신에 반가상화 KVM 드라이버를 쉽고 효율적으로 설치할 수 있습니다.

(BZ#1745298)

container-tools 업데이트

podman,**buildah**,**skopeo** 및 **runc** 툴이 포함된 **container-tools** 모듈이 업데이트되었습니다. 이제 컨테이너의 툴이 FIPS 모드가 활성화된 상태로 빌드됩니다. 또한 이번 업데이트에서는 몇 가지 버그와 보안 문제가 수정되었습니다.

(BZ#1783277)

Conmon 은 이제 별도의 패키지에 있습니다

OCI(Common open container Initiative) 컨테이너 런타임 모니터 유틸리티가 별도의 공통 패키지로 이동되었습니다. **podman** 패키지에서 더 이상 사용할 수 없습니다.

(BZ#1753209)

6장. RHEL 8.1.0 릴리스

6.1. 새로운 기능

이 부분에서는 Red Hat Enterprise Linux 8.1에 도입된 새로운 기능 및 주요 개선 사항에 대해 설명합니다.

6.1.1. 설치 프로그램 및 이미지 생성

킥스타트 설치 중에 모듈을 비활성화할 수 있음

이번 개선된 기능을 통해 이제 모듈을 비활성화하여 모듈에서 패키지 설치를 방지할 수 있습니다. Kickstart 설치 중에 모듈을 비활성화하려면 명령을 사용합니다.

module --name=foo --stream=bar --disable

(BZ#1655523)

repo.git 섹션에 대한 지원에서 블루프린트로 사용 가능

새 **repo.git** 청사진 섹션을 사용하면 사용자가 이미지 빌드에 추가 파일을 포함할 수 있습니다. 파일은 **lorax-composer** 빌드 서버에서 액세스할 수 있는 git 리포지토리에서 호스팅해야 합니다.

(BZ#1709594)

Image Builder에서 더 많은 클라우드 공급자에 대한 이미지 생성을 지원

이번 업데이트를 통해 Image Builder는 Image Builder에서 이미지를 생성할 수 있는 클라우드 프로바이더 수를 확장했습니다. 따라서 이제 Google Cloud 및¢ Cloud에도 배포할 수 있는 RHEL 이미지를 만들고 이러한 플랫폼에서 사용자 지정 인스턴스를 실행할 수 있습니다.

(BZ#1689140)

6.1.2. 소프트웨어 관리

dnf-utils 의 이름이 yum-utils로 변경되었습니다.

이번 업데이트를 통해 **YUM** 스택의 일부인 **dnf-utils** 패키지의 이름이 **yum-utils** 로 변경되었습니다. 호환성을 위해 **dnf-utils** 이름을 사용하여 패키지를 계속 설치할 수 있으며 시스템을 업그레이드할 때 원래 패키지를 자동으로 대체합니다.

(BZ#1722093)

6.1.3. 서브스크립션 관리

subscription-manager 에서 역할, 사용량 및 애드온 값을 보고

이번 업데이트를 통해 **subscription-manager** 는 이제 고객 포털 또는 Satellite에 등록된 현재 조직에서 사용 가능한 각 서브스크립션의 Role, Usage 및 Add-ons 값을 표시할 수 있습니다.

- 해당 서브스크립션에 Role, Usage 및 Add-ons 값이 추가되어 사용 가능한 서브스크립션을 표시하려면 다음을 사용합니다.

```
# subscription-manager list --available
```

- 추가 Role, Usage 및 Add-ons 값을 포함하여 소비된 서브스크립션을 표시하려면 다음을 사용합니다.

```
# subscription-manager list --consumed
```

(BZ#1665167)

6.1.4. 인프라 서비스

버전 2.12로 업데이트 조정

tuned 패키지가 업스트림 버전 2.12로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- 제거 및 재연결된 장치 처리가 수정되었습니다.
- CPU 목록 부정 지원이 추가되었습니다.
- **sysctl** 툴에서 **Tuned** 와 관련된 새로운 구현으로 전환하여 런타임 커널 매개변수 구성의 성능이 향상되었습니다.

(BZ#1685585)

Chrony 가 버전 3.5로 업데이트

chrony 패키지가 업스트림 버전 3.5로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- RHEL 8.1 커널의 하드웨어 타임스탬프를 통한 시스템 클록의 보다 정확한 동기화 지원이 추가되었습니다.
- 하드웨어 타임스탬프가 대폭 개선되었습니다.
- 사용 가능한 폴링 간격 범위가 확장되었습니다.
- 필터 옵션이 NTP 소스에 추가되었습니다.

(BZ#1685469)

새로운 FSRouting 라우팅 프로토콜 스택을 사용할 수 있습니다.

이번 업데이트를 통해 **Quagga** 는 새로운 라우팅 프로토콜 스택인 **Free Range Routing** (**Free Range** Routing **)**(즉, 새 라우팅 프로토콜 스택)으로 교체되었습니다. **GAR은** AppStream 리포지토리에서 사용할 수 있는 **frr** 패키지에서 제공합니다.

pvcR 은 **BGP**,**IS-IS**,**OSPF**,**PIM** 및 **RIP** 와 같은 여러 IPv4 및 IPv6 라우팅 프로토콜을 지원하는 TCP/IP 기반 라우팅 서비스를 제공합니다.

pvc **R** 을 설치하면 시스템은 전용 라우터 역할을 하며, 내부 또는 외부 네트워크의 다른 라우터와 라우팅 정보를 교환할 수 있습니다.

(BZ#1657029)

GNU enscript에서 ISO-8859-15 인코딩 지원

이번 업데이트를 통해 ISO-8859-15 인코딩 지원이 GNU 서브스크립션 프로그램에 추가되었습니다.

(BZ#1664366)

phc2sys에서 시스템 클럭 오프셋 측정의 정확도 향상

linuxptp 패키지의 **phc2sys** 프로그램은 이제 시스템 클록의 오프셋을 측정하는 보다 정확한 방법을 지원합니다.

(BZ#1677217)

ptp4l 에서 active-backup 모드에서 팀 인터페이스를 지원

이번 업데이트를 통해 active-backup 모드에서 팀 인터페이스에 대한 지원이 **PTP 경계/조직 시계** (ptp4l)에 추가되었습니다.

(BZ#1685467)

macvlan 인터페이스의 PTP 시간 동기화 지원

이번 업데이트에서는 **macvlan** 인터페이스의 하드웨어 타임스탬프 지원이 Linux 커널에 추가되었습니다. 결과적으로 **macvlan** 인터페이스는 이제 시간 동기화에 PTP(**Precision Time Protocol**)를 사용할 수 있습니다.

(BZ#1664359)

6.1.5. 보안

새 패키지: fapolicyd

fapolicyd 소프트웨어 프레임워크에는 사용자 정의 정책에 따라 애플리케이션 화이트리스트 및 블랙리스트 형식이 도입되었습니다. 애플리케이션 화이트리스트 기능은 시스템에서 신뢰할 수 없고 악의적인 애플리케이션 실행을 방지하기 위한 가장 효율적인 방법 중 하나를 제공합니다.

fapolicyd 프레임워크는 다음 구성 요소를 제공합니다.

- **fapolicyd** 서비스
- **fapolicyd** 명령줄 유틸리티
- **yum** 플러그인
- 규칙 언어

관리자는 모든 애플리케이션에 대한 경로, 해시, MIME 유형 또는 신뢰에 따라 감사 가능성으로 **허용** 및 **거부** 규칙을 정의할 수 있습니다.

모든 **fapolicyd** 설정은 전반적인 시스템 성능에 영향을 미칩니다. 성능 저하는 사용 사례에 따라 다릅니다. 애플리케이션에서 **open() 및 exec()** 시스템 호출을 허용 목록에 추가하므로 이러한 시스템 호출을 자주 수행하는 애플리케이션에 주로 영향을 미칩니다.

자세한 내용은 **fapolicyd(8)**, **fapolicyd.rules(5)** 및 **fapolicyd.conf(5)** 도움말 페이지를 참조하십시오.

(BZ#1673323)

새 패키지: udica

새 **udica** 패키지는 컨테이너에 대한 SELinux 정책을 생성하는 도구를 제공합니다. 오디 **카를 사용하면** 컨테이너에서 스토리지, 장치 및 네트워크와 같은 호스트 시스템 리소스에 액세스하는 방법을 보다 효과적으로 제어하기 위한 맞춤형 보안 정책을 만들 수 있습니다. 이를 통해 보안 위반에 대해 컨테이너 배포를 강화할 수 있으며 규정 준수의 달성 및 유지를 단순화할 수 있습니다.

자세한 내용은 RHEL 8 Using SELinux 제목의 컨테이너에 대한 SELinux 정책 만들기 섹션을 참조하십시오.

(BZ#1673643)

SELinux 사용자 공간 도구가 버전 2.9로 업데이트

libsepol,**libselinux**,**libsemanage**,**policycoreutils**,**checkpolicy** 및 **mcstrans** SELinux 사용자 공간 툴이 최신 업스트림 릴리스 2.9로 업그레이드되어 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다.

(BZ#1672638,BZ#1672642,BZ#1672637,BZ#1672640,BZ#1672635,BZ#1672641)

setools 버전 4.2.2로 업데이트

툴 및 라이브러리의 SETools 컬렉션이 다음 변경 사항을 제공하는 최신 업스트림 릴리스 4.2.2로 업그레이드되었습니다.

- 소스 정책 로드가 더 이상 지원되지 않으므로 도움말 페이지에서 제거된 소스 정책 참조
- 별칭 로드에서 성능 회귀 문제 수정

(BZ#1672631)

SELinux-policy 가 3.14.3으로 업데이트

selinux-policy 패키지가 업스트림 버전 3.14.3으로 업그레이드되었으며 이전 버전에 비해 허용 규칙에 많은 버그 수정 및 개선 사항을 제공합니다.

(BZ#1673107)

새로운 SELinux 유형: excludedd_t

3개의 장치를 관리하기 위한 시스템 데몬인 새로운 SELinux 유형인 salt **d _t** 는 바뀝니다. 결과적으로 **이제** SELinux 강제 모드에서 제한된 서비스로 강제 실행됩니다.

(BZ#1684103)

새 SELinux 정책 클래스: bpf

새로운 SELinux 정책 클래스 **bpf** 가 도입되었습니다. **bpf** 클래스를 사용하면 사용자가 SElinux를 통해 BPF(Berkeley Packet Filter) 흐름을 제어할 수 있으며, EBPF(Extended Berkeley Packet Filter) 프로그램과 맵을 검사하고 간단하게 조작할 수 있습니다.

(BZ#1673056)

OpenSCAP을 버전 1.3.1로 업데이트

openscap 패키지가 업스트림 버전 1.3.1로 업그레이드되어 이전 버전에 대해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- SCAP 1.3 소스 데이터 스트림 지원: 평가, XML 스키마, 검증
- 맞춤형 파일은 ARF 결과 파일에 포함되어 있습니다.
- OVAL 세부 정보는 항상 HTML 보고서에 표시됩니다. 사용자는 **--oval-results** 옵션을 제공하지 않아도 됩니다.

- HTML 보고서에는 OVAL **extend_definition** 요소를 사용하여 다른 OVAL 정의에서 포함된 OVAL 테스트 세부 정보도 표시됩니다.
- OVAL 테스트 ID가 HTML 보고서에 표시됩니다.
- 규칙 ID가 HTML 가이드에 표시됩니다

(BZ#1718826)

OpenSCAP 에서 SCAP 1.3 지원

OpenSCAP 제품군은 SCAP 1.3 최신 버전을 준수하는 데이터 스트림을 지원합니다. **scap-security-guide** 패키지에 포함된 것과 같은 SCAP 1.3 데이터 스트림을 추가 사용 제한 없이 SCAP 1.2 데이터 스트림과 동일한 방식으로 사용할 수 있습니다.

(BZ#1709429)

scap-security-guide 가 버전 0.1.46로 업데이트

scap-security-guide 패키지가 업스트림 버전 0.1.46로 업그레이드되어 이전 버전에 대해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 * SCAP 콘텐츠는 SCAP 표준의 최신 버전을 준수하는 SCAP 1.3 * SCAP 콘텐츠는 UBI 이미지를 지원합니다.

(BZ#1718839)

OpenSSH 가 8.0p1로 업데이트

openssh 패키지가 업스트림 버전 8.0p1로 업그레이드되어 이전 버전에 대해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- **ssh-keygen** 툴의 기본 RSA 키 크기가 3072비트로 향상되었습니다.
- **ShowPatchLevel** 설정 옵션에 대한 지원 삭제
- Kerberos 정리 절차 수정과 같은 여러 GSSAPI 키 교환 코드 수정 적용
- **sshd_net_t** SELinux 컨텍스트로 대체
- **일치 최종** 블록에 대한 지원 추가
- **ssh-copy-id** 명령에서 마이너 문제 수정
- **scp** 유틸리티와 관련된 CVE(Common Vulnerabilities and Exposures) (CVE-2019-6111, CVE-2018-20685, CVE-2019-6109)

이 릴리스에서는 CVE-2019-6111을 완화하는 **scp** 의 마이너 비호환성이 도입되었습니다. 스크립트가 scp 다운로드 중에 경로의 고급 bash 확장에 의존하는 경우 **-T** 스위치를 사용하여 신뢰할 수 있는 서버에 연결할 때 이러한 완화 조치를 일시적으로 끌 수 있습니다.

(BZ#1691045)

libssh 가 시스템 차원의 암호화 정책을 준수합니다.

이제 **libssh** 클라이언트와 서버는 이제 각각 **/etc/libssh/libssh_client.config** 파일과 **/etc/libssh/libssh_server.config** 파일을 자동으로 로드합니다. 이 구성 파일에는 **libssh 백엔드를 위한 시스템 전체의 crypto-policies 구성 요소와 /etc/ssh** /ssh **_config 또는 /etc/ssh/sshd_config** OpenSSH 구성 파일에 설정된 옵션이 포함됩니다. 구성 파일의 자동 로드를 통해 **libssh** 는 이제 **crypto-policies** 에 의해 설정된 시스템 전체 암호화 설정을 사용합니다. 이러한 변경으로 인해 애플리케이션에서 사용하는 암호화 알고리즘 집합에 대한 제어가 간소화됩니다.

(BZ#1610883, BZ#1610884)

rsyslog 가 FROMHOST 케이스를 유지하는 옵션을 사용할 수 있습니다.

이번 업데이트에서는 **imudp 및 im tcp** 모듈에 대한 **FROMHOST** 속성의 문자 대소문자 보존을 관리하는 **옵션을** 도입했습니다. **preservecase** 값을 **on** 으로 설정하면 **FROMHOST** 속성이 대/소문자를 구분하여 처리됩니다. 기존 구성을 중단하지 않으려면 **imtcp 및 off 의 경우 preservecase 의 기본값이 im udp** 에 설정되어 있습니다.

(BZ#1614181)

6.1.6. 네트워킹

VXLAN 및 GENEVE 터널에서 PMTU 검색 및 경로 리디렉션 지원

RHEL(Red Hat Enterprise Linux) 8.0의 커널은 VXLAN(Virtual Extensible LAN) 및GENEVE(Generic Network Virtualization Encapsulation) 터널을 위한 ICMP(Internet Control Message Protocol) 및 ICMPv6 메시지를 처리하지 않았습니다. 그 결과 RHEL 릴리스의 VXLAN 및 GENEVE 터널에서는 8.1 이전의 Path MTU(PMTU) 검색 및 경로 리디렉션이 지원되지 않았습니다. 이번 업데이트를 통해 커널은 PMTU를 조정하고 전달 정보를 수정하여 ICMP "Destination Unreachable" 및 "Redirect Message"와 ICMPv6 "Packet Too Big" 및 "Destination Unreachable" 오류 메시지를 처리합니다. 결과적으로 RHEL 8.1은 VXLAN 및 GENEVE 터널을 사용하여 PMTU 검색 및 경로 리디렉션을 지원합니다.

(BZ#1652222)

커널의 XDP 및 네트워킹 eBPF 기능 주요 변경 사항

커널 패키지의 XDP 및 네트워킹 eBPF 기능이 업스트림 버전 5.0으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- eBPF 프로그램은 이제 TCP/IP 스택과 보다 효과적으로 상호 작용하고, 흐름 분산을 수행하고, 광범위한 **bpf** 도우미를 사용할 수 있으며 새로운 맵 유형에 액세스할 수 있습니다.
- 이제 AF_XDP 소켓에서 XDP 메타데이터를 사용할 수 있습니다.

(BZ#1687459)

ioctl() 의 새로운 PTP_SYS_OFFSET_EXTENDED 제어는 측정된 system-PHC ofsets의 정확성을 개선합니다.

이 향상된 기능으로 **PTP_SYS_OFFSET_EXTENDED** 제어를 추가하여 **ioctl()** 함수에 PTP_SYS_OFFSET_EXTENDED 제어를 추가하여 시스템 PTP(Precision Time Protocol) 오프셋을 더욱 정확하게 측정할 수 있습니다. 예를 들어, **chrony** 서비스에서 PHC와 시스템 클록 간의 오프셋을 측정하는 데 사용하는 **PTP_SYS_OFFSET** 제어는 충분히 정확하지 않습니다. 새로운 **PTP_SYS_OFFSET_EXTENDED** 제어를 사용하면 드라이버에서 가장 낮은 비트 읽기를 격리할 수 있습니다. 이렇게 하면 측정된 오프셋의 정확도가 향상됩니다. 일반적으로 네트워크 드라이버는 여러 PCI 레지스터를 읽고 드라이버는 두 개의 시스템 클록 읽기 사이에 PHC 타임스탬프의 가장 낮은 비트를 읽지 않습니다.

(BZ#1677215)

ipset을 7.1 버전으로 다시 설정

ipset 패키지가 업스트림 버전 7.1으로 업그레이드되어 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다.

- **ipset** 프로토콜 버전 7에는 **IPSET_CMD_GET_BYNAME** 및 **IPSET_CMD_GET_BYINDEX** 작업이 도입되었습니다. 또한 사용자 공간 구성 요소에서 커널 구성 요소에서 지원하는 정확한 호환성 수준을 감지할 수 있습니다.

- 메모리 누수 및 사용 후 무료 버그와 같은 많은 버그가 수정되었습니다.

(BZ#1649090)

6.1.7. 커널

RHEL 8.1의 커널 버전

Red Hat Enterprise Linux 8.1은 커널 버전 4.18.0-147과 함께 배포됩니다.

(BZ#1797671)

커널의 라이브 패치 사용 가능

커널 **kpatch** 에 대한 실시간 패치는 프로세스를 재부팅하거나 다시 시작하지 않고도 실행 중인 커널을 패치하는 메커니즘을 제공합니다. 심각 및 중요한 CVE를 해결하기 위해 EUS (Extended Update Support) 정책에 적용되는 일부 RHEL 마이너 릴리스 스트림에 대한 라이브 커널 패치가 제공됩니다.

RHEL 8.1 버전의 커널에 대한 **kpatch** 스트림을 구독하려면 RHEA-2019:3695 권고에서 제공하는 **kpatch-patch-4_18_0-147** 패키지를 설치하십시오.

자세한 내용은 커널 관리, 모니터링 및 업데이트에서 커널 라이브 패치를 사용하여 패치 적용을 참조하십시오.

(BZ#1763780)

RHEL 8의 Extended Berkeley Packet Filter

eBPF(Extended Berkeley Packet Filter)는 제한된 기능 집합에 액세스할 수 있는 제한된 샌드박스 환경에서 커널 공간에서 코드를 실행할 수 있는 커널 내 가상 시스템입니다. 가상 시스템은 특수 어셈블리와 유사한 코드를 실행합니다. 그런 다음 코드가 커널로 로드되고 즉시 컴파일을 사용하여 기본 머신 코드로 변환됩니다. Red Hat은 **eBPF** 가상 시스템을 활용하는 수많은 구성 요소를 제공합니다. 각 구성 요소는 다른 개발 단계에 있으므로 현재 모든 구성 요소가 완전히 지원되지는 않습니다.

RHEL 8.1에서는 **BCC(BPF Compiler Collection)** 툴 패키지가 AMD 및 Intel 64비트 아키텍처에서 완벽하게 지원됩니다. **BCC** 툴 패키지는 **eBPF** 가상 시스템을 사용하는 동적 커널 추적 유틸리티 컬렉션입니다.

다음 **eBPF** 구성 요소는 현재 기술 프리뷰로 사용할 수 있습니다.

- **BCC** 툴은 64비트 ARM 아키텍처, IBM Power Systems, Little Endian, IBM Z 아키텍처에서 패키지됩니다.

- 모든 아키텍처의 **BCC** 라이브러리

- **bpftrace** 추적 언어

- eXpress Data Path(XDP) 기능

기술 프리뷰 구성 요소에 대한 자세한 내용은 6.5.2절. "커널" 을 참조하십시오.

(BZ#1780124)

Red Hat Enterprise Linux 8이 초기 kdump지원

early kdump 기능을 사용하면 크래시 커널과 initramfs가 초기 충돌 시 **vmcore** 정보를 캡처할 수 있을 만큼 충분히 빨리 로드할 수 있습니다.

early kdump 에 대한 자세한 내용은 **/usr/share/doc/kexec-tools/early-kdump-howto.txt** 파일을 참조하십시오.

(BZ#1520209)

RHEL 8에서 ipcmni_extend지원

Red Hat Enterprise Linux 8에 새로운 커널 명령행 매개 변수 **ipcmni_extend** 가 추가되었습니다. 매개 변수는 현재 최대 32KB(15비트)에서 16MB(24비트)까지 고유한 시스템 V 프로세스 간 통신(IPC) 식별자를 확장합니다. 결과적으로 많은 공유 메모리 세그먼트를 생성하는 애플리케이션이 32KB 제한을 초과하지 않고 더 강력한 IPC 식별자를 만들 수 있습니다.

경우에 따라 **ipcmni_extend** 를 사용하면 성능 오버헤드가 적으며 애플리케이션에 고유한 IPC 식별자가 32KB 이상 필요한 경우에만 사용해야 합니다.

(BZ#1710480)

영구 메모리 초기화 코드에서 병렬 초기화 지원

영구 메모리 초기화 코드를 사용하면 영구 메모리 노드가 여러 개인 시스템에서 병렬 초기화가 가능합니다. 병렬 초기화는 대량의 영구 메모리가 있는 시스템의 전체 메모리 초기화 시간이 크게 단축됩니다. 따라서 이제 이러한 시스템을 훨씬 더 빨리 부팅할 수 있습니다.

(BZ#1634343)

TPM 사용자 공간 도구가 마지막 버전으로 업데이트되었습니다

tpm2-tools 사용자 공간 도구가 버전 2.0으로 업데이트되었습니다. 이번 업데이트를 통해 **tpm2-tools** 는 많은 결함을 수정할 수 있습니다.

(BZ#1664498)

The rngd 데몬은 이제 루트가 아닌 권한으로 실행될 수 있습니다.

임의 번호 생성기 데몬(**rngd**)은 임의로 소스에서 제공한 데이터가 임의로 임의로 지정되었는지 확인한 다음 커널의 임의 번호 엔트로피 풀에 데이터를 저장합니다. 이번 업데이트를 통해 **rngd** 는 루트가 아닌 사용자 권한으로 를 실행하여 시스템 보안을 강화할 수 있습니다.

(BZ#1692435)

ibmvnic 드라이버에 대한 전체 지원

Red Hat Enterprise Linux 8.0이 도입되면서 IBM POWER 아키텍처용 IBM VNIC(Virtual Network Interface Controller) 드라이버인 **ibmvnic** 을 기술 프리뷰로 사용할 수 있었습니다. vNIC는 엔터프라이즈 기능을 제공하고 네트워크 관리를 간소화하는 PowerVM 가상 네트워킹 기술입니다. SR-IOV NIC와 결합하면 가상 NIC 수준에서 대역폭 제어 QoS(Quality of Service) 기능을 제공하는 고성능의 효율적인 기술입니다. vNIC는 가상화 오버헤드를 크게 줄여 네트워크 가상화에 필요한 CPU 및 메모리를 포함하여 대기 시간을 줄이고 서버 리소스가 줄어듭니다.

Red Hat Enterprise Linux 8.1부터 **ibmvnic** 장치 드라이버는 IBM POWER9 시스템에서 완전히 지원됩니다.

(BZ#1665717)

Intel ® Fedora-Path Architecture(OPA) 호스트 소프트웨어

Intel MBA(OPA) 호스트 소프트웨어는 Red Hat Enterprise Linux 8.1에서 완벽하게 지원됩니다. Intel OPA는 클러스터형 환경의 컴퓨팅 노드와 I/O 노드 간의 고성능 데이터 전송(고급 대역폭, 높은 메시지 속도, 짧은 대기 시간)을 위해 HFI(Host Fabric Interface) 하드웨어에 초기화 및 설정을 제공합니다.

(BZ#1766186)

RHEL 8의 디버그 커널에서 UBSan 이 활성화되었습니다

The **undefined Behavior Sanitizer** (UB**San)**유틸리티는 런타임 시 C 코드 언어에서 정의되지 않은 동작 결함을 노출합니다. 컴파일러 동작이 개발자의 기대치와 다른 경우도 있기 때문에 이 유틸리티는 디버그 커널에서 활성화되었습니다. 특히 미묘한 버그가 나타나는 컴파일러 최적화의 경우. 결과적으로 **UBSan** 이 활성화된 디버그 커널을 실행하면 시스템에서 이러한 버그를 쉽게 감지할 수 있습니다.

(BZ#1571628)

fadump 인프라에서 RHEL 8의 재등록 지원

크래시 메모리 범위를 업데이트하기 위해 메모리 핫 애드/제거 작업 후에 펌웨어 지원 덤프(f**dump**) 인프라의 재등록(등록 및 등록 취소)에 대한 지원이 추가되었습니다. 이 기능은 **udev** 이벤트 중 사용자 공간에서 **fadump** 를 취소하고 등록하는 동안 시스템이 잠재적인 경쟁 문제를 방지하는 것을 목표로 합니다.

(BZ#1710288)

RHEL for Real Time 8에서 determine_maximum_mpps.sh 스크립트가 도입되었습니다.

queuelat 테스트 프로그램을 사용하는 데 도움이 되도록 **determine_maximum_mpps.sh** 스크립트가 도입되었습니다. 스크립트는 **대기열에 따라 시스템이** 처리할 수 있는 초당 최대 패킷을 결정합니다.

(BZ#1686494)

kernel-rt 소스 트리가 최신 RHEL 8 트리와 일치

커널-rt 소스는 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공하는 최신 Red Hat Enterprise Linux 커널 소스 트리를 기반으로 업그레이드되었습니다.

(BZ#1678887)

RHEL for Real Time 8에 ssdd 테스트가 추가되었습니다.

추적 하위 시스템의 스트레스 테스트를 활성화하기 위해 **ssdd** 테스트가 추가되었습니다. 테스트에서는 추적 시스템 내에서 잠금이 올바른지 확인하기 위해 여러 추적 스레드를 실행합니다.

(BZ#1666351)

6.1.8. 하드웨어 활성화

Optane DC 영구 메모리 기술의 메모리 모드가 완전히 지원됩니다.

Intel Optane DC 영구 메모리 스토리지 장치는 데이터 센터급 영구 메모리 기술을 제공하여 트랜잭션 처리량을 크게 높일 수 있습니다.

Memory Mode 기술을 사용하기 위해 시스템에 특별한 드라이버나 특정 인증이 필요하지 않습니다. 메모리 모드는 운영 체제에 투명합니다.

(BZ#1718422)

IBM Z에서 시스템 부팅 서명 확인 지원

Secure Boot를 사용하면 시스템 펌웨어가 커널 공간 코드에 서명하는 데 사용된 암호화 키의 신뢰성을 확인할 수 있습니다. 따라서 신뢰할 수 있는 벤더의 코드만 실행할 수 있으므로 이 기능을 통해 보안이 향상됩니다.

Secure Boot를 사용하려면 IBM z15가 필요합니다.

(BZ#1659399)

6.1.9. 파일 시스템 및 스토리지

DIF/DIX(데이터 무결성 필드/데이터 무결성 확장) 지원

DIF/DIX는 하드웨어 벤더가 이를 검증하고 RHEL의 특정 HBA(Host Bus Adapter) 및 스토리지 어레이 구성에 대한 완벽한 지원을 제공하는 구성에서 지원됩니다.

DIF/DIX는 다음 설정에서 지원되지 않습니다.

- 부팅 장치에서는 사용할 수 없습니다.
- 가상화된 게스트에서는 지원되지 않습니다.
- Red Hat은 DIF/DIX가 활성화된 경우 ASMLib(Automatic Storage Management library) 사용을 지원하지 않습니다.

DIF/DIX는 스토리지 장치에서 활성화 또는 비활성화되며, 애플리케이션에 이르기까지 다양한 계층이 포함됩니다. 스토리지 장치에서 DIF를 활성화하는 방법은 장치 종속적입니다.

DIF/DIX 기능에 대한 자세한 내용은 What is DIF/DIX 를 참조하십시오.

(BZ#1649493)

Optane DC 메모리 시스템에서 EDAC 보고서 지원

이전 버전에서는 메모리 주소가 NVDIMM 모듈 내에 있는 경우 EDAC에서 메모리 수정/올바른 이벤트를 보고하지 않았습니다. 이번 업데이트를 통해 EDAC는 올바른 메모리 모듈 정보를 사용하여 이벤트를 올바르게 보고할 수 있습니다.

(BZ#1571534)

VDO Ansible 모듈이 Ansible 패키지로 이동

이전에는 VDO Ansible 모듈이 **vdo** RPM 패키지에서 제공되었습니다. 이 릴리스에서는 모듈이 **ansible** 패키지에서 대신 제공됩니다.

VDO Ansible 모듈 파일의 원래 위치는 다음과 같습니다.

```
/usr/share/doc/vdo/examples/ansible/vdo.py
```

파일의 새 위치는 다음과 같습니다.

```
/usr/lib/python3.6/site-packages/ansible/modules/system/vdo.py
```

vdo 패키지는 Ansible 플레이북을 계속 배포합니다.

Ansible에 대한 자세한 내용은 http://docs.ansible.com/ 을 참조하십시오.

(BZ#1669534)

Aero 어댑터가 완전히 지원됨

이전에 기술 프리뷰로 사용할 수 있는 다음과 같은 Aero 어댑터가 이제 완전하게 지원됩니다.

- PCI ID 0x1000:0x00e2 및 0x1000:0x00e6, **mpt3sas** 드라이버에 의해 제어됨
- PCI ID 0x1000:Ox10e5 및 0x1000:0x10e6, **megaraid_sas** 드라이버에 의해 제어됨

(BZ#1663281)

LUKS2에서 온라인 재암호화 지원

Linux 통합 키 설정 버전 2(LUKS2) 형식은 이제 장치가 사용 중인 동안 암호화된 장치를 재암호화하는 기능을 지원합니다. 예를 들어 다음 작업을 수행하기 위해 장치에서 파일 시스템을 마운트 해제할 필요가 없습니다.

- 볼륨 키 변경
- 암호화 알고리즘 변경

암호화되지 않은 장치를 암호화할 때 파일 시스템을 마운트 해제해야 하지만 이제 암호화 속도가 훨씬 빨라집니다. 암호화를 간단히 초기화한 후 파일 시스템을 다시 마운트할 수 있습니다.

또한 LUKS2 재암호화의 복원력이 향상되었습니다. 재암호화 프로세스 중에 성능 또는 데이터 보호 우선순위를 지정하는 여러 옵션 중에서 선택할 수 있습니다.

LUKS2 재암호화를 수행하려면 **cryptsetup reencrypt** 하위 명령을 사용합니다. Red Hat에서는 더 이상 LUKS2 포맷에 **cryptsetup-reencrypt** 유틸리티 사용을 권장하지 않습니다.

LUKS1 형식은 온라인 재암호화 기능을 지원하지 않으며 **cryptsetup reencrypt** 하위 명령은 LUKS1과 호환되지 않습니다. LUKS1 장치를 암호화하거나 다시 암호화하려면 **cryptsetup-reencrypt** 유틸리티를 사용합니다.

디스크 암호화에 대한 자세한 내용은 LUKS를 사용하여 블록 장치 암호화를 참조하십시오.

(BZ#1676622)

RHEL 8에서 사용 가능한 ext4의 새로운 기능

RHEL8에서 다음은 ext4의 새로운 완전히 지원되는 기능입니다.

- 기본이 아닌 기능:
  - **project**
  - **할당량**
  - **mmp**
- 기본이 아닌 마운트 옵션 :
  - **bsddf|minixdf**
  - **grpid|bsdgroups 및 nogrpid|sysvgroups**
  - **resgid=n 및 resuid=n**
  - **errors={continue|remount-ro|panic}**

- **commit=nrsec**
- **max_batch_time=usec**
- **min_batch_time=usec**
- **grpquota|noquota|quota|usrquota**
- **prjquota**
- **dax**
- **lazytime|nolazytime**
- **discard|nodiscard**
- **init_itable|noinit_itable**
- **jqfmt={vfsold|vfsv0|vfsv1}**
- **usrjquota=aquota.user|grpjquota=aquota.group**

기능 및 마운트 옵션에 대한 자세한 내용은 **ext4** 도움말 페이지를 참조하십시오. 기타 ext4 기능, 마운트 옵션 또는 두 가지 기능 조합, 마운트 옵션 또는 둘 다 Red Hat에서 완전히 지원하지 않을 수도 있습니다. 특정 워크로드에 Red Hat 릴리스에서 완전히 지원되지 않는 기능 또는 마운트 옵션이 필요한 경우 Red Hat 지원팀에 문의하여 지원 목록에 포함되도록 평가하십시오.

(BZ#1741531)

NVMe over RDMA에서 IBM Coral 시스템의 대상 모드에서 Infiniband 지원

RHEL 8.1에서 NVMe over RDMA는 이제 IBM Coral 시스템의 대상 모드에서 **Infiniband** 를 지원하며 하나의 NVMe PCIe가 대상 카드로 추가됩니다.

(BZ#1721683)

6.1.10. 고가용성 및 클러스터

Pacemaker에서 동시 펜싱 클러스터 속성을 true로 기본값으로 설정합니다.

여러 클러스터 노드를 동시에 펜싱해야 하고 구성된 다른 펜스 장치를 사용하는 경우 Pacemaker에서 이전과 같이 직렬화되지 않고 동시에 펜싱을 실행합니다. 이로 인해 여러 노드를 펜싱해야 하는 경우 대규모 클러스터에서 복구가 크게 증가할 수 있습니다.

(BZ#1715426)

공유 논리 볼륨을 확장해도 더 이상 모든 클러스터 노드에서 새로 고침할 필요가 없습니다.

이번 릴리스에서는 공유 논리 볼륨을 확장하는 데 한 클러스터 노드에서 **lvextend** 명령을 실행한 후 모든 클러스터 노드에서 더 이상 새로 고침할 필요가 없습니다. GFS2 파일 시스템의 크기를 확장하기 위한 전체 절차는 GFS2 파일 시스템 증가를 참조하십시오.

(BZ#1649086)

지원되는 RHEL HA 클러스터의 최대 크기 16개 노드에서 32개 노드로 증가

이번 릴리스에서는 Red Hat은 최대 32개의 전체 클러스터 노드의 클러스터 배포를 지원합니다.

(BZ#1693491)

corosync 링크 추가, 변경 및 제거 명령이 pcs에 추가되었습니다.

이제 Kronosnet(knet) 프로토콜을 사용하여 실행 중인 클러스터에서 knet 링크를 추가하고 제거할 수 있습니다. 이 기능을 지원하기 위해 **pcs** 명령은 knet 링크를 추가, 변경 및 제거하고 기존 클러스터에서 upd/udpu 링크를 변경하는 명령을 제공합니다. 기존 클러스터에서 링크 추가 및 수정에 대한 자세한 내용은 기존 클러스터에서 링크 추가 및 수정을 참조하십시오. (BZ#1667058)

6.1.11. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

새 모듈 스트림: php:7.3

RHEL 8.1에는 여러 가지 새로운 기능과 향상된 기능을 제공하는 **PHP 7.3** 이 도입되었습니다. 주요 변경 사항은 다음과 같습니다.

- 향상되고 더 유연해진 **heredoc** 및 **nowdoc** 구문
- PCRE 확장을 PCRE2로 업그레이드
- 개선된 멀티 바이트 문자열 처리
- LDAP 제어 지원
- FPM(FastCGI Process Manager) 로깅 개선
- 몇 가지 사용 중단 및 이전 버전과 호환되지 않는 변경

자세한 내용은 PHP 7.2.x에서 PHP 7.3.x로 마이그레이션을 참조하십시오.

RHEL 8 버전의 **PHP 7.3** 은 **Argon2** 암호 해싱 알고리즘을 지원하지 않습니다.

php:7.3 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install php:7.3
```

php:7.2 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

(BZ#1653109)

새 모듈 스트림: ruby:2.6

새 모듈 스트림 **ruby:2.6** 을 사용할 수 있습니다. RHEL 8.1에 포함된 **Ruby 2.6.3** 은 RHEL 8.0에 배포된 버전 2.5에 비해 여러 가지 새로운 기능, 개선 사항, 버그 및 보안 수정 사항 및 성능 개선 사항을 제공합니다.

주요 개선 사항은 다음과 같습니다.

- 이제 일정한 이름을 ASCII가 아닌 문자로 시작할 수 있습니다.
- 무한한 범위에 대한 지원이 추가되었습니다.
- 새로운 **Binding#source_location** 메서드가 제공되었습니다.
- 이제 **$SAFE** 는 프로세스 글로벌 상태이며 **0** 으로 다시 설정할 수 있습니다.

다음과 같은 성능 개선이 구현되었습니다.

- **Proc#call** 및 **block.call** 프로세스가 최적화되었습니다.
- 새 가비지 컬렉터에서 heap, Transient heap(**theap**)을 관리했습니다.
- 개별 아키텍처에 대한 기본 코루틴 구현이 도입되었습니다.

또한 **ruby:2.5** 스트림에서 제공하는 **Ruby 2.5** 가 버전 2.5.5로 업그레이드되어 여러 버그 및 보안 수정 사항을 제공합니다.

ruby:2.6 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install ruby:2.6
```

ruby:2.5 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

(BZ#1672575)

새 모듈 스트림: nodejs:12

RHEL 8.1에는 버전 10에 비해 여러 가지 새로운 기능과 향상된 기능을 제공하는 **Node.js 12** 가 도입되었습니다. 주요 변경 사항은 다음과 같습니다.

- V8 엔진이 버전 7.4로 업그레이드
- 새로운 기본 HTTP 구문 분석기, **llhttp** (더 이상 실험적이지 않음)
- 힙 덤프 생성의 통합 기능
- ECMAScript 2015 (ES6) 모듈 지원
- 네이티브 모듈 지원 개선
- 작업자 스레드에는 더 이상 플래그가 필요하지 않습니다.
- 새로운 실험적 진단 보고서 기능
- 성능 향상

nodejs:12 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install nodejs:12
```

nodejs:10 스트림에서 업그레이드하려면 Switching 을 이후 스트림으로 참조하십시오.

(BZ#1685191)

CRB에서 Judy-devel 사용 가능

Judy-devel 패키지는 이제 CRB(CodeReady Linux Builder 리포지토리) 에서 **mariadb-devel:10.3** 모듈의 일부로 사용할 수 있습니다. 결과적으로 개발자는 이제 **Judy** 라이브러리를 사용하여 애플리케이션을 빌드할 수 있습니다.

Judy-devel 패키지를 설치하려면 **mariadb-devel:10.3** 모듈을 먼저 활성화합니다.

```
# yum module enable mariadb-devel:10.3
# yum install Judy-devel
```

(BZ#1657053)

Python 3의 FIPS 준수

이번 업데이트에서는 OpenSSL FIPS 모드 지원이 **Python 3** 에 추가되었습니다. 이름:

- FIPS 모드에서 **blake2**,**sha3** 및 **shake** 해시는 OpenSSL 래퍼를 사용하고 확장된 기능(예: 키, 트리 해시 또는 사용자 지정 다이제스트 크기)을 제공하지 않습니다.
- FIPS 모드에서 **hmac.HMAC** 클래스는 OpenSSL 래퍼 또는 OpenSSL 해시 이름이 있는 문자열을 **digestmod** 인수로만 인스턴스화할 수 있습니다. **md5** 알고리즘에 기본값을 지정하지 않고 인수를 지정해야 합니다.

해시 함수는 OpenSSL FIPS 모드에서 안전하지 않은 해시를 사용할 수 있는 **usedforsecurity** 인수를 지원합니다. 사용자는 모든 관련 표준을 준수할 책임이 있습니다.

(BZ#1731424)

python3-서브스크립트의 FIPS 준수 변경

이번 python3-¢ 패키지 업데이트는 FIPS와 호환되지 않는 데이터를 서명하고 확인하기 위한 기본 구현을 제거합니다.

(BZ#1731526)

새 모듈 스트림: nginx:1.16

버전 1.14에 비해 여러 가지 새로운 기능과 향상된 기능을 제공하는 nginx 1.16 웹 및 프록시 서버를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- **SSL과 관련된 수많은 업데이트(변수의 SSL 인증서 및 비밀 키 로드, ssl_certificate 및 ssl_certificate _key 지시문의 변수 지원, 새 ssl_early_data 지시문)**
- **새로운 keepalive- 관련 지시문**
- **분산 로드 밸런싱을 위한 새로운 random 지시문**
- **새로운 매개변수 및 기존 지시문의 개선 사항(listen 지시문의 포트 범위, limit_req 지시문에 대한 새로운 지연 매개 변수, 2단계 속도 제한 활성화)**
- **새로운 $upstream_bytes_sent 변수**

- UDP(User Datagram Protocol) 프록시 개선

기타 주요 변경 사항은 다음과 같습니다.

- nginx:1.16 스트림에서 nginx 패키지에 nginx -all-modules 패키지가 필요하지 않으므로 nginx 모듈을 명시적으로 설치해야 합니다. nginx 를 모듈로 설치하면 nginx-all-modules 패키지가 기본 프로필인 common 프로필의 일부로 설치됩니다.

- ssl 지시문은 더 이상 사용되지 않습니다. 대신 listen 지시문에 ssl 매개 변수를 사용합니다.

- Nginx 에서 구성 테스트 중에 누락된 SSL 인증서를 탐지합니다.

- listen 지시문에서 호스트 이름을 사용할 때 nginx 는 이제 호스트 이름이 분석하는 모든 주소에 대해 수신 대기 소켓을 생성합니다.

nginx:1.16 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install nginx:1.16
```

nginx:1.14 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

(BZ#1690292)

perl-IO-Socket-SSL 을 2.066 버전으로 업데이트

perl-IO-Socket-SSL 패키지가 버전 2.066으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 예를 들면 다음과 같습니다.

- TLS 1.3 지원 개선, 특히 클라이언트측의 세션 재사용 및 자동 포스트셰이크 인증

- 여러 곡선 지원, 곡선 자동 설정, 부분적인 신뢰 체인 지원, 동일한 도메인에서 RSA 및 ECDSA 인증서 지원 기능 추가

(BZ#1632600)

perl-Net-SSLeay 가 버전 1.88로 업데이트

perl-Net-SSLeay 패키지가 버전 1.88로 업그레이드되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 인증서 스택 및 X509 저장소 조작, 선형 곡선 및 그룹 선택과 같은 OpenSSL 1.1.1과의 호환성 향상
- TLS 1.3과의 호환성 향상(예: 세션 재사용 및 post-handshake 인증)
- cb_data_advanced_put() 서브루틴에서 고정 메모리 누수.

(BZ#1632597)

6.1.12. 컴파일러 및 개발 도구

GCC Toolset 9 사용 가능

Red Hat Enterprise Linux 8.1에는 최신 버전의 개발 툴이 포함된 애플리케이션 스트림인 GCC Toolset 9가 도입되었습니다.

다음 도구와 버전은 GCC Toolset 9에서 제공합니다.

툴	버전
GCC	9.1.1
GDB	8.3
valgrind	3.15.0
SystemTap	4.1
Dyninst	10.1.0

툴	버전
binutils	2.32
elfutils	0.176
dwz	0.12
Make	4.2.1
strace	5.1
ltrace	0.7.91
annobin	8.79

GCC Toolset 9는 **AppStream** 리포지토리의 소프트웨어 컬렉션 형태로 애플리케이션 스트림으로 사용할 수 있습니다. **GCC Toolset**은 **RHEL 7**용 **Red Hat** 개발자 도구 세트와 유사한 도구 집합입니다.

GCC Toolset 9를 설치하려면 다음을 수행합니다.

```
# yum install gcc-toolset-9
```

GCC Toolset 9에서 도구를 실행하려면 다음을 수행합니다.

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

쉘 세션을 실행하려면 **GCC Toolset 9**의 툴 버전이 이러한 툴의 시스템 버전보다 우선합니다.

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

사용법에 대한 자세한 지침은 **GCC Toolset** 사용을 참조하십시오.

(BZ#1685482)

업그레이드된 컴파일러 도구 세트

애플리케이션 스트림으로 배포된 다음 컴파일러 툴 세트가 RHEL 8.1로 업그레이드되었습니다.

- LLVM 컴파일러 인프라 프레임워크, C 및 C++ 언어용 Clang 컴파일러, LLDB 디버거, 코드 분석을 위한 관련 툴을 버전 8.0.1에 제공하는 clang 및 LLVM Toolset
- 사전 빌드 툴과 종속성 관리자 , 필수 라이브러리를 버전 1.37에 제공하는 toolet
- Go(golang) 프로그래밍 언어 도구 및 라이브러리를 버전 1.12.8에 제공하는 Go 도구 세트.

(BZ#1731502, BZ#1691975, BZ#1680091, BZ#1677819, BZ#1681643)

SystemTap 버전 4.1로 업데이트

SystemTap 계측 툴이 업스트림 버전 4.1로 업데이트되었습니다. 주요 개선사항은 다음과 같습니다.

- eBPF 런타임 백엔드는 문자열 변수 및 풍부한 형식의 인쇄와 같은 스크립팅 언어의 추가 기능을 처리할 수 있습니다.
- 변환기의 성능이 크게 향상되었습니다.
- 이제 DWARF4 debuginfo 구문을 사용하여 최적화된 C 코드의 더 많은 데이터 유형을 추출할 수 있습니다.

(BZ#1675740)

DHAT 툴의 GA

Red Hat Enterprise Linux 8.1은 DHAT 툴의 GA를 도입했습니다. valgrind 툴 버전 3.15.0을 기반으로 합니다.

아래의 valgrind 툴 기능에서 변경 사항/부충 사항을 확인할 수 있습니다.

- *--tool= exp-dhat 대신 --tool=dhat* 를 사용합니다.

- *--show-top-n* 및 *--sort-by* 옵션이 제거되었습니다. dhat 툴은 이제 프로그램이 종료된 후 최소 데이터를 인쇄하기 때문에 제거되었습니다.

- JavaScript 프로그램인 새로운 뷰어 dh_view.html 에는 프로필 결과가 포함되어 있습니다. 짧은 메시지는 실행이 종료된 후 결과를 보는 방법을 설명합니다.

- 뷰어 설명서는 */usr/libexec/valgrind/dh_view.html에 있습니다.*

- DHAT 툴에 대한 설명서는 */usr/share/doc/valgrind/html/dh-manual.html에 있습니다.*

- amd64(x86_64) 지원: RDRAND 및 F16C insn 세트 확장 기능이 추가되었습니다.

- cachegrind 에서 cg_annotate 명령에는 모든 이벤트 수 옆에 백분율을 출력하는 *--show-percs* 옵션이 있습니다.

- callgrind _annotate 명령에는 모든 이벤트 수 옆에 백분율을 출력하는 새로운 옵션인 *--show-percs* 가 있습니다.

- *--read-inline-info* 의 기본값이 yes이면 이제 yes 가 됩니다.

- x *tree 형식의 누수 결과를 출력하는 memcheck 옵션 --xtree* -leak=yes 에서 *--show-leak-kinds=all* 옵션을 자동으로 활성화합니다.

- 새로운 옵션 *--show-error-list=no|yes* 는 탐지된 오류 목록과 실행이 끝나면 사용된 억제를 표시합니다. 이전에는 valgrind 명령에 *-v* 옵션을 지정할 수 있었습니다. 이로 인해 혼동을 일으킬 수 있는 많은 정보를 확인할 수 있었습니다. 옵션은 *--show-error-list=yes* 옵션과 *동일합니다.*

(BZ#1683715)

elfutils를 버전 0.176으로 다시 기반

elfutils 패키지가 업스트림 버전 **0.176**으로 업데이트되었습니다. 이 버전은 다양한 버그 수정을 제공하고 다음 취약점을 해결합니다.

- CVE-2019-7146
- CVE-2019-7149
- CVE-2019-7150
- CVE-2019-7664
- CVE-2019-7665

주요 개선사항은 다음과 같습니다.

- **libdw** 라이브러리는 압축 파일을 처리하는 **elf _begin()**의 변형인 **dfirmf_elf _begin()** 함수를 통해 확장되었습니다.
- 새로운 **--reloc-debug-sections-only** 옵션이 다른 제거 없이 디버그 섹션 간의 모든 간단한 재배치를 해결하기 위해 **eu-strip** 툴에 추가되었습니다. 이 기능은 특정 상황에서 **ET_REL** 파일에만 관련이 있습니다.

(BZ#1683705)

glibc에서 추가 메모리 할당 검사

애플리케이션 메모리 손상은 애플리케이션 및 보안 결함의 주요 원인입니다. 이러한 손상을 조기 감지하여 탐지 비용과 균형을 이루면 애플리케이션 개발자에게 상당한 이점을 제공할 수 있습니다.

탐지 기능을 개선하기 위해 **RHEL**의 핵심 **C** 라이브러리인 **GNU C** 라이브러리(**Glibc**)의 **idle oc** 메타데이터에 **6**개의 추가 메모리 손상 검사가 추가되었습니다. 이러한 추가 검사는 런타임 성능에 매우 낮은 비용으로 추가되었습니다.

(BZ#1651283)

GDB는 더 많은 POWER8 레지스터에 액세스할 수 있습니다.

이번 업데이트를 통해 GDB(GNU 디버거) 및 원격 스텁 gdbserver 는 다음과 같은 추가 레지스터에 액세스하고 IBM의 POWER8 프로세서 라인의 레지스터 세트에 액세스할 수 있습니다.

- PPR
- DSCR
- TAR
- EBB/PMU
- HTM

(BZ#1187581)

binutils disassemble r는 N개의 바이너리 파일을 처리할 수 있습니다.

binutils 패키지의 disassembler 툴이 NFS(Netronome Flow Processor) 하드웨어 시리즈의 바이너리 파일을 처리하도록 확장되었습니다. 이 기능은 bpftool Berkeley Packet Filter(BPF) 코드 컴파일러에서 추가 기능을 활성화하는 데 필요합니다.

(BZ#1644391)

IBM Z 아키텍처에서 부분적으로 쓰기 가능한 GOT 섹션 지원

로더의 "lazy 바인딩" 기능을 사용하는 IBM Z 바이너리는 부분적으로 쓰기 가능한 GOT(Global offset table) 섹션을 생성하여 강화할 수 있습니다. 이러한 바이너리에는 읽기-쓰기 GOT가 필요하지만 모든 항목을 쓸 수 있는 것은 아닙니다. 이번 업데이트에서는 잠재적인 공격으로부터 항목을 보호합니다.

(BZ#1525406)

binutils 에서 IBM Z의 Arch13 프로세서 지원

이번 업데이트에서는 Arch13 프로세서와 관련된 확장 기능을 IBM Z 아키텍처의 binutils 패키지에 추가로 지원합니다. 결과적으로 IBM Z의 arch13 지원 CPU에서 사용할 수 있는 기능을 사용할 수 있는 커널을 구축할 수 있습니다.

(BZ#1659437)

Dyninst 가 버전 10.1.0으로 업데이트

Dyninst 계측 라이브러리가 업스트림 버전 10.1.0으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- Dyninst는 Linux PowerPC Little Endian(ppcle) 및 64비트 ARM(aarch64)아키텍처를 지원합니다.
- 병렬 코드 분석을 사용하여 시작 시간이 향상되었습니다.

(BZ#1648441)

일본어 Reiwa 기간의 업데이트 포맷 날짜

GNU C 라이브러리는 이제 2019년 5월 1일부터 Reiwa 시대를 위한 올바른 일본어 시대 이름 포맷을 제공합니다. strftime 및 strptime 함수에서 사용하는 데이터를 포함하여 API 데이터 처리 시간이 업데이트되었습니다. 모든 API는 %EC, %EY 또는 % Ey 와 같은 시대 변환 지정자 중 하나와 함께 strftime 을 사용하는 경우를 포함하여 Reiwa 시대를 올바르게 인쇄합니다.

(BZ#1577438)

Performance Co-Pilot이 버전 4.3.2로 업데이트

RHEL 8.1에서는 PCP(Performance Co-Pilot) 툴이 업스트림 버전 4.3.2로 업데이트되었습니다. 주요 개선사항은 다음과 같습니다.

- Linux 커널 엔트로피, 부하 정체 정보, Nvidia GPU 통계 등 새로운 지표가 추가되었습니다.
- pcp-dstat,pcp-atop, perfevent PMDA 등의 툴이 새 지표를 보고하도록 업데이트되었습니

다.

- Grafana와 고성능 PCP 통합을 위한 pmseries 및 pmproxy 유틸리티가 업데이트되었습니다.

이 릴리스는 라이브러리, 유선 프로토콜 및 디스크 PCP 아카이브 형식과 이전 버전과 호환됩니다.

(BZ#1685302)

6.1.13. IdM (Identity Management)

IdM에서 설치 및 관리를 위한 Ansible 역할 및 모듈 지원

이번 업데이트에서는 IdM(Identity Management) 배포 및 관리를 위한 Ansible 역할 및 모듈을 제공하는 ansible-freeipa 패키지가 도입되었습니다. Ansible 역할을 사용하여 IdM 서버, 복제본 및 클라이언트를 설치 및 제거할 수 있습니다. Ansible 모듈을 사용하여 IdM 그룹, 토폴로지 및 사용자를 관리할 수 있습니다. 사용 가능한 예제 플레이북도 있습니다.

이 업데이트는 IdM 기반 솔루션의 설치 및 구성을 간소화합니다.

(JIRA:RHELPLAN-2542)

IdM 배포의 전반적인 적합성을 테스트하는 새로운 도구는 다음과 같습니다. 상태 점검

이번 업데이트에서는 IdM(Identity Management)의 Healthcheck 도구가 도입되었습니다. 툴에서는 현재 IdM 서버가 올바르게 구성되고 실행되고 있는지 확인하는 테스트를 제공합니다.

현재 적용되는 주요 영역은 * 인증서 구성 및 만료일 * 복제 오류 * 복제 토폴로지 * AD Trust 구성 * 서비스 상태 * 중요한 구성 파일의 파일 권한 * 파일 시스템 공간

Healthcheck 도구는 CLI(명령줄 인터페이스)에서 사용할 수 있습니다.

(JIRA:RHELPLAN-13066)

서버가 오프라인 상태일 때 IdM에서 만료된 시스템 인증서 갱신 지원

이 향상된 기능을 통해 IdM(Identity Management)이 오프라인 상태일 때 관리자가 만료된 시스템 인증서를 갱신할 수 있습니다. 시스템 인증서가 만료되면 IdM이 시작되지 않습니다. 새로운 ipa-cert-fix 명령은 갱신 프로세스를 진행하도록 날짜를 수동으로 설정하기 위한 해결방법을 대체합니다. 따라서 언급된 시나리오에서는 다운타임 및 지원 비용이 줄어듭니다.

(JIRA:RHELPLAN-13074)

ID 관리는 Windows Server 2019를 통한 신뢰를 지원합니다.

Identity Management를 사용하면 이제 Windows Server 2019에서 실행되는 Active Directory 포리스트에 지원되는 포리스트 신뢰성을 설정할 수 있습니다. 지원되는 포리스트 및 도메인 기능 수준은 변경되지 않았으며 최대 Windows Server 2016까지 지원됩니다.

(JIRA:RHELPLAN-15036)

Samba 기반 버전 4.10.4

samba 패키지가 업스트림 버전 4.10.4로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- Samba 4.10은 Python 3을 완벽하게 지원합니다. 향후 Samba 버전에는 Python 2에 대한 런타임 지원이 제공되지 않습니다.
- JSON(JavaScript Object Notation) 로깅 기능은 인증 메시지에 대한 Windows 이벤트 ID 및 로그온 유형을 기록합니다.
- FUSE(사용자 공간) 모듈의 새로운 vfs_glusterfs_fuse 파일 시스템은 Samba가 GlusterFS 볼륨에 액세스할 때 성능을 향상시킵니다. 이 모듈을 활성화하려면 glusterfs_fuse 를 /etc/samba/smb.conf 파일에 있는 공유의 vfs_objects 매개 변수에 추가합니다. vfs_glusterfs_fuse 는 기존 vfs_glusterfs 모듈을 대체하지 않습니다.
- 이제 서버 메시지 블록(SMB) 클라이언트 Python 바인딩이 더 이상 사용되지 않으며 향후 Samba 릴리스에서 제거됩니다. 이는 Samba Python 바인딩을 사용하여 자체 유틸리티를 작성하는 사용자에게만 영향을 미칩니다.

smbd,nmbd 또는 winbind 서비스가 시작될 때 Samba는 tdb 데이터베이스 파일을 자동으로 업데이트합니다. Samba를 시작하기 전에 데이터베이스 파일을 백업합니다. Red Hat은 tdb 데이터베이스 파일

다운그레이드를 지원하지 않습니다.

주요 변경 사항에 대한 자세한 내용은 업데이트하기 전에 업스트림 릴리스 노트를 참조하십시오. https://www.samba.org/samba/history/samba-4.10.0.html

(BZ#1638001)

OpenLDAP에 대한 시스템 전체 인증서 저장소 위치 업데이트

OpenLDAP의 신뢰할 수 있는 CA의 기본 위치는/etc/ openldap/certs 대신 시스템 전체 인증서 저장소(/etc/pki/ca-trust/ source)를 사용하도록 업데이트되었습니다. 이 변경은 CA 신뢰의 설정을 간소화하기 위해 만들어졌습니다.

서비스별 요구 사항이 없으면 CA 트러스트를 설정하는 데 추가 설정이 필요하지 않습니다. 예를 들어 LDAP 클라이언트 연결에서만 LDAP 서버의 인증서를 신뢰해야 하는 경우 이 경우 이전에 CA 인증서를 설정해야 합니다.

(JIRA:RHELPLAN-7109)

IdM CRL 마스터 관리를 간소화하기 위해 새로운 ipa-crl-generation 명령이 도입되었습니다.

이번 업데이트에서는 ipa-crl-generation status/enable/disable 명령이 도입되었습니다. 이러한 명령은 root 사용자가 실행하고 IdM의 CRL(인증서 폐기 목록)으로 작업을 간소화합니다. 이전에는 CRL 생성 마스터를 한 IdM CA 서버에서 다른 서버로 이동하는 것은 길고 오류가 발생하기 쉬운 절차였습니다.

ipa-crl-generation status 명령은 현재 호스트가 CRL 생성 마스터인지 확인합니다. 현재 호스트가 IdM CA 서버인 경우 ipa-crl-generation enable 명령은 현재 호스트를 IdM의 CRL 생성 마스터로 만듭니다. ipa-crl-generation disable 명령은 현재 호스트에서 CRL 생성을 중지합니다.

또한 ipa-server-install --uninstall 명령에는 이제 호스트가 CRL 생성 마스터인지 여부를 확인합니다. 이 방법으로 IdM은 시스템 관리자가 토폴로지에서 CRL 생성 마스터를 제거하지 않도록 합니다.

(JIRA:RHELPLAN-13068)

keycloak-httpd-client-install에서 OpenID Connect 지원

keycloak-httpd-client-install ID 프로바이더는 이전에 mod_auth_mellon 인증 모듈을 사용하여 SAML(Security Assertion Markup Language) 인증만 지원했습니다. 이 리베이스에는 OpenID

Connect 인증 인증도 구성할 수 있는 mod_auth_openidc 인증 모듈 지원이 도입되었습니다.

keycloak-httpd-client-install ID 프로바이더를 사용하면 mod_auth_openidc 를 구성하여 apache 인스턴스를 OpenID Connect 클라이언트로 구성할 수 있습니다.

(BZ#1553890)

숨겨진 복제본으로 IdM을 기술 프리뷰로 설정할 수 있습니다

이 향상된 기능을 통해 관리자는 IdM(Identity Management) 복제본을 숨겨진 복제본으로 설정할 수 있습니다. 숨겨진 복제본은 모든 서비스가 실행 중이고 사용 가능한 IdM 서버입니다. 그러나 DNS의 서비스에 대한 SRV 레코드가 없고 LDAP 서버 역할이 활성화되어 있지 않으므로 다른 클라이언트 또는 마스터에 알리지 않습니다. 따라서 클라이언트는 서비스 검색을 사용하여 숨겨진 복제본을 탐지할 수 없습니다.

숨겨진 복제본은 주로 클라이언트를 중단할 수 있는 전용 서비스용으로 설계되었습니다. 예를 들어 IdM의 전체 백업은 마스터 또는 복제본의 모든 IdM 서비스를 종료해야 합니다. 숨겨진 복제본을 사용하지 않으므로 관리자는 클라이언트에 영향을 주지 않고 이 호스트의 서비스를 일시적으로 종료할 수 있습니다. 다른 사용 사례에는 IdM API 또는 LDAP 서버의 높은 로드 작업(예: 대량 가져오기 또는 포괄적인 쿼리)이 포함됩니다.

숨겨진 새 복제본을 설치하려면 ipa-replica-install --hidden-replica 명령을 사용합니다. 기존 복제본의 상태를 변경하려면 ipa server-state 명령을 사용합니다.

(BZ#1719767)

SSSD에서 기본적으로 AD GPO 적용

이제 SSSD 옵션 ad_gpo_access_control 의 기본 설정이 강제 적용됩니다. RHEL 8에서 SSSD는 기본적으로 Active Directory Group Policy Objects(GPO)를 기반으로 액세스 제어 규칙을 적용합니다.

RHEL 7에서 RHEL 8로 업그레이드하기 전에 Active Directory에 GPO가 올바르게 구성되었는지 확인하는 것이 좋습니다. GPO를 적용하지 않으려면 /etc/sssd/sssd.conf 파일의 ad_gpo_access_control 옵션 값을 허용 으로 변경합니다.

(JIRA:RHELPLAN-51289)

6.1.14. 데스크탑

GNOME Classic에서 수정된 작업 공간 전환기

GNOME Classic 환경의 작업 공간 전환기가 수정되었습니다. 스위터는 이제 아래쪽 막대의 오른쪽 부분에 위치하며 수평면 패널로 설계되었습니다. 필요한 축소판 이미지를 클릭하면 작업 영역 간 전환이 가능합니다. 또는 **Ctrl+Alt+**아래쪽/위 화살표 키의 조합을 사용하여 작업 영역 간에 전환할 수도 있습니다. 활성 작업 공간의 내용은 *창 목록 형태로 하단 표시줄의 왼쪽 부분에 표시됩니다*.

특정 작업 영역에서 **Super** 키를 누르면 이 작업 영역에서 열려 있는 모든 *창이 포함된 창 선택기* 가 표시됩니다. 그러나 *창 선택기에*는 이전 **RHEL** 릴리스에서 사용 가능한 다음 요소가 더 이상 표시되지 않습니다.

- *접두어* (화면 왼쪽에 있는 정형 막대)
- *작업 공간 전환기* (화면 오른쪽에 있는 정형 막대)
- *검색 항목*

이러한 요소의 도움을 통해 이전에 달성한 특정 작업의 경우 다음과 같은 방법을 채택하십시오.

- 애플리케이션을 시작하려면 *다음을* 수행할 수 있습니다.
  - 상단 표시줄에서 **Applications** 메뉴 사용
  - **kdb:[Alt + F2]** 키를 눌러 **Enter a Command** (명령 입력) 화면을 표시하고 실행 파일의 이름을 이 화면에 작성합니다.
- 수직 작업 공간 *스위처를 사용하는 대신 작업 영역* 간에 전환하려면 오른쪽 하단 표시줄에서 수평 *작업 공간 전환기* 를 사용합니다.
- *검색 항목* 또는 수직 *작업 영역 전환기* 가 필요한 경우 **GNOME Classic** 대신 **GNOME Standard** 환경을 사용합니다.

(**BZ#1704360**)

6.1.15. 그래픽 인프라

부트 스트랩에서 Linux 커널 버전 5.1로 업데이트

DRM(Direct Rendering Manager) 커널 그래픽 하위 시스템은 업스트림 Linux 커널 버전 5.1로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 가장 중요한 것은 다음과 같습니다.

- mgag200 드라이버가 업데이트되었습니다. 드라이버는 Matrox G200 eH3 GPU를 사용하는 HPE Proliant Gen10 Systems에 대한 지원을 계속 제공합니다. 업데이트된 드라이버는 현재 및 새로운 Dell EMC PowerEdge 서버도 지원합니다.
- NVIDIA GPU를 사용하는 현재 및 향후 Lenovo 플랫폼에 하드웨어 기능을 제공하도록 no½ 드라이버가 업데이트되었습니다.
- 현재 및 새 Intel GPU를 지속적으로 지원하도록 i915 디스플레이 드라이버가 업데이트되었습니다.
- Aspeed AST BMC 디스플레이 칩에 대한 버그 수정이 추가되었습니다.
- AMD Raven 2 세트의 AMQP(Acccelerated Processing Units) 지원이 추가되었습니다.
- AMD Picasso APU에 대한 지원이 추가되었습니다.
- AMD Vega GPU 지원이 추가되었습니다.
- Intel Amber Lake-Y 및 Intel¢t Lake-U GPU에 대한 지원이 추가되었습니다.

(BZ#1685552)

AMD Picasso 그래픽 카드 지원

이번 업데이트에서는 amdgpu 그래픽 드라이버가 도입되었습니다. 그 결과 이제 RHEL 8에서 AMD Picasso 그래픽 카드가 완전히 지원됩니다.

(BZ#1685427)

6.1.16. 웹 콘솔

SMT 활성화 및 비활성화

RHEL 8에서는 동시 SMT(Multi-Threading) 구성을 사용할 수 있습니다. 웹 콘솔에서 SMT를 비활성화하면 다음과 같은 CPU 보안 취약점 클래스를 완화할 수 있습니다.

- Microarchitectural Data Sampling
- L1 터미널 오류 공격

(BZ#1678956)

서비스 페이지에 검색 상자 추가

이제 Services 페이지에 다음과 같이 서비스를 필터링하기 위한 검색 상자가 있습니다.

- 이름
- 설명
- 상태

또한 서비스 상태가 하나의 목록으로 병합되었습니다. 페이지 상단에 있는 전환기 버튼도 Services (서비스) 페이지의 사용자 환경을 개선하기 위해 탭으로 변경되었습니다.

(BZ#1657752)

방화벽 영역에 대한 지원 추가

Networking 페이지의 방화벽 설정에서 다음을 지원합니다.

- 영역 추가 및 제거
- 임의의 영역에 서비스 추가 또는 제거
- **firewalld** 서비스 외에 사용자 지정 포트 구성.

(**BZ#1678473**)

가상 머신 구성 개선 사항 추가

이번 업데이트를 통해 **RHEL 8** 웹 콘솔에는 **Virtual Machines**(가상 시스템) 페이지에 많은 개선 사항이 포함되어 있습니다. 이제 다음을 수행할 수 있습니다.

- 다양한 유형의 스토리지 풀 관리
- **VM** 자동 시작 구성
- 기존 **qcow** 이미지 가져오기
- **PXE** 부팅을 통해 **VM** 설치
- 메모리 할당 변경
- 가상 머신 일시 중지/재개
- 캐시 특성 구성(**directsync, writeback**)
- 부팅 순서 변경

(BZ#1658847)

6.1.17. Red Hat Enterprise Linux 시스템 역할

RHEL 시스템 역할에 추가된 새로운 스토리지 역할

스토리지 역할은 **rhel-system-roles** 패키지에서 제공하는 **RHEL** 시스템 역할에 추가되었습니다. 스토리지 역할은 **Ansible**을 사용하여 로컬 스토리지를 관리하는 데 사용할 수 있습니다.

현재 스토리지 역할은 다음과 같은 유형의 작업을 지원합니다.

- 전체 디스크에서 파일 시스템 관리
- **LVM** 볼륨 그룹 관리
- 논리 볼륨 및 파일 시스템 관리

자세한 내용은 파일 시스템 관리 및 논리 볼륨 구성 및 관리를 참조하십시오.

(BZ#1691966)

6.1.18. 가상화

WALinuxAgent **가 2.2.38 버전으로 업데이트**

WALinuxAgent 패키지가 업스트림 버전 **2.2.38**로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

또한 ***WALinuxAgent*** 는 **Python 2**와 더 이상 호환되지 않으며 애플리케이션은 **Python 2**에 의존합니다. 결과적으로 ***WALinuxAgent*** 과의 호환성을 구축하기 위해 **Python 2**에서 작성된 애플리케이션과 확장 기능을 **Python 3**으로 변환해야 합니다.

(BZ#1722848)

Windows는 필요한 virtio-win 드라이버를 자동으로 찾습니다.

이제 Windows는 사용자가 위치한 폴더를 선택할 필요 없이 드라이버 ISO에서 필요한 virtio-win 드라이버를 자동으로 찾을 수 있습니다.

(BZ#1223668)

KVM이 5 레벨 페이징 지원

Red Hat Enterprise Linux 8을 통해 KVM 가상화는 5단계 페이징 기능을 지원합니다. 선택한 호스트 CPU에서 호스트 및 게스트 시스템에서 사용할 수 있는 실제 및 가상 주소 공간이 크게 증가합니다.

(BZ#1526548)

ActivClient 드라이버를 사용하여 Windows 게스트에서 스마트 카드 공유 지원

이번 업데이트에서는 Windows 게스트 OS 및 ActivClient 드라이버를 사용하는 VM(가상 머신)의 스마트 카드 공유를 지원합니다. 이는 이러한 VM에서 에뮬레이트된 또는 공유 스마트 카드를 사용하여 사용자 로그인에 대한 스마트 카드 인증을 활성화합니다.

(BZ#1615840)

virt-xml에 대한 새로운 옵션이 추가되었습니다

virt-xml 유틸리티는 이제 다음 명령줄 옵션을 사용할 수 있습니다.

- --no-define - virt-xml 명령에 의해 VM(가상 머신)에 대한 변경 사항은 영구 구성에 저장되지 않습니다.
- --start - 요청된 변경을 수행한 후 VM을 시작합니다.

이 두 옵션을 함께 사용하면 사용자가 VM 구성을 변경하고 변경 사항을 영구적으로 만들지 않고도 새 구성으로 VM을 시작할 수 있습니다. 예를 들어 다음 명령은 다음 부팅을 위해 *testguest* VM의 부팅 순서를 네트워크로 변경하고 부팅을 시작합니다.

```
virt-xml testguest  --start --no-define --edit --boot network
```

(JIRA:RHELPLAN-13960)

KVM에서 지원하는 IBM z14 GA2 CPU

이번 업데이트를 통해 KVM은 IBM z14 GA2 CPU 모델을 지원합니다. 따라서 RHEL 8을 게스트의 IBM z14 GA2 CPU가 있는 호스트 OS로 사용하는 IBM z14 GA2 호스트에서 가상 시스템을 생성할 수 있습니다.

(JIRA:RHELPLAN-13649)

NVIDIA NVLink2가 IBM POWER9의 가상 머신과 호환 가능

NVLink2 기능을 지원하는 NVIDIA VGPU를 이제 IBM POWER9 시스템의 RHEL 8 호스트에서 실행 중인 VM(가상 머신)에 할당할 수 있습니다. 이렇게 하면 해당 VM이 NVLink2의 전체 성능 잠재력을 사용할 수 있습니다.

(JIRA:RHELPLAN-12811)

6.2. 새 드라이버

네트워크 드라이버

- 직렬 라인 인터넷 프로토콜 지원 (slip.ko.xz)
- C_CAN 컨트롤러용 플랫폼 JDK 버스 드라이버 (c_can_platform.ko.xz)
- 가상 CentOS 인터페이스 (vcan.ko.xz)
- DPRAM DPRAM 드라이버 (softing.ko.xz)
- 직렬 회선 인터페이스 (slcan.ko.xz)
- 제이보스 박사를 위한 피사 드라이버. Thomas Wuensche 0.0/DVD 인터페이스 (ems_usb.ko.xz)

- esdCAN-jpg/2 및CAN-jpg/Micro 인터페이스용 JDK 드라이버 (esd_usb2.ko.xz)
- 플랫폼 버스에서 SJA1000용 소켓-CA 드라이버(sja1000_platform.ko.xz)
- SJA1000 칩(plx_pci.ko.xz)을 장착한 PCI-bridge 카드용 소켓-CA 드라이버
- CPC-PCI/PCIe/104P용 소켓-카운트 드라이버(ems_pci.ko.xz)
- KVASER PCAN PCI 카드용 소켓 기반 드라이버(kvaser_pci.ko.xz)
- Intel® 2.5G 이더넷 Linux 드라이버(igc.ko.xz)
- Realtek 802.11ac 무선 PCI 드라이버 (rtwpci.ko.xz)
- Realtek 802.11ac 무선 코어 모듈 (rtw88.ko.xz)
- MediaTek MT76 장치 지원 (mt76.ko.xz)
- MediaTek MT76x0U () 지원 (mt76x0u.ko.xz)
- MediaTek MT76x2U () 지원 (mt76x2u.ko.xz)

그래픽 드라이버 및 기타 드라이버

- 가상 커널 모드 설정 (vkms.ko.xz)
- Intel GTT (Graphics Translation Table) 루틴 (intel-gtt.ko.xz)
- Xen frontend/backend 페이지 디렉토리 공유 버퍼 처리 (xen-front-pgdir-shbuf.ko.xz)

- 오디오 음소거 컨트롤을 위한 **pvc** 트리거 **(ledtrig-audio.ko.xz)**
- 호스트 어댑터 라디오 제어 드라이버 **(hwa-rc.ko.xz)**
- 네트워크 블록 장치 **(nbd.ko.xz)**
- **Pericom330532 Type-C mux** 드라이버 **(pi3usb30532.ko.xz)**
- **Fairchild F302 Type-Cœ Driver (fusb302.ko.xz)**
- **TI TPS6598x USB Power Delivery Controller Driver (tps6598x.ko.xz)**
- **Intel PCH Thermal** 드라이버 **(intel_pch_thermal.ko.xz)**
- **PCIe AER** 소프트웨어 오류 인젝터 **(aer_inject.ko.xz)**
- **PCI SR-IOV PF** 장치 용 간단한 스텁 드라이버 **(pci-pf-stub.ko.xz)**
- **mISDN DigitalSDN Processing** 지원 **(mISDN_dsp.ko.xz)**
- **ISDN** 계층 **1** 컬렉션 **HFC-4S/8S** 칩 **(hfc4s8s_l1.ko.xz)**
- **ISDN4Linux:** 전환 지원 호출 **(dss1_divert.ko.xz)**
- **CAPI4Linux:** 사용자 공간 **/dev/capi20** 인터페이스 **(capi.ko.xz)**
- **Gigaset 307x**용 **USB** 드라이버 **(bas_gigaset.ko.xz)**

- **ISDN4Linux: HYSDN 카드 드라이버 (hysdn.ko.xz)**
- **mISDN DigitalSDN Processing 지원 (mISDN_dsp.ko.xz)**
- **Winbond w6692 기반 카드용 mISDN 드라이버 (w6692.ko.xz)**
- **CCD의 hfc-pci 기반 카드용 mISDN 드라이버 (hfcpci.ko.xz)**
- **hfc-4s/hfc-8s/hfc-e1 기반 카드용 mISDN 드라이버 (hfcmulti.ko.xz)**
- **NETJet용 mISDN 드라이버(netowned.ko.xz)**
- **AVM RAWITZ용 mISDN 드라이버!CARD PCI ISDN 카드 (avmfritz.ko.xz)**

스토리지 드라이버

- **Fabrics TCP 호스트(nvme-tcp.ko.xz)를 통한 NVMe**
- **Fabrics TCP 대상의 NVMe(nvmet-tcp.ko.xz)**
- **device-mapper writecache 대상 (dm-writecache.ko.xz)**

6.3. 업데이트된 드라이버

네트워크 드라이버 업데이트

- **Qlogic FastLinQ 4xxxx 이더넷 드라이버(qede.ko.xz)가 8.37.0.20 버전으로 업데이트되었습니다.**
- **Qlogic FastLinQ 4xxxx 코어 모듈(qed.ko.xz)이 8.37.0.20 버전으로 업데이트되었습니다.**
- **Broadcom BCM573xx 네트워크 드라이버(bnxt_en.ko.xz)가 버전 1.10.0으로 업데이트되었**

습니다.

- Qlogic BCM57710/57711/57711E/57712/57712_MF/57800/57800_MF/57810/57810_MF/57840/57840_MF 드라이버(bnx2x.ko.xz)가 버전 1.713.36-0으로 업데이트되었습니다.

- Intel® 기가비트 이더넷 네트워크 드라이버(igb.ko.xz)가 5.6.0-k 버전으로 업데이트되었습니다.

- Intel® 10 기가비트 가상 기능 네트워크 드라이버(ixgbevf.ko.xz)가 버전 4.1.0-k-rh8.1.0으로 업데이트되었습니다.

- Intel® 10 기가비트 PCI Express 네트워크 드라이버(ixgbe.ko.xz)가 버전 5.1.0-k-rh8.1.0으로 업데이트되었습니다.

- Intel® Ethernet Switch Host Interface Driver(fm10k.ko.xz)가 버전 0.26.1-k로 업데이트되었습니다.

- Intel® Ethernet Connection E800 Series Linux Driver(ice.ko.xz)가 0.2.4-k 버전으로 업데이트되었습니다.

- Intel® Ethernet Connection710 Network Driver(i40e.ko.xz)가 버전 2.8.20-k로 업데이트되었습니다.

- NFS(Netronome Flow Processor) 드라이버(nfp.ko.xz)가 4.18.0-147.el8.x86_64로 업데이트되었습니다.

- EA(Elastic Network Adapter)(ena.ko.xz)가 버전 2.0.3K로 업데이트되었습니다.

그래픽 및 기타 드라이버 업데이트

- VMware SVGA 장치(vmwgfx.ko.xz)용 독립형 drm 드라이버가 버전 2.15.0.0으로 업데이트되었습니다.

- **HPE 워치독 드라이버(hpwdt.ko.xz)가 버전 2.0.2로 업데이트되었습니다.**

스토리지 드라이버 업데이트

- **HP Smart Array Controller 버전 3.4.20-170-RH3(hpsa.ko.xz)의 드라이버가 버전 3.4.20-170-RH3으로 업데이트되었습니다.**

- **LSI MPT Fusion SAS 3.0 장치 드라이버(mpt3sas.ko.xz)가 버전 28.100.00.00으로 업데이트되었습니다.**

- **Emulex LightPulse Fibre Channel SCSI 드라이버 12.2.0.3 (lpfc.ko.xz)이 버전 0:12.2.0.3으로 업데이트되었습니다.**

- **Qlogic QEDF 25/40/50/100Gb FCoE Driver(qedf.ko.xz)가 버전 8.37.25.20으로 업데이트되었습니다.**

- **Cisco FCoE HBA Driver(fnic.ko.xz)가 버전 1.6.0.47로 업데이트되었습니다.**

- **Qlogic 파이버 채널 HBA 드라이버(qla2xxx.ko.xz)가 버전 10.01.00.15.08.1-k1로 업데이트되었습니다.**

- **Microsemi Smart Family Controller 버전 1.2.6-015(smartpqi.ko.xz)의 드라이버가 버전 1.2.6-015로 업데이트되었습니다.**

- **Qlogic FastLinQ 4xxxx iSCSI 모듈(qedi.ko.xz)이 8.33.0.21 버전으로 업데이트되었습니다.**

- **BroadcomRAID SAS Driver(megaraid_sas.ko.xz)가 07.707.51.00-rc1 버전으로 업데이트되었습니다.**

6.4. 버그 수정

이 부분에서는 사용자에게 중요한 영향을 미치는 **Red Hat Enterprise Linux 8.1**의 버그에 대해 설명합니다.

6.4.1. 설치 프로그램 및 이미지 생성

버전 또는 inst.version 커널 부팅 매개변수를 사용하면 더 이상 설치 프로그램이 중지되지 않습니다.

이전에는 버전 또는 inst.version 부팅 매개 변수를 사용하여 커널 명령줄에서 설치 프로그램을 부팅하는 경우 버전이 출력되었습니다 (예: anaconda 30.25.6).

이번 업데이트를 통해 설치 프로그램이 커널 명령줄에서 부팅될 때 version 및 inst.version 매개 변수가 무시되므로 설치 프로그램이 중지되지 않습니다.

(BZ#1637472)

xorg-x11-drv-fbdev,xorg-x11-drv-vesa 및 xorg-x11-drv-vmware 비디오 드라이버는 기본적으로 설치됩니다.

이전에는 특정 AMD 가속화 처리 장치가 있는 NVIDIA 그래픽 카드 및 워크스테이션 모델이 있는 워크스테이션에서 RHEL 8.0 서버를 설치한 후 그래픽 로그인 창을 표시하지 않았습니다. 이 문제는 Hyper-V와 같은 그래픽 지원을 위해 EFI에 의존하는 가상 시스템도 영향을 받았습니다. 이번 업데이트를 통해 xorg-x11-drv-fbdev,xorg-x11-drv-vesa 및 xorg-x11-drv-vmware 비디오 드라이버가 기본적으로 설치되고 RHEL 8.0 이상 서버 설치 후 그래픽 로그인 창이 표시됩니다.

(BZ#1687489)

오류 메시지를 표시하지 않고 복구 모드가 더 이상 실패하지 않습니다

이전 버전에서는 Linux 파티션이 없는 시스템에서 복구 모드를 실행하여 설치 프로그램이 예외로 실패했습니다. 이번 업데이트를 통해 Linux 파티션이 없는 시스템이 감지되면 설치 프로그램에 "Linux 파티션이 없습니다" 오류 메시지가 표시됩니다.

(BZ#1628653)

설치 프로그램에서 이미지 설치에 대한 lvm_metadata_backup Blivet 플래그를 설정합니다.

이전에는 설치 프로그램에서 이미지 설치에 대한 lvm_metadata_backup Blivet 플래그를 설정하지 못했습니다. 결과적으로 LVM 백업 파일은 이미지 설치 후 /etc/lvm/ 하위 디렉터리에 있었습니다. 이번 업데이트를 통해 설치 프로그램에서 lvm_metadata_backup Blivet 플래그를 설정하므로 이미지 설치 후 /etc/lvm/ 하위 디렉터리에 LVM 백업 파일이 없습니다.

(BZ#1673901)

RHEL 8 설치 프로그램은 RPM의 문자열을 처리

이전에는 python3-rpm 라이브러리에서 문자열을 반환할 때 설치 프로그램이 예외로 실패했습니다. 이번 업데이트를 통해 이제 설치 프로그램에서 RPM의 문자열을 처리할 수 있습니다.

(BZ#1689909)

inst.repo 커널 부트 매개변수는 루트가 아닌 경로가 있는 하드 드라이브의 리포지토리에서 작동합니다.

이전에는 inst.repo=hd:<device>:<path> 커널 부팅 매개 변수가 하드 드라이브의 리포지토리(ISO 이미지가 아님)를 가리키고 있고 루트가 아닌(/) 경로가 사용된 경우 수동으로 조작하지 않고 RHEL 8 설치 프로세스를 진행할 수 없었습니다. 이번 업데이트를 통해 이제 설치 프로그램에서 하드 드라이브에 있는 리포지토리에 대해 <path> 를 전파하여 설치가 정상적으로 진행되도록 할 수 있습니다.

(BZ#1689194)

--changesok 옵션을 사용하면 설치 프로그램에서 루트 암호를 변경할 수 있습니다.

이전에는 Kickstart 파일에서 Red Hat Enterprise Linux 8을 설치할 때 --changesok 옵션을 사용하여 설치 프로그램에서 root 암호를 변경할 수 없었습니다. 이번 업데이트를 통해 Kickstart에 --changesok 옵션이 성공적으로 전달되므로 Kickstart 파일에 pwpolicy root -changesok 옵션을 지정하는 사용자는 Kickstart에서 이미 암호를 설정한 경우에도 GUI를 사용하여 root 암호를 변경할 수 있습니다.

(BZ#1584145)

lorax-composer API를 사용할 때 이미지 빌드가 더 이상 실패하지 않습니다

이전에는 서브스크립션된 RHEL 시스템에서 lorax-composer API를 사용할 때 이미지 빌드 프로세스가 항상 실패했습니다. 호스트의 서브스크립션 인증서가 전달되지 않으므로 Anaconda에서 리포지토리에 액세스할 수 없습니다. 문제를 해결하려면 lorax-composer,pykickstart 및 Anaconda 패키지를 업데이트합니다. 지원하는 CDN 인증서를 전달할 수 있습니다.

(BZ#1663950)

6.4.2. 쉘 및 명령행 툴

디버그 모드의 systemd 가 더 이상 불필요한 로그 메시지를 생성하지 않음

디버그 모드에서 systemd 시스템 및 서비스 관리자를 사용할 때 이전에 systemd 에서 시작한 불필

요한 로그 메시지가 생성되었습니다.

> "Failed to add rule for system call ..."

이번 업데이트를 통해 systemd 가 더 이상 불필요한 디버그 메시지를 생성하지 않도록 수정되었습니다.

(BZ#1658691)

6.4.3. 보안

fapolicyd 가 더 이상 RHEL 업데이트를 금지하지 않음

업데이트가 실행 중인 애플리케이션의 바이너리를 교체하면 커널은 " (deleted)" 접미사를 추가하여 메모리의 애플리케이션 바이너리 경로를 수정합니다. 이전에는 fapolicyd 파일 액세스 정책 데몬이 애플리케이션을 신뢰할 수 없는 것으로 처리하여 다른 파일을 열고 실행할 수 없었습니다. 그 결과 업데이트를 적용한 후 시스템을 부팅할 수 없는 경우가 있었습니다.

RHBA-2020:5241 권고가 릴리스되면서 fapolicyd 는 바이너리 경로의 접미사를 무시하므로 바이너리가 신뢰 데이터베이스와 일치할 수 있습니다. 결과적으로 fapolicyd 는 규칙을 올바르게 적용하고 업데이트 프로세스를 완료할 수 있습니다.

(BZ#1897092)

SELinux가 더 이상 Tomcat이 이메일을 보내지 않도록 차단하지 않습니다

이번 업데이트 이전에는 SELinux 정책에서 tomcat_t 및 pki_tomcat_t 도메인이 SMTP 포트에 연결하는 것을 허용하지 않았습니다. 그 결과 SELinux는 Tomcat 서버의 애플리케이션이 이메일을 보내는 것을 거부했습니다. 이 selinux-policy 패키지를 업데이트하면 이 정책을 통해 Tomcat 도메인의 프로세스가 SMTP 포트에 액세스할 수 있으며 SELinux는 더 이상 Tomcat의 애플리케이션이 이메일을 보내지 않습니다.

(BZ#1687798)

Lockdev 가 SELinux에서 올바르게 실행됩니다.

이전에는 lockdev _t의 SELinux 정책이 정의된 경우에도 lockdev 툴이 lockdev_t 컨텍스트로 전환할 수 없었습니다. 그 결과 root 사용자가 사용할 때 'unconfined_t' 도메인에서 lockdev 를 실행할 수 있

었습니다. 이로 인해 시스템에 취약점이 발생했습니다. 이번 업데이트를 통해 lockdev_t 로 전환이 정의되어 이제 강제 모드에서 SELinux에서 lockdev 를 올바르게 사용할 수 있습니다.

(BZ#1673269)

이제 SELinux에서 iotop 이 올바르게 실행됩니다.

이전에는 SELinux 정책 for iotop _t가 정의된 경우에도 theiotop 툴이 iotop_t 컨텍스트로 전환할 수 없었습니다. 그 결과, iotop 은 root 사용자가 사용할 때 'unconfined_t' 도메인에서 실행할 수 있었습니다. 이로 인해 시스템에 취약점이 발생했습니다. 이번 업데이트를 통해 전환을 iotop_t 로 정의했습니다. 이제 강제 모드에서 SELinux에서 and iotop 을 올바르게 사용할 수 있습니다.

(BZ#1671241)

이제 SELinux가 NFS 'crossmnt'를 올바르게 처리합니다.

프로세스가 서버에서 마운트 지점으로 이미 사용된 하위 디렉터리에 액세스할 때 crossmnt 옵션이 있는 NFS 프로토콜은 내부 마운트를 자동으로 생성합니다. 이전에는 SELinux에서 NFS 마운트 디렉토리에 액세스하는 프로세스에 마운트 권한이 있는지 확인하여 AVC 거부가 발생했습니다. 현재 버전에서 SELinux 권한 확인은 이러한 내부 마운트를 건너뜁니다. 결과적으로 서버측에 마운트된 NFS 디렉터리에 액세스할 때 마운트 권한이 필요하지 않습니다.

(BZ#1647723)

SELinux 정책을 다시 로드해도 더 이상 잘못된 ENOMEM 오류가 발생하지 않습니다

이전에는 SELinux 정책을 다시 로드하면 내부 보안 컨텍스트 조회 테이블이 응답하지 않았습니다. 그 결과 정책을 다시 로드하는 동안 커널이 새 보안 컨텍스트가 발생했을 때 잘못된 "메모리의 출력" (ENOMEM) 오류로 인해 작업이 실패했습니다. 이번 업데이트를 통해 내부 보안 식별자(SID) 조회 테이블이 다시 설계되어 더 이상 중지되지 않습니다. 결과적으로 커널은 SELinux 정책 다시 로드 중에 더 이상 잘못된 ENOMEM 오류를 반환하지 않습니다.

(BZ#1656787)

제한되지 않은 도메인에서 smc_socket을 사용할 수 있음

이전에는 SELinux 정책에 smc_socket 클래스에 대한 허용 규칙이 없었습니다. 결과적으로 SELinux는 제한되지 않은 도메인의 smc_socket 에 대한 액세스를 차단했습니다. 이번 업데이트를 통해 SELinux 정책에 허용 규칙이 추가되었습니다. 결과적으로 제한되지 않은 도메인에서 smc_socket 을 사용할 수 있습니다.

(BZ#1683642)

Kerberos 정리 절차가 이제 krb5.conf의 GSSAPIDelegateCredentials 및 기본 캐시와 호환됩니다.

이전 버전에서는 default_ccache_name 옵션이 krb5.conf 파일에 구성될 때 kerberos 자격 증명이 GSSAPIDelegateCredentials 및 GSSAPIupCredentials 옵션으로 정리되지 않았습니다. 이 버그는 설명된 사용 사례에서 인증 정보 캐시를 정리하도록 소스 코드를 업데이트하여 해결되었습니다. 구성 후 사용자가 구성하면 인증 정보 캐시가 종료 시 정리됩니다.

(BZ#1683295)

OpenSSH에서 일치하지 않는 키의 PKCS #11 URI를 올바르게 처리합니다.

이전에는 개체 부분(키 레이블)으로 PKCS #11 URI를 지정하면 OpenSSH가 PKCS #11에서 관련 개체를 찾지 못할 수 있었습니다. 이번 업데이트를 통해 일치하는 오브젝트를 찾을 수 없는 경우 라벨이 무시되고 키는 해당 ID와만 일치합니다. 결과적으로 OpenSSH는 이제 전체 PKCS #11 URI를 사용하여 참조되는 스마트 카드에서 키를 사용할 수 있습니다.

(BZ#1671262)

VMware 호스트 시스템과의 SSH 연결이 올바르게 작동합니다

이전 버전의 OpenSSH 제품군에서는 SSH 패킷의 기본 IPQoS(IPQoS) 플래그를 변경하여 VMware 가상화 플랫폼에서 올바르게 처리하지 않았습니다. 결과적으로 VMware의 시스템과 SSH 연결을 설정할 수 없었습니다. VMWare Workstation 15에서 이 문제가 해결되었으며 VMware 호스트 시스템과의 SSH 연결이 올바르게 작동합니다.

(BZ#1651763)

curve25519-sha256 은 OpenSSH에서 기본적으로 지원

이전에는 기본 정책 수준을 준수하더라도 OpenSSH 클라이언트 및 서버의 시스템 전체 암호화 정책 구성에서 curve25519-sha256 SSH 키 교환 알고리즘이 누락되었습니다. 결과적으로 클라이언트 또는 서버가 curve25519-sha256 을 사용하고 이 알고리즘이 호스트에서 지원하지 않는 경우 연결에 실패할 수 있습니다. 이번 crypto-policies 패키지 업데이트는 버그를 수정하고 설명된 시나리오에서 SSH 연결이 더 이상 실패하지 않습니다.

(BZ#1678661)

OSPP 및 PCI-DSS 프로필에 대한 Ansible 플레이북이 더 이상 실패하면 종료되지 않습니다

이전에는 OSPP(Security Content Automation Protocol) 및 PCI-DSS(Payment Card Industry Data Security Standard) 프로필에 대한 Ansible 수정이 잘못된 순서 및 수정의 기타 오류로 인해 실패했습니다. 이번 업데이트에서는 생성된 Ansible 해결 플레이북의 순서 및 오류를 수정하고 Ansible 해결이 올바르게 작동합니다.

(BZ#1741455)

Audit transport=KRB5 가 올바르게 작동합니다.

이번 업데이트 이전에는 감사 KRB5 전송 모드가 올바르게 작동하지 않았습니다. 결과적으로 Kerberos 피어 인증을 사용한 감사 원격 로깅이 작동하지 않았습니다. 이번 업데이트를 통해 문제가 수정되었으며 설명된 시나리오에서 감사 원격 로깅이 제대로 작동합니다.

(BZ#1730382)

6.4.4. 네트워킹

커널은 bitmap:ipmac, hash:ipmac 및 hash:mac IP 세트 유형에서 대상 MAC 주소를 지원합니다.

이전에는 bitmap:ipmac, hash:ipmac 및 hash:mac IP 세트 유형의 커널 구현은 소스 MAC 주소에서만 일치하는 것을 허용했지만 대상 MAC 주소를 지정할 수는 있었지만 설정된 항목과 일치하지 않았습니다. 결과적으로 관리자는 이러한 IP 집합 유형 중 하나에서 대상 MAC 주소를 사용한 iptables 규칙을 만들 수 있지만 지정된 사양과 일치하는 패킷은 실제로 분류되지 않았습니다. 이번 업데이트를 통해 커널은 대상 MAC 주소를 비교하고 지정된 분류가 패킷의 대상 MAC 주소에 해당하는 경우 일치를 반환합니다. 결과적으로 대상 MAC 주소에 대한 패킷과 일치하는 규칙이 올바르게 작동합니다.

(BZ#1649087)

gnome-control-center 애플리케이션에서 고급 IPsec 설정 편집 지원

이전에는 gnome-control-center 애플리케이션에 IPsec VPN 연결의 고급 옵션만 표시되었습니다. 결과적으로 사용자는 이러한 설정을 변경할 수 없었습니다. 이번 업데이트를 통해 이제 고급 설정의 필드를 편집할 수 있으며 사용자는 변경 사항을 저장할 수 있습니다.

(BZ#1697329)

iptables-extensions(8) 도움말 페이지의 TRACE 대상이 업데이트되었습니다.

이전에는 iptables-extensions(8) 도움말 페이지의 TRACE 대상에 대한 설명이 Compat 변형 만 참조했지만 Red Hat Enterprise Linux 8에서는 the nf_tables 변형을 사용합니다. 결과적으로 도움말 페이

지에서는 **TRACE** 이벤트를 표시하기 위해 **xtables-monitor** 명령줄 유틸리티를 참조하지 않았습니다. 도움말 페이지가 업데이트되어 이제 **xtables-monitor** 가 표시됩니다.

(**BZ#1658734**)

ipset 서비스에 로그인하는 중 오류가 개선되었습니다.

이전에는 **ipset** 서비스에서 **systemd** 로그의 의미 있는 심각도와 함께 구성 오류를 보고하지 않았습니다. 유효하지 않은 구성 항목의 심각도 수준은 정보로만 제공 되었으며 서비스에서 사용할 수 없는 구성에 대한 오류를 보고하지 않았습니다. 그 결과 관리자가 **ipset** 서비스 구성에서 문제를 식별하고 해결하기 어려웠습니다. 이번 업데이트를 통해 **ipset** 는 **systemd** 로그 의 구성 문제를 경고로 보고하고 서비스가 시작되지 않으면 자세한 내용을 포함하여 오류 심각도가 있는 항목을 기록합니다. 결과적으로 이제 **ipset** 서비스 구성에서 문제를 쉽게 해결할 수 있습니다.

(**BZ#1683711**)

ipset 서비스에서 시작하는 동안 잘못된 설정 항목을 무시합니다

ipset 서비스는 구성을 별도의 파일에 세트로 저장합니다. 이전 버전에서는 서비스가 시작되면 수동으로 세트를 편집하여 삽입할 수 있는 유효하지 않은 항목을 필터링하지 않고 단일 작업에서 모든 세트의 구성이 복원되었습니다. 이로 인해 단일 구성 항목이 유효하지 않은 경우 서비스가 관련이 없는 추가 세트를 복원하지 않았습니다. 문제가 해결되었습니다. 결과적으로 **ipset** 서비스는 복원 작업 중에 유효하지 않은 구성 항목을 탐지하고 제거하고 잘못된 구성 항목을 무시합니다.

(**BZ#1683713**)

ipset list 명령은 해시 세트 유형에 대한 일관된 메모리를 보고합니다.

해시 세트 유형에 항목을 추가할 때 **ipset** 유틸리티는 메모리 블록을 할당하여 새 항목의 크기를 에 맞게 조정해야 합니다. 이전에는 **ipset** 에서 할당된 총 크기를 현재 메모리 내 크기에 값을 추가하는 대신 새 블록의 크기로만 설정했습니다. 그 결과 **ip list** 명령은 일관되지 않은 메모리 크기를 보고했습니다. 이번 업데이트를 통해 **ipset** 은 메모리 내 크기를 올바르게 계산합니다. 결과적으로 **ipset list** 명령은 이제 세트의 올바른 메모리 내 크기를 표시하고, 출력은 해시 세트 유형에 대해 실제 할당된 메모리와 일치합니다.

(**BZ#1714111**)

ICMPv6 패킷 **Too Big** 메시지를 받을 때 커널이 **PMTU**를 올바르게 업데이트합니다.

링크-로컬 주소 등의 특정 상황에서는 둘 이상의 경로가 소스 주소와 일치할 수 있습니다. 이전에는 커널이**ICMPv6)** 패킷을 수신할 때 입력 인터페이스를 확인하지 않았습니다. 따라서 경로 조회에서 입력 인터페이스와 일치하지 않는 대상을 반환할 수 있었습니다. 그 결과 **ICMPv6** 패킷 **Too Big** 메시지를 수신할 때 커널은 다른 입력 인터페이스에 대해 **PMTU(Path maximum maximum Transmission Unit)**를 업데

이트할 수 있습니다. 이번 업데이트를 통해 커널은 경로 조회 중에 입력 인터페이스를 확인합니다. 그 결과 커널이 소스 주소를 기반으로 올바른 대상을 업데이트하고 설명된 시나리오에서 PMTU가 예상대로 작동합니다.

(BZ#1721961)

/etc/hosts.allow 및 /etc/hosts.deny 파일에 더 이상 tcp_wrappers제거에 대한 오래된 참조가 포함되어 있지 않습니다.

이전에는 /etc/hosts.allow 및 /etc/hosts.deny 파일에 tcp_wrappers 패키지에 대한 오래된 정보가 포함되어 있었습니다. 파일은 제거된 tcp_wrappers 에 더 이상 필요하지 않으므로 RHEL 8에서 제거됩니다.

(BZ#1663556)

6.4.5. 커널

tpm2-abrmd-selinux 에 이제 selinux-policy-targeted에 올바르게 종속되어 있습니다.

이전에는 tpm2-abrmd-selinux 패키지에 selinux-policy- targeted 패키지 대신 selinux-policy-base 패키지에 종속되어 있었습니다. 결과적으로 시스템에 selinux-policy- targeted 대신 selinux-policy- minimum 이 설치된 경우 tpm2-abrmd-selinux 패키지 설치에 실패했습니다. 이번 업데이트에서는 버그가 수정되어 설명된 시나리오에 tpm2-abrmd-selinux 를 올바르게 설치할 수 있습니다.

(BZ#1642000)

모든 /sys/kernel/debug 파일에 액세스할 수 있습니다.

이전에는 오류와 관계없이 함수가 끝날 때까지 EPERM(운영 불가) 오류에 대한 반환 값이 설정되었습니다. 결과적으로 특정 /sys/kernel/debug (debug fs) 파일에 액세스하는 모든 시도가 보장되지 않은 EPERM 오류로 실패했습니다. 이번 업데이트에서는 EPERM 반환 값을 다음 블록으로 이동합니다. 따라서 설명된 시나리오에서 문제 없이 debugfs 파일에 액세스할 수 있습니다.

(BZ#1686755)

NIC는 41000 및 45000 FastLinQ 시리즈의 qede 드라이버의 버그의 더 이상 영향을 받지 않습니다.

이전에는 41000 및 45000 FastLinQ 시리즈의 qede 드라이버의 버그로 인해 펌웨어 업그레이드 및 디버그 데이터 수집 작업이 실패했습니다. NIC를 사용할 수 없게 되었습니다. 호스트의 재부팅(PCI 재설정)으로 NIC가 다시 작동했습니다.

이 문제는 다음과 같은 시나리오에서 발생할 수 있습니다.

- 인박스 드라이버를 사용하여 **NIC** 펌웨어 업그레이드 중
- **ethtool -d ethx** 명령을 실행하는 디버그 데이터 수집 중
- **ethtool -d ethx**를 포함한 **sosreport** 명령을 실행하는 동안.
- **I/O** 시간 초과, 메일 박스 명령 시간 제한 및 하드웨어 **Attention**과 같은 **inbox** 드라이버에서 자동 디버그 데이터 수집을 시작하는 동안.

이 문제를 해결하기 위해 **Red Hat**은 **RHBA(Red Hat Bug Advisory)**를 통해 에라타를 릴리스했습니다. **RHBA**가 릴리스되기 전에는 https://access.redhat.com/support 에서 지원되는 수정 사항을 요청하는 케이스를 생성하는 것이 좋습니다.

(BZ#1697310)

일반 **EDACES** 드라이버에서 오류를 보고한 **DIMM**을 감지합니다.

이전에는 **EDACES** 드라이버 에서 오류를 보고한 **DIMM**을 탐지할 수 없었습니다. 결과적으로 다음과 같은 오류 메시지가 표시되었습니다.

```
DIMM location: not present. DMI handle: 0x<ADDRESS>
```

이제 드라이버가 **DMI(**데스크탑 관리 인터페이스**)** 핸들 **0x<ADDRESS>** 와 일치하는 특정 **DIMM**을 감지하도록 **DMI(SMBIOS)** 테이블을 스캔하도록 업데이트되었습니다. 결과적으로 **EDAC¢ES**는 하드웨어 오류를 보고한 특정 **DIMM**을 올바르게 감지합니다.

(BZ#1721386)

Podman 은 **RHEL 8**의 컨테이너를 확인할 수 있습니다.

이전에는 **CRIU(Checkpoint and Restore In Userspace)** 패키지 버전이 오래되었습니다. 결과적으로 **CRIU**는 컨테이너 체크포인트 및 복원 기능을 지원하지 않았으며 **podman** 유틸리티에서 컨테이너를

확인하지 못했습니다. podman container checkpoint 명령을 실행할 때 다음과 같은 오류 메시지가 표시되었습니다.

```
'checkpointing a container requires at least CRIU 31100'
```

이번 업데이트에서는 CRIU 패키지 버전을 업그레이드하여 문제를 해결합니다. 결과적으로 podman 에서 컨테이너 체크포인트 및 복원 기능을 지원합니다.

(BZ#1689746)

dracut.conf에서 add_dracutmodules+=earlykdump 옵션을 사용하면 early-kdump 및 표준 kdump 가 더 이상 실패하지 않습니다.

이전에는 early-kdump 를 위해 설치 중인 커널 버전과 커널 버전 initramfs 간에 불일치가 발생했습니다. 그 결과 kdump 가 활성화되면 부팅에 실패했습니다. 또한 early-kdump 가 표준 kdump initramfs 이미지에 포함되어 있음을 감지하면 종료가 강제되었습니다. 따라서 early-kdump 가 기본 dracut 모듈로 추가된 경우 kdump initramfs를 다시 빌드하려고 할 때도 표준 kdump 서비스도 실패했습니다. 그 결과 early-kdump 및 표준 kdump 는 둘 다 실패했습니다. 이번 업데이트를 통해 early-kdump 는 설치 중에 일관된 커널 이름을 사용하므로 버전만 실행 중인 커널과 다릅니다. 또한 표준 kdump 서비스는 이미지 생성 실패를 방지하기 위해 early-kdump 를 강제로 삭제합니다. 따라서 설명된 시나리오에서 early-kdump 및 표준 kdump 가 더 이상 실패하지 않습니다.

(BZ#1662911)

SME를 활성화한 첫 번째 커널이 vmcore 덤프에 성공

이전에는 활성 SME(Secure Memory Encryption) 기능을 사용한 첫 번째 커널의 암호화된 메모리로 인해 kdump 메커니즘이 실패했습니다. 결과적으로 첫 번째 커널은 메모리의 콘텐츠(vmcore)를 덤프할 수 없었습니다. 이번 업데이트를 통해 암호화된 메모리를 다시 매핑하고 관련 코드를 수정하기 위해 ioremap_encrypted() 함수가 추가되었습니다. 결과적으로 암호화된 첫 번째 커널의 메모리에 올바르게 액세스하고 설명된 시나리오의 크래시 툴에서 vmcore를 덤프하고 구문 분석할 수 있습니다.

(BZ#1564427)

SEV를 활성화한 첫 번째 커널이 vmcore 덤프에 성공

이전에는 활성 SEV(Secure Encrypted Virtualization) 기능을 사용한 첫 번째 커널의 암호화된 메모리로 인해 kdump 메커니즘이 실패했습니다. 결과적으로 첫 번째 커널은 메모리의 콘텐츠(vmcore)를 덤프할 수 없었습니다. 이번 업데이트를 통해 암호화된 메모리를 다시 매핑하고 관련 코드를 수정하기 위해 ioremap_encrypted() 함수가 추가되었습니다. 결과적으로 첫 번째 커널의 암호화된 메모리에 올바르게 액세스하고 설명된 시나리오의 크래시 툴에서 vmcore를 덤프하고 구문 분석할 수 있습니다.

(BZ#1646810)

커널이 SWIOTLB에 더 많은 공간을 예약

이전에는 커널에서 SEV(Secure Encrypted Virtualization) 또는 SME(Secure Memory Encryption) 기능이 활성화되었을 때 SWIOTLB(Software Input Output Translation Lookaside Buffer) 기술을 활성화하고 상당한 양의 메모리를 사용해야 했습니다. 결과적으로 캡처 커널이 부팅되지 않거나 메모리 부족 오류가 발생했습니다. 이번 업데이트에서는 SEV/SME가 활성화된 상태에서 SWIOTLB에 대한 추가 크래시커널 메모리를 예약하여 버그가 수정되었습니다. 결과적으로 캡처 커널은 SWIOTLB용으로 예약된 메모리가 많으며 설명된 시나리오에는 더 이상 버그가 표시되지 않습니다.

(BZ#1728519)

이제 hwlatdetect 실행 중에 C 상태 전환을 비활성화할 수 있습니다

실시간 성능을 달성하려면 hwlatdetect 유틸리티에서 테스트 실행 중에 CPU 절전을 비활성화할 수 있어야 합니다. 이번 업데이트를 통해 테스트 실행 기간 동안 hwlatdetect 가 C 상태 전환을 해제하고 hwlatdetect 는 하드웨어 대기 시간을 보다 정확하게 감지할 수 있습니다.

(BZ#1707505)

6.4.6. 하드웨어 활성화

openmpi 패키지를 지금 설치할 수 있습니다

이전에는 opensm 패키지의 리베이스로 인해 soname 메커니즘이 변경되었습니다. 결과적으로 확인되지 않은 종속성으로 인해 openmpi 패키지를 설치할 수 없었습니다. 이번 업데이트에서는 문제가 해결되었습니다. 그 결과 openmpi 패키지를 문제없이 설치할 수 있습니다.

(BZ#1717289)

6.4.7. 파일 시스템 및 스토리지

RHEL 8 설치 프로그램은 이제 항목 ID를 사용하여 기본 부팅 항목을 설정합니다.

이전에는 RHEL 8 설치 프로그램에서 첫 번째 부팅 항목의 색인을 항목 ID를 사용하는 대신 기본값으로 사용했습니다. 그 결과 새 부팅 항목을 추가하는 것이 먼저 정렬되어 첫 번째 인덱스로 설정되었으므로 기본값이 되었습니다. 이번 업데이트를 통해 설치 프로그램은 항목 ID를 사용하여 기본 부팅 항목을 설정하며, 결과적으로 부팅 항목이 추가되어 기본값 앞에 정렬된 경우에도 기본 항목이 변경되지 않습니다.

(BZ#1671047)

이제 SME가 smartpqi로 활성화되면 시스템이 성공적으로 부팅됩니다.

이전에는 SME(Secure Memory Encryption) 기능이 활성화되어 루트 디스크에서 smartpqi 드라이버를 사용하는 경우 특정 AMD 시스템에서 시스템을 부팅하지 못했습니다.

부팅이 실패하면 시스템에 부팅 로그에 다음과 유사한 메시지가 표시되었습니다.

```
smartpqi 0000:23:00.0: failed to allocate PQI error buffer
```

이 문제는 DMA(동적 직접 메모리 액세스) 마스크가 설정되지 않았기 때문에 SWIOTLB(Software Input Output Translation Lookaside Buffer)로 대체되는 smartpqi 드라이버로 인해 발생했습니다.

이번 업데이트를 통해 일관성 있는 DMA 마스크가 올바르게 설정됩니다. 그 결과 루트 디스크에 smartpqi 드라이버를 사용하는 시스템에서 SME가 활성화되면 시스템이 성공적으로 부팅됩니다.

(BZ#1712272)

FCoE LUN은 bnx2fc 카드에서 생성된 후 사라집니다.

이전에는 bnx2fc 카드에 FCoE LUN을 생성한 후 FCoE LUN이 올바르게 연결되지 않았습니다. 결과적으로 RHEL 8.0의 bnx2fc 카드에 생성된 후 FCoE LUN이 사라졌습니다. 이번 업데이트를 통해 FCoE LUN이 올바르게 연결됩니다. 결과적으로 bnx2fc 카드에 생성된 후 FCoE LUN을 검색할 수 있습니다.

(BZ#1685894)

다른 엔드 플랫폼으로 이동한 후 더 이상 VDO 볼륨의 중복 제거 조언이 손실되지 않습니다

이전에는 VDO 볼륨을 다른 endian을 사용하는 플랫폼으로 이동한 후 UDS(Universal Deduplication Service) 인덱스가 중복 제거되는 모든 권고를 손실했습니다. 결과적으로 VDO는 볼륨을 이동하기 전에 저장된 데이터에 대해 새로 작성된 데이터를 중복 제거할 수 없어 공간 절약을 줄일 수 있었습니다.

이번 업데이트를 통해 중복 제거 권고를 손실하지 않고 다른 최종 버전을 사용하는 플랫폼 간에 VDO 볼륨을 이동할 수 있습니다.

(BZ#1696492)

Kdump 서비스는 대규모 **IBM POWER** 시스템에서 작동합니다.

이전에는 **RHEL8 kdump** 커널이 시작되지 않았습니다. 결과적으로 대형 **IBM POWER** 시스템에서 **kdump initrd** 파일이 생성되지 않았습니다. 이번 업데이트를 통해 **squashfs-tools-4.3-19.el8** 구성 요소가 추가되었습니다. 이번 업데이트에서는 사용 가능한 모든 **CPU**를 사용하는 대신 **squashfs-tools-4.3-19.el8** 구성 요소가 사용할 수 있는 **CPU** 수에 제한(**128**)이 추가되었습니다. 이로 인해 리소스 부족 오류가 수정되었습니다. 결과적으로 **kdump** 서비스는 대규모 **IBM POWER** 시스템에서 작동합니다.

(BZ#1716278)

이제 **nfs.conf**에 자세한 정보 표시 디버그 옵션이 추가되었습니다.

이전에는 **/etc/nfs.conf** 파일과 **nfs.conf(5)** 도움말 페이지에 다음 옵션이 포함되지 않았습니다.

- 상세 정보 표시
- **rpc-verbosity**

결과적으로 사용자는 이러한 디버그 플래그를 인식하지 못했습니다. 이번 업데이트를 통해 이러한 플래그는 이제 **/etc/nfs.conf** 파일의 **[gssd]** 섹션에 포함되며 **nfs.conf (8)** 도움말 페이지에도 설명되어 있습니다.

(BZ#1668026)

6.4.8. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

socket::inet_aton() 을 여러 스레드에서 안전하게 사용할 수 있음

이전에는 안전하지 않은 **gethostbyname () glibc** 함수라는 여러 **Perl** 스레드에서 도메인 이름을 확인하는 데 사용된 **Socket::inet_aton ()** 함수가 있었습니다. 결과적으로 잘못된 **IPv4** 주소가 반환되거나 **Perl** 인터프리터가 예기치 않게 종료되었습니다. 이번 업데이트를 통해 **gethostbyname ()** 대신 **thread-safe getaddrinfo() glibc** 함수를 사용하도록 **Socket::inet_aton ()** 구현이 변경되었습니다. 결과적으로 **Perl** 소켓 모듈의 **inet_aton()** 함수를 여러 스레드에서 안전하게 사용할 수 있습니다.

(BZ#1699793, BZ#1699958)

6.4.9. 컴파일러 및 개발 도구

메모리가 부족한 경우에도 gettext 는 번역되지 않은 텍스트를 반환합니다.

이전에는 텍스트 로컬화에 대한 gettext() 함수에서 메모리 부족 시 텍스트 값이 아닌 NULL 값을 반환하여 애플리케이션에 텍스트 출력 또는 레이블이 없었습니다. 이 버그가 수정되어 이제 gettext() - 메모리 부족 시 해석되지 않은 텍스트를 예상대로 반환합니다.

(BZ#1663035)

이제 locale 명령으로 실행 중에 오류가 발생할 때마다 LOCPATH 가 설정됨을 경고합니다.

이전에는 locale 명령에서 잘못된 LOCPATH로 인해 오류가 발생할 때 LOCPATH 환경 변수에 대한 진단을 제공하지 않았습니다 . LOCPATH가 실행 중에 오류가 발생할 때마다 LOCPATH 가 설정되었음을 경고하도록 locale 명령이 설정됩니다. 그 결과 로케일 에서 발생하는 기본 오류와 함께 LOCPATH 를 보고합니다.

(BZ#1701605)

GDB 는 aarch64 SVE의 코어 파일에서 z 레지스터를 읽고 올바르게 나타낼 수 있습니다.

이전에는 gdb 구성 요소가 aarch64 확장 가능한 벡터 확장(SVE) 아키텍처를 사용하여 코어 파일에서 z 레지스터를 읽지 못했습니다. 이번 업데이트를 통해 이제 gdb 구성 요소가 코어 파일에서 z 레지스터를 읽을 수 있습니다. 결과적으로 info register 명령이 z 레지스터 콘텐츠를 성공적으로 표시합니다.

(BZ#1669953)

GCC가 버전 8.3.1으로 업데이트

GCC(GNU 컴파일러 컬렉션)가 업스트림 버전 8.3.1으로 업데이트되었습니다. 이 버전은 많은 수의 버그 수정을 제공합니다.

(BZ#1680182)

6.4.10. IdM (Identity Management)

freeradacy에서 IPv6 주소를 가리키는 호스트 이름을 확인합니다.

이전 RHEL 8 버전의 FreeRADIUS에서 ipaddr 유틸리티는 IPv4 주소만 지원했습니다. 결과적으로 IPv6 주소를 확인하기 위해 시스템을 RHEL 7에서 RHEL 8로 업그레이드한 후 구성의 수동 업데이트가

필요했습니다. 이번 업데이트에서는 기본 코드가 수정되었으며 FreeRADIUS의 ipaddr 도 IPv6 주소를 사용합니다.

(BZ#1685546)

Nuxwdog 서비스는 더 이상 HSM 환경에서 PKI 서버를 시작하지 못합니다.

이전 버전에서는 버그로 인해 keyutils 패키지가 pki-core 패키지의 종속성으로 설치되지 않았습니다. 또한 Nuxwdog 워치독 서비스에서 HSM(하드웨어 보안 모듈)을 사용하는 환경에서 PKI(공개 키 인프라) 서버를 시작하지 못했습니다. 이러한 문제는 해결되었습니다. 결과적으로 필수 keyutils 패키지가 종속성으로 자동으로 설치되고 Nuxwdog 는 HSM이 있는 환경에서 PKI 서버를 예상대로 시작합니다.

(BZ#1695302)

IdM 서버가 FIPS 모드에서 올바르게 작동합니다.

이전에는 Tomcat 서버의 SSL 커넥터가 불완전하게 구현되었습니다. 결과적으로 인증서 서버가 설치된 IdM(Identity Management) 서버가 FIPS 모드가 활성화된 시스템에서 작동하지 않았습니다. 이 버그는 JSSTrustManager 및 JSSKeyManager 를 추가하여 해결되었습니다. 결과적으로 설명된 시나리오에서 IdM 서버가 올바르게 작동합니다.

RHEL 8의 FIPS 모드에서 IdM 서버가 실행되지 않는 여러 버그가 있습니다. 이번 업데이트에서는 해당 중 하나만 수정했습니다.

(BZ#1673296)

KCM 인증 정보 캐시가 단일 인증 정보 캐시의 많은 인증 정보에 적합합니다.

이전에는 KCM(Kerberos Credential Manager)에 많은 수의 자격 증명이 포함된 경우 kinit 와 같은 Kerberos 작업은 데이터베이스의 항목 크기와 이러한 항목 수를 제한하여 실패했습니다.

이번 업데이트에서는 sssd.conf 파일의 kcm 섹션에 다음과 같은 새로운 구성 옵션이 도입되었습니다.

- max_kontch (통합)
- max_uid_ destinations (integer)

- max_ccache_size (integer)

결과적으로 KCM은 이제 단일 ccache에서 많은 수의 자격 증명을 처리할 수 있습니다.

구성 옵션에 대한 자세한 내용은 sssd-kcm 도움말 페이지를 참조하십시오.

(BZ#1448094)

sss ID 매핑 플러그인을 사용할 때 Samba에서 더 이상 액세스를 거부하지 않습니다

이전 버전에서는 이 구성이 있는 도메인 멤버에서 Samba를 실행하고 sss ID 매핑 백엔드를 /etc/samba/smb.conf 파일에 사용한 구성을 추가하면 디렉터리를 공유하면 ID 매핑 백엔드가 변경되어 오류가 발생했습니다. 그 결과 Samba는 사용자 또는 그룹이 존재하는 경우에도 특정 사례에서 파일에 대한 액세스를 거부하고 SSSD에서 알고 있었습니다. 문제가 해결되었습니다. 따라서 sss 플러그인을 사용할 때 Samba가 더 이상 액세스를 거부하지 않습니다.

(BZ#1657665)

기본 SSSD 시간 제한 값이 더 이상 서로 충돌하지 않음

이전에는 기본 시간 제한 값 사이에 충돌이 발생했습니다. 다음 옵션의 기본값이 페일오버 기능을 개선하도록 변경되었습니다.

- dns_resolver_op_timeout - 2s (이전 6s)로 설정합니다.
- dns_resolver_timeout - 4s (이전 6s)로 설정
- ldap_opt_timeout - 8s (이전 6s)로 설정합니다.

또한 기본값이 1000ms인 새로운 dns_resolver_server_timeout 옵션이 추가되어 SSSD가 한 DNS 서버에서 다른 DNS 서버로 전환하는 시간 초과 기간을 지정합니다.

(BZ#1382750)

6.4.11. 데스크탑

systemctl isolate multi-user.target 에 콘솔 프롬프트가 표시

systemctl isolate multi-user.target 명령을 GNOME 데스크탑 세션에서 GNOME Terminal에서 실행할 때 콘솔 프롬프트가 아니라 커서만 표시되었습니다. 이번 업데이트 fixgdm 및 설명된 상황에서 콘솔 프롬프트가 예상대로 표시됩니다.

(BZ#1678627)

6.4.12. 그래픽 인프라

'i915' 디스플레이 드라이버는 이제 디스플레이 구성을 최대 34K까지 지원합니다.

이전에는 Xorg 세션에서 'i915' 표시 드라이버를 사용할 때 표시 구성이 24K보다 큰 경우가 있었습니다. 이번 업데이트를 통해 'i915' 드라이버는 이제 최대 34K의 디스플레이 구성을 지원합니다.

(BZ#1664969)

GPU 드라이버를 초기화할 때 Linux 게스트에 더 이상 오류가 표시되지 않습니다

이전에는 GPU 드라이버를 초기화할 때 Linux 게스트에서 경고를 반환했습니다. 이는 Intel Graphics Virtualization Technology -g (GVT -g)가 게스트에 대한 DisplayPort (DP) 인터페이스만 시뮬레이션하고 'EDP_PSR_IMR' 및 'EDP_PSR_IIR' 레지스터를 기본 메모리 매핑 I/O(MMIO) 읽기/쓰기 레지스터로 등록하기 때문에 발생했습니다. 이 문제를 해결하기 위해 핸들러가 이러한 레지스터에 추가되고 경고가 더 이상 반환되지 않습니다.

(BZ#1643980)

6.4.13. 웹 콘솔

session_recording 쉘을 사용하여 RHEL 웹 콘솔에 로그인할 수 있습니다.

이전에는 세션 기록을 활성화하는 tlog 쉘의 사용자가 RHEL 웹 콘솔에 로그인할 수 없었습니다. 이번 업데이트에서는 버그가 수정되었습니다. 업데이트를 설치한 후 tlog-rec-session 쉘을 /etc/shells/ 에 추가하는 이전 해결방법을 복원해야 합니다.

(BZ#1631905)

6.4.14. 가상화

pcie-to-pci 브리지 컨트롤러에 **PCI** 장치를 핫플러그하는 것이 올바르게 작동합니다.

이전 버전에서는 게스트 가상 머신 구성에 게스트가 시작될 때 엔드포인트 장치가 연결되지 않은 **pcie-to-pci-bridge** 컨트롤러가 포함되어 있으면 해당 컨트롤러에 새 장치를 핫플러그할 수 있었습니다. 이번 업데이트에서는 **PCIe** 시스템에서 레거시 **PCI** 장치를 핫플러그하는 방법이 개선되어 문제가 발생하지 않습니다.

(BZ#1619884)

중첩된 가상화를 활성화해도 더 이상 실시간 마이그레이션이 차단되지 않습니다

이전에는 중첩된 가상화 기능이 실시간 마이그레이션과 호환되지 않았습니다. 결과적으로 **RHEL 8** 호스트에서 중첩된 가상화를 활성화하면 호스트에서 **VM**(가상 시스템)을 마이그레이션하고 **VM** 상태 스냅샷을 디스크에 저장하지 못했습니다. 이번 업데이트에서는 설명된 문제가 해결되어 영향을 받는 **VM**을 마이그레이션할 수 있습니다.

(BZ#1689216)

6.4.15. 지원 관련 기능

redhat-support-tool 에서 **sosreport** 아카이브 생성

이전에는 **redhat-support-tool** 유틸리티에서 **sosreport** 아카이브를 생성할 수 없었습니다. 해결방법은 **sosreport** 명령을 별도로 실행한 다음 **redhat-support-tool addattachment -c** 명령을 입력하여 아카이브를 업로드하는 것이었습니다. 또한 사용자는 고객 사례를 생성하고 **sosreport** 아카이브를 업로드하는 고객 포털에서 웹 **UI**를 사용할 수 있습니다.

또한 **findkerneldebugs,btextract,**분석 또는 진단과 같은 명령 옵션은 예상대로 작동하지 않으며 향후 릴리스에서 수정될 예정입니다.

(BZ#1688274)

6.5. 기술 프리뷰

다음 부분에서는 **Red Hat Enterprise Linux 8.1**에서 사용할 수 있는 모든 기술 프리뷰 목록을 설명합니다.

기술 프리뷰 기능에 대한 Red Hat 지원 범위 내용은 기술 프리뷰 기능 지원 범위를 참조하십시오.

6.5.1. 네트워킹

TIPC 는 완전 지원

TIPC(Transparent Inter Process Communication)는 느슨하게 연결된 노드의 클러스터 내에서 효율적인 통신을 위해 특별히 설계된 프로토콜입니다. 커널 모듈로 작동하며 iproute2 패키지에서 팁 도구를 제공하여 설계자가 클러스터 내부의 위치에 관계없이 다른 애플리케이션과 빠르고 안정적으로 통신할 수 있는 애플리케이션을 만들 수 있습니다. 이 기능은 이제 RHEL 8에서 완벽하게 지원됩니다.

(BZ#1581898)

tc용 eBPF를 기술 프리뷰로 이용 가능

기술 프리뷰로 tc(트래픽 제어) 커널 하위 시스템과 the tc 툴은 eBPF(extended Berkeley Packet Filtering) 프로그램을 패킷 분류기 및 수신 및 송신 대기열 지정 규칙 모두에 대한 작업으로 연결할 수 있습니다. 이를 통해 커널 네트워크 데이터 경로 내에서 프로그래밍 가능한 패킷 처리가 가능합니다.

(BZ#1699825)

NMState 를 기술 프리뷰로 사용 가능

NMState는 호스트에 대한 네트워크 API입니다. 기술 프리뷰로 사용할 수 있는 nmstate 패키지는 선언적 방식으로 호스트 네트워크 설정을 관리하는 라이브러리 및 nmstatectl 명령줄 유틸리티를 제공합니다. 네트워킹 상태는 사전 정의된 스키마에서 설명합니다. 현재 상태를 보고하고 원하는 상태로 변경 사항이 모두 스키마를 준수합니다.

자세한 내용은 /usr/share/doc/nmstate/README.md 파일과 /usr/share/doc/nmstate/examples 디렉토리의 예제를 참조하십시오.

(BZ#1674456)

AF_XDP 를 기술 프리뷰로 사용 가능(_X)

AF_XDP(Address Family eXpress Data Path) 소켓은 고성능 패킷 처리를 위해 설계되었습니다. XDP와 결합하고 추가 처리를 위해 프로그래밍 방식으로 선택한 패킷을 사용자 공간 애플리케이션에 효율적으로 리디렉션합니다.

(BZ#1633143)

XDP를 기술 프리뷰로 이용 가능

기술 프리뷰로 사용할 수 있는 eXpress Data Path(XDP) 기능은 커널 수신 데이터 경로의 초기 지점에서 고성능 패킷 처리를 위해 eBPF(Extended Berkeley Packet Filter) 프로그램을 연결하여 효율적으로 프로그래밍 가능한 패킷 분석, 필터링 및 조작을 허용합니다.

(BZ#1503672)

KTLS는 기술 프리뷰로 사용 가능

Red Hat Enterprise Linux 8에서 KTLS(Kernel Transport Layer Security)는 기술 프리뷰로 제공됩니다. KTLS는 AES-GCM 암호화를 위한 커널에서 대칭 암호화 또는 암호 해독 알고리즘을 사용하여 TLS 레코드를 처리합니다. 또한 KTLS는 이 기능을 지원하는 NIC(네트워크 인터페이스 컨트롤러)로 TLS 레코드 암호화를 오프로드하는 인터페이스를 제공합니다.

(BZ#1570255)

systemd-resolved 서비스를 기술 프리뷰로 사용 가능

systemd 확인 서비스는 로컬 애플리케이션에 대한 이름 확인을 제공합니다. 이 서비스는 캐싱을 구현하고 DNS 스텁 확인자, LLMNR(링크-로컬 멀티캐스트 이름 확인자) 및 멀티캐스트 DNS 확인자 및 응답자를 검증합니다.

systemd 패키지가 systemd -resolved 를 제공하는 경우에도 이 서비스는 지원되지 않는 기술 프리뷰입니다.

(BZ#1906489)

6.5.2. 커널

Control Group v2를 RHEL 8에서 기술 프리뷰로 이용 가능

Control Group v2 메커니즘은 통합된 계층 컨트롤 그룹입니다. Control Group v2는 프로세스를 계층적으로 구성하고 제어 및 설정 가능한 방식으로 계층에 따라 시스템 리소스를 배포합니다.

이전 버전과 달리 Control Group v2에는 하나의 계층만 있습니다. 이 단일 계층을 통해 Linux 커널에

서는 다음을 수행할 수 있습니다.

- 소유자의 역할에 따라 프로세스 분류
- 여러 계층에서 충돌하는 정책 문제 해결

Control Group v2에서는 다양한 컨트롤러가 지원되고 있습니다.

- **CPU** 컨트롤러가 **CPU** 사이클의 배분을 조정합니다. 이 컨트롤러는 다음을 구현합니다.
  - 일반적인 스케줄링 정책에 대한 가중치 및 절대 대역폭 제한 모델
  - 실시간 스케줄링 정책에 대한 절대 대역폭 할당 모델
- 메모리 컨트롤러가 메모리 할당을 조정합니다. 현재 다음과 같은 유형의 메모리 사용을 추적할 수 있습니다.
  - **Userland** 메모리 **-** 페이지 캐시 및 익명 메모리
  - **dentries** 및 **inode**와 같은 커널 데이터 구조
  - **TCP** 소켓 버퍼
- **I/O** 컨트롤러가 **I/O** 리소스 배분을 제한합니다.
- 쓰기 저장 컨트롤러는 메모리 및 **I/O** 컨트롤러와 상호작용하며 **Control Group v2** 고유의 것입니다.

위의 정보는 **https://www.kernel.org/doc/Documentation/cgroup-v2.txt** 링크를 기반으로 합니다. 동일한 링크를 참조하여 특정 **Control Group v2** 컨트롤러에 대한 자세한 정보를 얻을 수 있습니다.

(BZ#1401552)

기술 프리뷰로 kexec 빠른 재부팅

kexec 빠른 재부팅 기능은 기술 프리뷰로 계속 사용할 수 있습니다. 이제 kexec 빠른 재부팅으로 인해 재부팅 속도가 훨씬 빨라졌습니다. 이 기능을 사용하려면 kexec 커널을 수동으로 로드한 다음 운영 체제를 재부팅합니다.

(BZ#1769727)

eBPF를 기술 프리뷰로 이용 가능

eBPF(Extended Berkeley Packet Filter) 는 제한된 기능 집합에 액세스할 수 있는 제한된 샌드박스 환경에서 커널 공간에서 코드를 실행할 수 있는 커널 내 가상 시스템입니다.

가상 시스템에는 다양한 유형의 맵 생성을 지원하고 특수 어셈블리와 유사한 코드로 프로그램을 로드할 수 있는 새로운 시스템 호출 bpf() 가 포함되어 있습니다. 그런 다음 코드가 커널로 로드되고 즉시 컴파일을 사용하여 기본 머신 코드로 변환됩니다. bpf() syscall은 root 사용자와 같이 CAP_SYS_ADMIN 기능을 가진 사용자만 사용할 수 있습니다. 자세한 내용은 bpf(2) 도움말 페이지를 참조하십시오.

로드된 프로그램을 다양한 지점(소켓, 추적 지점, 패킷 수신)에 연결하여 데이터를 수신 및 처리할 수 있습니다.

Red Hat은 eBPF 가상 시스템을 활용하는 수많은 구성 요소를 제공합니다. 각 구성 요소는 다른 개발 단계에 있으므로 현재 모든 구성 요소가 완전히 지원되지는 않습니다. 특정 구성 요소가 지원됨으로 표시되지 않는 한 모든 구성 요소는 기술 프리뷰로 사용할 수 있습니다.

다음과 같은 주요 eBPF 구성 요소는 현재 기술 프리뷰로 사용할 수 있습니다.

- eBPF 가상 시스템을 사용하는 동적 커널 추적 유틸리티 컬렉션인 BCC(BPF Compiler Collection) 툴 패키지. BCC 툴 패키지는 64비트 ARM 아키텍처, IBM Power Systems, Little Endian, IBM Z 아키텍처에서 기술 프리뷰로 사용할 수 있습니다. AMD 및 Intel 64비트 아키텍처에서 완전하게 지원됩니다.
- eBPF 가상 시스템을 활용하는 고급 추적 언어인 bpftrace.
-

eBPF 가상 시스템을 사용하여 커널에서 빠른 패킷 처리를 가능하게 하는 네트워킹 기술인 eXpress Data Path(XDP) 기능입니다.

(BZ#1559616)

soft-RoCE를 기술 프리뷰로 이용 가능

RoCE(Remote Direct Memory Access) over Converged Ethernet (RoCE)는 이더넷을 통해 RDMA를 구현하는 네트워크 프로토콜입니다. 소프트 로빈은 RoCE v1 및 RoCE v2의 두 프로토콜 버전을 지원하는 RoCE의 소프트웨어 구현입니다. soft-RoCE 드라이버인 rdma_rxe 는 RHEL 8에서 지원되지 않는 기술 프리뷰로 사용할 수 있습니다.

(BZ#1605216)

6.5.3. 하드웨어 활성화

RHEL 8의 기술 프리뷰로 사용 가능한 igc 드라이버

이제 igc Intel 2.5G 이더넷 Linux 유선 LAN 드라이버를 RHEL 8의 모든 아키텍처에서 기술 프리뷰로 사용할 수 있습니다. ethtool 유틸리티는 igc 유선 LAN도 지원합니다.

(BZ#1495358)

6.5.4. 파일 시스템 및 스토리지

NVMe/TCP를 기술 프리뷰로 사용 가능

TCP/IP 네트워크(NVMe/TCP)를 통한 NVMe(Nonvolatile Memory Express) 스토리지 액세스 및 공유 및 해당 nvme-tcp.ko 및 nvmet-tcp.ko 커널 모듈이 기술 프리뷰로 추가되었습니다.

NVMe/TCP를 스토리지 클라이언트 또는 대상으로 사용하는 것은 nvme-cli 및 nvm etcli 패키지에서 제공하는 툴을 사용하여 관리할 수 있습니다.

NVMe/TCP는 RDMA(Remote Direct Memory Access) 및 NVMe(Fibre Channel)를 포함하는 기존 NVMe over Fabrics(NVMe-oF) 전송과 함께 스토리지 전송 옵션을 제공합니다.

(BZ#1696451)

ext4 및 XFS에서 기술 프리뷰로 파일 시스템 DAX 사용 가능

Red Hat Enterprise Linux 8.1에서는 DAX 파일 시스템을 기술 프리뷰로 사용할 수 있습니다. DAX는 애플리케이션이 영구 메모리를 주소 공간으로 직접 매핑할 수 있는 수단을 제공합니다. DAX를 사용하려면 시스템에 몇 가지 형태의 영구 메모리를 사용할 수 있어야 합니다. 일반적으로 하나 이상의 비Volatile 듀얼 인라인 메모리 모듈(NVDIMM) 형식이며 DAX를 지원하는 파일 시스템은 NVDIMM에서 생성해야 합니다. 또한 dax 마운트 옵션을 사용하여 파일 시스템을 마운트해야 합니다. 그런 다음 dax 마운트된 파일 시스템에 있는 파일의 mmap 을 통해 스토리지가 애플리케이션의 주소 공간에 직접 매핑됩니다.

(BZ#1627455)

OverlayFS

Overlayfs는 유니언 파일 시스템 유형입니다. 이를 통해 한 파일 시스템을 다른 파일 시스템에서 오버레이할 수 있습니다. 변경 사항은 상위 파일 시스템에 기록되는 반면 하위 파일 시스템은 수정되지 않았습니다. 이를 통해 여러 사용자가 기본 이미지가 읽기 전용 미디어에 있는 컨테이너 또는 DVD-ROM과 같은 파일 시스템 이미지를 공유할 수 있습니다.
https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt 에 대한 자세한 내용은 Linux 커널 설명서를 참조하십시오.

Overlayfs는 대부분의 환경에서 기술 프리뷰로 남아 있습니다. 따라서 커널은 이 기술이 활성화되면 경고를 기록합니다.

다음 제한 사항에 따라 지원되는 컨테이너 엔진(podman,cri-o 또는 buildah)과 함께 사용할 때 OverlayFS에 완전 지원을 사용할 수 있습니다.

- Overlayfs는 컨테이너 엔진 그래프 드라이버로만 사용됩니다. 이 용도는 영구저장장치가 아닌 컨테이너 COW 콘텐츠에만 지원됩니다. 비OverlayFS 볼륨에 영구 스토리지를 배치해야 합니다. 기본 컨테이너 엔진 구성만 사용할 수 있습니다. 즉, 한 레벨의 오버레이, 한 개의 하위 디렉토리, 하위 수준 및 상위 수준 모두 동일한 파일 시스템에 있습니다.

- 현재 XFS만 더 낮은 계층 파일 시스템으로 사용하도록 지원됩니다.

또한 OverlayFS를 사용하는 경우 다음 규칙과 제한 사항이 적용됩니다.

- OverlayFS 커널 ABI 및 사용자 공간 동작은 안정적이지 않으며 향후 업데이트가 변경될 수 있습니다.

-

Overlayfs는 POSIX 표준의 제한된 집합을 제공합니다. OverlayFS를 사용하여 배포하기 전에 애플리케이션을 철저하게 테스트합니다. 다음 사례는 POSIX와 호환되지 않습니다.

- O_RDONLY 로 열린 하위 파일은 파일을 읽을 때 st_atime 업데이트를 받지 않습니다.
- O_RDONLY 로 더 낮은 파일을 연 다음 MAP_SHARED 로 매핑된 파일은 후속 수정과 일치하지 않습니다.
- 전체 호환 st_ 또는 d_ 값은 RHEL 8에서 기본적으로 활성화되어 있지 않지만 모듈 옵션 또는 마운트 옵션을 사용하여 전체 POSIX 규정 준수를 활성화할 수 있습니다.

  일관된 inode 번호 지정을 얻으려면 x=on 마운트 옵션을 사용합니다.

  redirect_dir=on 및 index=on 옵션을 사용하여 POSIX 규정 준수를 개선할 수도 있습니다. 이 두 가지 옵션은 이러한 옵션 없이 오버레이와 호환되지 않는 상위 계층의 형식을 만듭니다. 즉, redirect_dir=on 또는 index=on 으로 오버레이를 생성하고 오버레이를 마운트 해제한 다음 이러한 옵션 없이 오버레이를 마운트하면 예기치 않은 결과 또는 오류가 발생할 수 있습니다.

- XFS에 사용되는 명령:
  - 오버레이로 사용할 수 있도록 -n ftype=1 옵션을 활성화하여 XFS 파일 시스템을 생성해야 합니다.
  - rootfs 및 시스템 설치 중에 생성된 모든 파일 시스템을 사용하여 Anaconda kickstart 에서 --mkfsoptions=-n ftype=1 매개 변수를 설정합니다.
  - 설치 후 새 파일 시스템을 만들 때 # mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE 명령을 실행합니다.
  - 기존 파일 시스템이 오버레이로 사용할 수 있는지 여부를 확인하려면 # xfs_info /PATH/TO/DEVICE | grep ftype 명령을 실행하여 ftype=1 옵션이 활성화되어 있는지 확인합니다.
- SELinux 보안 레이블은 OverlayFS를 사용하여 지원되는 모든 컨테이너 엔진에서 기본적으로 활성화됩니다.

- 이 릴리스에서 **OverlayFS**와 관련된 몇 가지 알려진 문제가 있습니다. 자세한 내용은 **Linux** 커널 설명서의 *비표준 동작을* 참조하십시오 . https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt.

(BZ#1690207)

Stratis를 기술 프리뷰로 사용 가능

Stratis는 새 로컬 스토리지 관리자입니다. 스토리지 풀에서 사용자에게 추가 기능을 제공하는 관리형 파일 시스템을 제공합니다.

Stratis를 사용하면 다음과 같은 스토리지 작업을 보다 쉽게 수행할 수 있습니다.

- 스냅샷 및 씬 프로비저닝 관리
- 필요에 따라 파일 시스템 크기 자동 확장
- 파일 시스템 관리

Stratis 스토리지를 관리하려면 **stratisd** 백그라운드 서비스와 통신하는 **stratis** 유틸리티를 사용합니다.

Stratis는 기술 프리뷰로 제공됩니다.

자세한 내용은 **Stratis** 설명서를 참조하십시오. **Stratis** 파일 시스템 설정.

(JIRA:RHELPLAN-1212)

IdM 호스트에 로그인한 **IdM** 및 **AD** 사용자가 사용할 수 있는 **Samba** 서버는 **IdM** 도메인 멤버에 기술 프리뷰로 설정할 수 있습니다.

이번 업데이트를 통해 **IdM(Identity Management)** 도메인 멤버에 **Samba** 서버를 설정할 수 있습니다.

동일한 패키지에서 제공하는 새로운 ipa-client-samba 유틸리티는 Samba별 Kerberos 서비스 주체를 IdM에 추가하고 IdM 클라이언트를 준비합니다. 예를 들어 유틸리티는 sss ID 매핑 백엔드에 대한 ID 매핑 구성을 사용하여 /etc/samba/smb.conf 를 만듭니다. 결과적으로 관리자가 IdM 도메인 멤버에 Samba를 설정할 수 있습니다.

IdM Trust 컨트롤러가 글로벌 카탈로그 서비스를 지원하지 않기 때문에 AD-Enrolled Windows 호스트는 Windows에서 IdM 사용자 및 그룹을 찾을 수 없습니다. 또한 IdM Trust 컨트롤러는 분산 컴퓨팅 환경 / DCE/RPC(원격 프로시저 호출) 프로토콜을 사용하여 IdM 그룹 확인을 지원하지 않습니다. 결과적으로 AD 사용자는 IdM 클라이언트의 Samba 공유 및 프린터에만 액세스할 수 있습니다.

자세한 내용은 IdM 도메인 멤버에서 Samba 설정을 참조하십시오.

(JIRA:RHELPLAN-13195)

6.5.5. 고가용성 및 클러스터

Pacemaker podman 번들을 기술 프리뷰로 이용 가능

이제 Pacemaker 컨테이너 번들은 기술 프리뷰로 사용할 수 있는 컨테이너 번들 기능과 함께 podman 컨테이너 플랫폼에서 실행됩니다. 이 기능에는 기술 프리뷰가 한 가지 예외가 있습니다. Red Hat은 Red Hat Openstack을 위한 Pacemaker 번들 사용을 완전히 지원합니다.

(BZ#1619620)

corosync-qdevice 의 추론을 기술 프리뷰로 사용 가능

복구는 시작 시 로컬로 실행되는 명령 집합, 클러스터 멤버십 변경, 성공적으로 연결되고 corosync-qnetd 에 연결되며 선택적으로 주기적으로 실행됩니다. 모든 명령이 시간에 성공적으로 완료되면(반환 오류 코드가 0임) 추론이 전달되고, 그렇지 않으면 실패합니다. 추론 결과는 corosync-qnetd 로 전송됩니다. 여기서 어떤 파티션을 정족수로 결정하기 위해 계산에 사용됩니다.

(BZ#1784200)

새로운 fence-agents-heuristics-ping 펜스 에이전트

Pacemaker는 기술 프리뷰로 fence_heuristics_ping 에이전트를 지원합니다. 이 에이전트는 자체적으로 실제 펜싱을 수행하지 않고 새로운 방식으로 펜싱 수준의 동작을 활용하는 실험적 펜스 에이전트 클래스를 여는 것을 목표로 합니다.

복구 에이전트가 실제 펜싱을 수행하지만 순서대로 구성되기 전에 펜싱을 구성하는 펜스 에이전트와 동일한 펜싱 수준에서 구성된 경우 펜싱은 펜싱을 수행하는 에이전트에서 복구 에이전트에서 끄기 조치를 수행합니다. 복구 에이전트가 off 조치에 대해 부정적인 결과를 제공하는 경우 펜싱 수준이 성공하지 않을 것으로 이미 명확하여 Pacemaker 펜싱에서 펜싱을 수행하는 에이전트에서 off 조치를 건너뛰는 단계를 건너뜁니다. 복구 에이전트는 이 동작을 악용하여 실제 펜싱이 특정 조건에서 노드를 펜싱하지 못하도록 할 수 있습니다.

사용자가 이 에이전트(특히 2-노드 클러스터에서)를 사용하기를 원할 수 있습니다. 이전에 알 수 있는 경우 노드가 피어를 펜싱하는 것이 적절하지 않을 수 있습니다. 예를 들어, 네트워킹 업링크에 도달하는 데 문제가 있는 경우 노드에서 서비스를 인계받는 것이 적절하지 않을 수 있으며, 이러한 경우 라우터에 대한 ping이 탐지될 수 있는 클라이언트에서 서비스에 연결할 수 없습니다.

(BZ#1775847)

6.5.6. IdM (Identity Management)

ID 관리 JSON-RPC API를 기술 프리뷰로 사용 가능

IdM(Identity Management)에 API를 사용할 수 있습니다. API를 보기 위해 IdM은 API 브라우저도 기술 프리뷰로 제공합니다.

Red Hat Enterprise Linux 7.3에서 IdM API는 여러 버전의 API 명령을 사용하도록 향상되었습니다. 이전에는 개선 사항이 호환되지 않는 방식으로 명령의 동작을 변경할 수 있었습니다. 이제 IdM API가 변경되더라도 사용자가 기존 툴 및 스크립트를 계속 사용할 수 있습니다. 이를 통해 다음을 수행할 수 있습니다.

- 관리자는 관리 클라이언트보다 이전 버전 이상의 IdM을 사용합니다.
- 서버에서 IdM 버전이 변경되더라도 개발자는 특정 버전의 IdM 호출을 사용합니다.

모든 경우에 한 쪽이 사용하더라도 서버 간 통신이 가능합니다(예: 기능에 대한 새로운 옵션을 도입하는 최신 버전).

API 사용에 대한 자세한 내용은 IdM 서버와 커밋하기 위해 ID 관리 API 사용을 참조하십시오(기술 PREVIEW). https://access.redhat.com/articles/2728021

(BZ#1664719)

IdM에서 DNSSEC 사용 가능

통합된 DNS가 있는 IdM(Identity Management) 서버는 DNS 프로토콜의 보안을 강화하는 DNS로의 확장 기능 세트인 DNSSEC(DNS Security Extensions)를 지원합니다. IdM 서버에서 호스팅되는 DNS 영역은 DNSSEC를 사용하여 자동으로 서명할 수 있습니다. 암호화 키는 자동으로 생성되고 순환됩니다.

DNSSEC를 사용하여 DNS 영역을 보안하기로 결정한 사용자는 다음 문서를 읽고 따르는 것이 좋습니다.

- DNSSEC 운영 사례, 버전 2: http://tools.ietf.org/html/rfc6781#section-2
- 보안 도메인 이름 시스템 (DNS) 배포 가이드 : http://dx.doi.org/10.6028/NIST.SP.800-81-2
- DNSSEC 키 롤오버 타이밍 고려 사항: http://tools.ietf.org/html/rfc7583

통합된 DNS가 있는 IdM 서버는 DNSSEC를 사용하여 다른 DNS 서버에서 얻은 DNS 응답을 확인합니다. 이는 권장 명명 방식에 따라 구성되지 않은 DNS 영역의 가용성에 영향을 줄 수 있습니다.

(BZ#1664718)

6.5.7. 그래픽 인프라

VNC 원격 콘솔은 64비트 ARM 아키텍처에 대한 기술 프리뷰로 사용 가능

64비트 ARM 아키텍처에서 VNC(Virtual Network Computing) 원격 콘솔은 기술 프리뷰로 사용할 수 있습니다. 나머지 그래픽 스택은 현재 64비트 ARM 아키텍처에 대해 확인되지 않습니다.

(BZ#1698565)

6.5.8. Red Hat Enterprise Linux 시스템 역할

RHEL 시스템 역할의 postfix 역할을 기술 프리뷰로 사용 가능

Red Hat Enterprise Linux 시스템 역할은 Red Hat Enterprise Linux 하위 시스템에 대한 구성 인터페이스를 제공하므로 Ansible 역할을 포함하여 시스템 구성이 더 쉬워집니다. 이 인터페이스를 사용하면

여러 버전의 **Red Hat Enterprise Linux**에서 시스템 구성을 관리할 수 있을 뿐 아니라 새로운 주요 릴리스를 채택할 수 있습니다.

rhel-system-roles 패키지는 **AppStream** 리포지토리를 통해 배포됩니다.

postfix 역할은 기술 프리뷰로 사용할 수 있습니다.

다음 역할은 완전히 지원됩니다.

- **kdump**
- **network**
- **selinux**
- **storage**
- **timesync**

자세한 내용은 **RHEL 시스템 역할에 대한 지식베이스 문서를 참조하십시오**.

(BZ#1812552)

rhel-system-roles-sap 을 기술 프리뷰로 이용 가능

rhel-system-roles-sap 패키지는 **SAP** 워크로드를 실행하기 위해 **RHEL** 시스템의 구성을 자동화하는 데 사용할 수 있는 **SAP**용 **RHEL(Red Hat Enterprise Linux)** 시스템 역할을 제공합니다. 이러한 역할은 관련 **SAP Notes**에 설명된 모범 사례를 기반으로 하는 최적의 설정을 자동으로 적용하여 **SAP** 워크로드를 실행하는 시스템을 구성하는 시간을 크게 단축합니다. 액세스는 **SAP** 솔루션용 **RHEL**로 제한됩니다. 서브스크립션에 대한 지원이 필요한 경우 **Red Hat** 고객 지원에 문의하십시오.

rhel-system-roles-sap 패키지의 새로운 역할은 기술 프리뷰로 사용할 수 있습니다.

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

자세한 내용은 SAP용 Red Hat Enterprise Linux 시스템 역할을 참조하십시오.

참고: RHEL 8.1 for SAP Solutions는 Intel 64 아키텍처 및 IBM POWER9에서 SAP HANA와 함께 사용할 수 있도록 검증될 예정입니다. SAP NetWeaver 및 SAP ASE와 같은 기타 SAP 애플리케이션 및 데이터베이스 제품에서는 RHEL 8.1 기능을 사용할 수 있습니다. 검증된 릴리스 및 SAP 지원에 대한 최신 정보는 SAP Notes 2369910 및 2235581을 참조하십시오.

(BZ#1660832)

rhel-system-roles-sap 이 버전 1.1.1로 업데이트

RHBA-2019:4258 권고를 통해 여러 버그 수정을 제공하도록 rhel-system-roles-sap 패키지가 업데이트되었습니다. 특히:

- 영어 이외의 로케일이 있는 호스트에서 SAP 시스템 역할 작업
- kernel.pid_max 는 sysctl 모듈에 의해 설정됩니다.
- nproc 는 HANA에 대해 무제한으로 설정되어 있습니다(SAP 참고 2772999 단계 9 참조)
- 하드 프로세스 제한은 소프트 프로세스 제한 전에 설정됩니다.
- 프로세스 제한을 설정하는 코드는 이제 역할 sap-preconfigure와 동일하게 작동합니다.
- handlers/main.yml 은 비uefi 시스템에서만 작동하며 uefi 시스템에서 자동으로 무시됩니다.

- rhel-system-roles에 사용하지 않는 종속성 제거
- sap_hana_preconfigure_packages에서 libssh2 제거
- 특정 CPU 설정이 지원되지 않을 때 실패를 방지하기 위해 추가 검사 추가
- 모든 true 및 false를 소문자로 변환
- 업데이트된 최소 패키지 처리
- 호스트 이름 및 도메인 이름이 올바르게 설정되었습니다
- 많은 마이너 수정

rhel-system-roles-sap 패키지는 기술 프리뷰로 사용할 수 있습니다.

(BZ#1766622)

6.5.9. 가상화

Intel 네트워크 어댑터가 Hyper-V의 RHEL 게스트에서 SR-IOV 지원

Hyper-V 하이퍼바이저에서 실행되는 Red Hat Enterprise Linux 게스트 운영 체제는 이제 ixgbevf 및 iavf 드라이버에서 지원하는 Intel 네트워크 어댑터에 SR-IOV(Single-root I/O Virtualization) 기능을 사용할 수 있습니다. 이 기능은 다음 조건이 충족되면 활성화됩니다.

- NIC(네트워크 인터페이스 컨트롤러)에 SR-IOV 지원이 활성화됨
- 가상 NIC에 대해 SR-IOV 지원이 활성화됨

- 가상 스위치에 SR-IOV 지원이 활성화됨
- NIC의 VF(가상 기능)가 가상 머신에 연결되어 있습니다.

이 기능은 현재 Microsoft Windows Server 2019 및 2016에서 지원됩니다.

(BZ#1348508)

RHEL 8 Hyper-V 가상 머신에서 KVM 가상화 사용 가능

이제 Microsoft Hyper-V 하이퍼바이저에서 중첩된 KVM 가상화를 기술 프리뷰로 사용할 수 있습니다. 결과적으로 Hyper-V 호스트에서 실행 중인 RHEL 8 게스트 시스템에 가상 머신을 생성할 수 있습니다.

현재 이 기능은 Intel 시스템에서만 작동합니다. 또한 중첩된 가상화는 Hyper-V에서 기본적으로 활성화되어 있지 않은 경우도 있습니다. 이를 활성화하려면 다음 Microsoft 문서를 참조하십시오.

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

(BZ#1519039)

KVM 가상 머신용 AMD SEV

RHEL 8은 KVM 하이퍼바이저를 사용하는 AMD EPYC 호스트 시스템을 위한 SEV(Secure Encrypted Virtualization) 기능을 기술 프리뷰로 도입하고 있습니다. 가상 머신(VM)에서 활성화된 경우 SEV는 VM 메모리를 암호화하여 호스트가 VM의 데이터에 액세스할 수 없도록 합니다. 이제 호스트가 악성 코드에에 의해 감염된 경우 VM의 보안이 향상됩니다.

단일 호스트에서 이 기능을 한 번에 사용할 수 있는 VM의 개수는 호스트 하드웨어에 의해 결정됩니다. 현재 AMD EPYC 프로세서는 SEV를 사용하여 최대 15개의 실행 중인 VM을 지원합니다.

또한 부팅할 수 있도록 SEV가 구성된 VM의 경우 하드 메모리 제한으로 VM을 구성해야 합니다. 이를 수행하려면 VM의 XML 구성에 다음을 추가합니다.

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

N에 권장되는 값은 게스트 RAM + 256MiB보다 크거나 같습니다. 예를 들어 게스트에 2GiB RAM이 할당되면 N은 2359296 이상이어야 합니다.

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

Intel vGPU

이제 기술 프리뷰로 물리적 Intel GPU 장치를 중재 장치라고 하는 여러 가상 장치로 나눌 수 있습니다. 그런 다음 이러한 중재된 장치를 여러 VM(가상 머신)에 가상 GPU로 할당할 수 있습니다. 결과적으로 이러한 VM은 단일 물리적 Intel GPU의 성능을 공유합니다.

선택한 Intel GPU만 vGPU 기능과 호환됩니다. 또한 VM에 물리적 GPU를 할당하면 호스트가 GPU를 사용할 수 없으며 호스트의 그래픽 디스플레이 출력이 작동하지 않을 수 있습니다.

(BZ#1528684)

IBM POWER 9에서 중첩된 가상화 사용 가능

이제 IBM POWER 9 시스템에서 실행 중인 RHEL 8 호스트 시스템에서 기술 프리뷰로 중첩된 가상화 기능을 사용할 수 있습니다. 중첩된 가상화를 통해 KVM 가상 머신(VM)이 하이퍼바이저로 작동하여 VM 내에서 VM을 실행할 수 있습니다.

중첩된 가상화도 AMD64 및 Intel 64 시스템에서 기술 프리뷰로 유지됩니다.

또한 중첩된 가상화가 IBM POWER 9에서 작동하려면 호스트, 게스트 및 중첩된 게스트가 현재 다음 운영 체제 중 하나를 실행해야 합니다.

- RHEL 8
- POWER 9용 RHEL 7

(BZ#1505999, BZ#1518937)

중첩된 가상 머신 생성

RHEL 8의 KVM 가상 머신(VM)에 중첩된 가상화를 기술 프리뷰로 사용할 수 있습니다. 이 기능을 사용하면 물리적 호스트에서 실행되는 VM이 하이퍼바이저 역할을 하며 고유한 VM을 호스팅할 수 있습니다.

중첩된 가상화는 AMD64 및 Intel 64 아키텍처에서만 사용할 수 있으며 중첩 호스트는 RHEL 7 또는 RHEL 8 VM이어야 합니다.

(JIRA:RHELPLAN-14047)

6.5.10. 컨테이너

podman-machine 명령은 지원되지 않음

가상 머신을 관리하는 podman-machine 명령은 기술 프리뷰로만 사용할 수 있습니다. 대신 명령줄에서 직접 Podman을 실행합니다.

(JIRA:RHELDOCS-16861)

6.6. 사용되지 않는 기능

이 부분에서는 Red Hat Enterprise Linux 8.1에서 *더 이상 사용되지* 않는 기능에 대한 개요를 제공합니다.

사용되지 않는 기능은 이 제품의 향후 주요 릴리스에서 지원되지 않을 가능성이 높으며 새로운 배포에 구현하는 것은 권장되지 않습니다. 특정 주요 릴리스 내에서 더 이상 사용되지 않는 기능의 최신 목록은 최신 릴리스 노트를 참조하십시오.

더 이상 사용되지 않는 기능의 지원 상태는 Red Hat Enterprise Linux 8에서는 변경되지 않습니다. 지원 기간에 대한 자세한 내용은 Red Hat Enterprise Linux 라이프 사이클 및 Red Hat Enterprise Linux Application Streams 라이프 사이클을 참조하십시오.

사용되지 않는 하드웨어 구성 요소는 현재 또는 향후 주요 릴리스의 새로운 배포에 구현하는 것을 권장하지 않습니다. 하드웨어 드라이버 업데이트는 보안 및 중요 수정 사항으로만 제한됩니다. Red Hat은 최

대한 빠른 시일 내에 이 하드웨어를 교체할 것을 권장합니다.

패키지가 더 이상 사용되지 않으며 향후 사용이 권장되지 않는 경우가 있습니다. 경우에 따라 패키지가 제품에서 삭제될 수 있습니다. 제품 설명서에 더 이상 사용되지 않는 기능과 유사 또는 동일하거나 보다 고급 기능을 제공하는 최근 패키지가 지정된 권장 사항이 기재됩니다.

RHEL 7에 있지만 **RHEL 8**에서 *제거된* 기능에 관한 자세한 내용은 **RHEL 8** 채택 고려 사항을 참조하십시오.

6.6.1. 설치 프로그램 및 이미지 생성

몇 가지 Kickstart 명령 및 옵션이 더 이상 사용되지 않음

RHEL 8 Kickstart 파일에서 다음 명령과 옵션을 사용하면 로그에 경고가 출력됩니다.

- **auth** 또는 **authconfig**
- **device**
- **deviceprobe**
- **dmraid**
- **install**
- **lilo**
- **lilocheck**
- 마우스
- 다중 경로

- **bootloader --upgrade**
- **ignoredisk --interactive**
- 파티션 **--active**
- **reboot --kexec**

특정 옵션만 나열되는 경우 기본 명령 및 해당 기타 옵션은 계속 사용할 수 있으며 더 이상 사용되지 않습니다.

Kickstart에 대한 자세한 내용 및 관련 변경 사항은 ***RHEL 8 채택 시 고려 사항의*** **Kickstart 변경** 섹션을 참조하십시오.

(BZ#1642765)

ignoredisk Kickstart 명령의 **--interactive** 옵션이 더 이상 사용되지 않음

Red Hat Enterprise Linux의 향후 릴리스에서 **--interactive option**을 사용하면 치명적인 설치 오류가 발생합니다. 옵션을 제거하려면 **Kickstart** 파일을 수정하는 것이 좋습니다.

(BZ#1637872)

6.6.2. 소프트웨어 관리

rpmbuild --sign 명령이 더 이상 사용되지 않음

이번 업데이트를 통해 **rpmbuild --sign** 명령이 더 이상 사용되지 않습니다. **Red Hat Enterprise Linux**의 향후 릴리스에서 이 명령을 사용하면 오류가 발생할 수 있습니다. 대신 **rpmsign** 명령을 사용하는 것이 좋습니다.

(**BZ#1688849**)

6.6.3. 보안

TLS 1.0 및 TLS 1.1이 더 이상 사용되지 않음

TLS 1.0 및 TLS 1.1 프로토콜은 DEFAULT 시스템 전체 암호화 정책 수준에서 비활성화됩니다. 예를 들어 Firefox 웹 브라우저에서 비디오 회의 애플리케이션을 시나리오에 사용해야 하는 경우 더 이상 사용되지 않는 프로토콜을 사용해야 하는 경우 시스템 전체 암호화 정책을 LEGACY 수준으로 전환합니다.

```
# update-crypto-policies --set LEGACY
```

자세한 내용은 RHEL 8의 powerful crypto defaults 및 Red Hat Customer Portal의 약한 암호화 알고리즘 지식 베이스 문서 및 update-crypto-policies(8) 도움말 페이지를 참조하십시오.

(BZ#1660839)

RHEL 8에서 DSA 사용 중단

Red Hat Enterprise Linux 8에서는 DSA(Digital Signature Algorithm)가 더 이상 사용되지 않습니다. DSA 키에 의존하는 인증 메커니즘은 기본 구성에서 작동하지 않습니다. OpenSSH 클라이언트는 LEGACY 시스템 전체 암호화 정책 수준에서도 DSA 호스트 키를 허용하지 않습니다.

(BZ#1646541)

SSL2 Client Hello가 NSS에서 더 이상 사용되지 않음

TLS(Transport Layer Security) 프로토콜 버전 1.2 이전의 SSL(Secure Sockets Layer) 프로토콜 버전 2와 역호환되는 방식으로 서식이 지정된 Client Hello 메시지와 협상을 시작할 수 있습니다. NSS(Network Security Services) 라이브러리에서 이 기능에 대한 지원은 더 이상 사용되지 않으며 기본적으로 비활성화되어 있습니다.

이 기능에 대한 지원이 필요한 애플리케이션은 새로운 SSL_ENABLE_V2_COMPATIBLE_HELLO API를 사용하여 활성화해야 합니다. 이 기능에 대한 지원은 Red Hat Enterprise Linux 8의 이후 릴리스에서 완전히 삭제될 수 있습니다.

(BZ#1645153)

TPM 1.2가 더 이상 사용되지 않음

TPM(신뢰할 수 있는 플랫폼 모듈) 보안 암호화 프로세서 표준 버전이 2016년 버전 2.0으로 업데이트되었습니다. TPM 2.0은 TPM 1.2보다 많은 개선 사항을 제공하며 이전 버전과는 역호환되지 않습니다. RHEL 8에서는 TPM 1.2가 더 이상 사용되지 않으며 다음 주요 릴리스에서 제거될 수 있습니다.

(BZ#1657927)

6.6.4. 네트워킹

RHEL 8에서 네트워크 스크립트가 더 이상 사용되지 않음

네트워크 스크립트가 Red Hat Enterprise Linux 8에서 더 이상 사용되지 않으므로 이제 기본적으로 제공되지 않습니다. 기본 설치는 nmcli 툴을 통해 NetworkManager 서비스를 호출하는 ifup 및 ifdown 스크립트의 새 버전을 제공합니다. Red Hat Enterprise Linux 8에서 ifup 및 ifdown 스크립트를 실행하려면 NetworkManager를 실행해야 합니다.

/sbin/ifup-local, ifdown-pre-local 및 ifdown-local 스크립트에서 사용자 지정 명령이 실행되지 않습니다.

이러한 스크립트가 필요한 경우 다음 명령을 사용하여 시스템에서 더 이상 사용되지 않는 네트워크 스크립트를 설치할 수 있습니다.

```
~]# yum install network-scripts
```

ifup 및 ifdown 스크립트는 설치된 레거시 네트워크 스크립트에 연결됩니다.

레거시 네트워크 스크립트를 호출하면 사용 중단을 알리는 경고 메시지가 표시됩니다.

(BZ#1647725)

6.6.5. 커널

디스크리스 부팅이 더 이상 사용되지 않음

디스크리스 부팅을 사용하면 여러 시스템에서 네트워크를 통해 루트 파일 시스템을 공유할 수 있습니다. 편리하지만 실시간 워크로드에서 네트워크 대기 시간을 소개하기 쉽습니다. 향후 RHEL for Real Time 8의 마이너 업데이트에서는 더 이상 디스크리스 부팅이 지원되지 않습니다.

(BZ#1748980)

The rdma_rxe soft -RoCE 드라이버는 더 이상 사용되지 않습니다.

소프트웨어 RXE(Remote Direct Memory Access over Converged Ethernet)는 RDMA(Remote Direct Memory Access)를 에뮬레이션하는 기능입니다. RHEL 8에서는 soft-RoCE 기능은 지원되지 않는 기술 프리뷰로 사용할 수 있습니다. 그러나 안정성 문제로 인해 이 기능은 더 이상 사용되지 않으며 RHEL 9에서 제거됩니다.

(BZ#1878207)

6.6.6. 하드웨어 활성화

qla3xxx 드라이버가 더 이상 사용되지 않음

RHEL 8에서는 qla3xxx 드라이버가 더 이상 사용되지 않습니다. 드라이버는 이 제품의 향후 주요 릴리스에서 지원되지 않을 가능성이 크므로 새로운 배포에 권장되지 않습니다.

(BZ#1658840)

dl2k,dnet,ethoc 및 dlci 드라이버는 더 이상 사용되지 않습니다.

RHEL 8에서는 dl2k,dnet,ethoc 및 dlci 드라이버가 더 이상 사용되지 않습니다. 드라이버는 이 제품의 향후 주요 릴리스에서 지원되지 않을 가능성이 크므로 새로운 배포에 권장되지 않습니다.

(BZ#1660627)

6.6.7. 파일 시스템 및 스토리지

종료된 커널 명령줄 매개변수는 더 이상 사용되지 않습니다.

이전 RHEL 릴리스에서는 모든 장치에 대한 디스크 스케줄러를 설정하는 데 종료된 커널 명령줄 매개변수가 사용되었습니다. RHEL 8에서는 매개 변수가 더 이상 사용되지 않습니다.

업스트림 Linux 커널은 구성요소 매개 변수에 대한 지원을 제거했지만 호환성을 위해 RHEL 8에서 계속 사용할 수 있습니다.

커널은 장치 유형에 따라 기본 디스크 스케줄러를 선택합니다. 일반적으로 최적의 설정입니다. 다른 스케줄러가 필요한 경우 udev 규칙 또는 Tuned 서비스를 사용하여 구성하는 것이 좋습니다. 선택한 장치와 일치하고 해당 장치에 대해서만 스케줄러를 전환합니다.

자세한 내용은 디스크 스케줄러 설정을 참조하십시오.

(BZ#1665295)

UDP를 통한 NFSv3이 비활성화

NFS 서버는 기본적으로 더 이상 UDP(User Datagram Protocol) 소켓을 열거나 수신하지 않습니다. 버전 4는 TCP(Transmission Control Protocol)가 필요하기 때문에 이 변경은 NFS 버전 3에만 영향을 미칩니다.

RHEL 8에서는 UDP를 통한 NFS가 더 이상 지원되지 않습니다.

(BZ#1592011)

6.6.8. 데스크탑

libgnome-keyring 라이브러리가 더 이상 사용되지 않음

libgnome-keyring 은 업스트림에서 유지 관리되지 않으며 RHEL에 필요한 암호화 정책을 따르지 않으므로 libgnome-keyring 라이브러리는 lib secret 라이브러리를 대신하여 더 이상 사용되지 않습니다. 새로운 libsecret 라이브러리는 필요한 보안 표준을 따르는 교체입니다.

(BZ#1607766)

6.6.9. 그래픽 인프라

AGP 그래픽 카드는 더 이상 지원되지 않습니다.

AGP(Acccelerated Graphics Port) 버스를 사용하는 그래픽 카드는 Red Hat Enterprise Linux 8에서는 지원되지 않습니다. PCI-Express 버스를 사용하는 그래픽 카드를 권장되는 대체로 사용합니다.

(BZ#1569610)

6.6.10. 웹 콘솔

웹 콘솔에서 더 이상 불완전한 번역을 지원하지 않습니다

RHEL 웹 콘솔은 더 이상 콘솔의 번역 가능한 문자열의 50% 미만으로 사용할 수 있는 언어에 대한 번역을 제공하지 않습니다. 브라우저가 이러한 언어로 번역을 요청하는 경우 사용자 인터페이스는 대신 영어로 진행됩니다.

(BZ#1666722)

6.6.11. 가상화

virt-manager가 더 이상 사용되지 않음

virt-manager라고도 하는 Virtual Machine Manager 애플리케이션은 더 이상 사용되지 않습니다. Cockpit라고도 하는 RHEL 8 웹 콘솔은 후속 릴리스에서 교체될 예정입니다. 따라서 GUI에서 가상화를 관리하기 위해 웹 콘솔을 사용하는 것이 좋습니다. 그러나 virt-manager 에서 사용할 수 있는 일부 기능은 아직 RHEL 8 웹 콘솔을 사용할 수 없다는 점에 유의하십시오.

(JIRA:RHELPLAN-10304)

RHEL 8에서 가상 머신 스냅샷이 올바르게 지원되지 않음

가상 머신(VM) 스냅샷을 생성하는 현재 메커니즘이 안정적으로 작동하지 않기 때문에 더 이상 사용되지 않습니다. 따라서 RHEL 8에서 VM 스냅샷을 사용하지 않는 것이 좋습니다.

새로운 VM 스냅샷 메커니즘이 개발 중이며 향후 RHEL 8의 마이너 릴리스에서 완전히 구현될 예정입니다.

(BZ#1686057)

Cirrus VGA 가상 GPU 유형이 더 이상 사용되지 않음

향후 Red Hat Enterprise Linux에 대한 주요 업데이트가 있을 경우 KVM 가상 머신에서 Cirrus VGA GPU 장치가 더 이상 지원되지 않습니다. 따라서 Red Hat은 Cirrus VGA 대신 stdvga, virtio-vga 또는 qxl 장치 사용을 권장합니다.

(BZ#1651994)

6.6.12. 사용되지 않는 패키지

다음 패키지는 더 이상 사용되지 않으며 향후 Red Hat Enterprise Linux 주요 릴리스에 포함되지 않을

수 있습니다.

- **389-ds-base-legacy-tools**
- **authd**
- **custodia**
- 호스트 이름
- **libidn**
- **net-tools**
- **network-scripts**
- **nss-pam-ldapd**
- **sendmail**
- **jp-tools**
- **ypbind**
- **ypserv**

6.7. 확인된 문제

다음 부분에서는 **Red Hat Enterprise Linux 8**의 알려진 문제에 대해 설명합니다.

6.7.1. 설치 프로그램 및 이미지 생성

auth 및 authconfig Kickstart 명령에는 AppStream 리포지토리가 필요

authselect-compat 패키지는 설치하는 동안 auth 및 authconfig Kickstart 명령이 필요합니다. 이 패키지가 없으면 auth 또는 authconfig가 사용되는 경우 설치에 실패합니다. 설계에 따라 authselect-compat 패키지는 AppStream 리포지토리에서만 사용할 수 있습니다.

이 문제를 해결하려면 설치 프로그램에 BaseOS 및 AppStream 리포지토리를 사용할 수 있는지 확인하거나 설치 중에 authselect Kickstart 명령을 사용합니다.

(BZ#1640697)

reboot --kexec 및 inst.kexec 명령은 예측 가능한 시스템 상태를 제공하지 않습니다.

reboot --kexec Kickstart 명령 또는 inst.kexec 커널 부팅 매개 변수를 사용하여 RHEL 설치를 수행해도 전체 재부팅과 동일한 예측 가능한 시스템 상태를 제공하지 않습니다. 결과적으로 재부팅하지 않고 설치된 시스템으로 전환하면 예측할 수 없는 결과가 발생할 수 있습니다.

kexec 기능은 더 이상 사용되지 않으며 향후 Red Hat Enterprise Linux 릴리스에서 제거됩니다.

(BZ#1697896)

Anaconda 설치에는 최소한의 리소스 설정 요구 사항의 낮은 제한이 포함되어 있습니다.

Anaconda는 사용 가능한 최소한의 리소스 설정이 있는 시스템에서 설치를 시작하고 성공적으로 설치를 수행하는 데 필요한 리소스에 대한 이전 메시지를 제공하지 않습니다. 결과적으로 설치에 실패할 수 있으며 출력 오류가 가능한 디버그 및 복구를 위한 명확한 메시지를 제공하지 않습니다. 이 문제를 해결하려면 시스템에 설치에 필요한 최소한의 리소스 설정이 있는지 확인합니다. PPC64(LE)의 메모리 2GB, x86_64의 경우 1GB. 따라서 성공적으로 설치를 수행할 수 있어야 합니다.

(BZ#1696609)

reboot --kexec 명령을 사용하는 경우 설치 실패

reboot --kexec 명령이 포함된 Kickstart 파일을 사용하면 RHEL 8 설치에 실패합니다. 문제를 방지하려면 Kickstart 파일에서 reboot --kexec 대신 reboot 명령을 사용합니다.

(BZ#1672405)

설치 프로그램에서 s390x의 보안 부팅 지원

RHEL 8.1은 보안 부팅 사용을 적용하는 IBM Z 환경에서 사용하기 위한 부팅 디스크를 준비하도록 지원합니다. 설치 중에 사용되는 서버 및 하이퍼바이저의 기능은 디스크상의 디스크 형식에 보안 부팅 지원이 포함되어 있는지 확인합니다. 설치 중에 디스크 형식에 영향을 줄 수 있는 방법은 없습니다.

따라서 보안 부팅을 지원하는 환경에 RHEL 8.1을 설치하는 경우 일부 장애 조치 시나리오에서 수행되므로 보안 부팅 지원이 부족한 환경으로 이동할 때 시스템을 부팅할 수 없습니다.

이 문제를 해결하려면 디스크 부팅 형식을 제어하는 zipl 도구를 구성해야 합니다. 실행 환경에서 보안 부팅을 지원하는 경우에도 이전 디스크 형식을 작성하도록 zipl 을 구성할 수 있습니다. RHEL 8.1 설치가 완료되면 다음 수동 단계를 root 사용자로 수행합니다.

1. 설정 파일 /etc/zipl.conf을 편집합니다.

2. "secure=0"을 포함하는 행을 "defaultboot"라고 레이블이 지정된 섹션에 추가합니다.

   Example contents of the `zipl.conf` file after the change:

   ```
   [defaultboot]
   defaultauto
   prompt=1
   timeout=5
   target=/boot
   secure=0
   ```

3. 매개 변수없이 zipl 도구를 실행합니다

이러한 단계를 수행해도 RHEL 8.1 부팅 디스크의 디스크 형식에는 더 이상 보안 부팅 지원이 포함되지 않습니다. 따라서 안전한 부팅 지원이 없는 환경에서 설치를 부팅할 수 있습니다.

(BZ#1659400)

RHEL 8 초기 설정은 SSH를 통해 수행할 수 없습니다.

현재 SSH를 사용하여 시스템에 로그인하면 RHEL 8 초기 설정 인터페이스가 표시되지 않습니다. 따

라서 SSH를 통해 관리되는 RHEL 8 시스템에서는 초기 설정을 수행할 수 없습니다. 이 문제를 해결하려면 기본 시스템 콘솔(ttyS0)에서 초기 설정을 수행하고 나중에 SSH를 사용하여 로그인합니다.

(BZ#1676439)

secure= 부팅 옵션의 기본값은 auto로 설정되어 있지 않습니다.

현재 secure= 부팅 옵션의 기본값은 auto로 설정되지 않습니다. 결과적으로 현재 기본값이 비활성화되어 있으므로 보안 부팅 기능을 사용할 수 없습니다. 이 문제를 해결하려면 /etc/zipl.conf 파일의 [defaultboot] 섹션에서 secure=auto 를 수동으로 설정합니다. 따라서 보안 부팅 기능을 사용할 수 있습니다. 자세한 내용은 zipl.conf 도움말 페이지를 참조하십시오.

(BZ#1750326)

Binary DVD.iso 파일의 내용을 파티션에 복사해도 .treeinfo 및 .discinfo 파일이 복사되지 않음

로컬 설치 중에 RHEL 8 바이너리 DVD.iso 이미지 파일의 내용을 파티션에 복사하는 동안 cp <path>/* <mounted partition>/dir 명령의 * 는 .treeinfo 및. discinfo 파일을 복사하지 못합니다. 이러한 파일은 성공적으로 설치되어야 합니다. 결과적으로 BaseOS 및 AppStream 리포지토리가 로드되지 않으며 anaconda.log 파일의 디버그 관련 로그 메시지가 문제의 유일한 레코드입니다.

이 문제를 해결하려면 누락된 .treeinfo 및 .discinfo 파일을 파티션에 복사하십시오.

(BZ#1687747)

Kickstart 설치에는 자체 서명 HTTPS 서버를 사용할 수 없습니다.

현재 설치 소스가 Kickstart 파일에 지정되고 --noverifyssl 옵션이 사용되는 경우 자체 서명된 https 서버에서 설치 프로그램이 설치되지 않습니다.

```
url --url=https://SERVER/PATH --noverifyssl
```

이 문제를 해결하려면 kickstart 설치를 시작할 때 커널 명령줄에 inst.noverifyssl 매개 변수를 추가합니다.

예를 들면 다음과 같습니다.

```
inst.ks=<URL> inst.noverifyssl
```

(BZ#1745064)

6.7.2. 소프트웨어 관리

yum repolist 는 skip_if_unavailable=false를 사용하여 처음 사용할 수 없는 리포지토리에서 종료됩니다.

리포지토리 구성 옵션 skip_if_unavailable 은 기본적으로 다음과 같이 설정됩니다.

```
skip_if_unavailable=false
```

이 설정은 yum repolist 명령이 처음 사용할 수 없는 리포지토리에서 오류, 종료 상태 1에서 강제로 종료되도록 합니다. 결과적으로 yum repolist 는 사용 가능한 리포지토리를 계속 나열하지 않습니다.

각 리포지토리의 *.repo 파일에서 이 설정을 재정의할 수 있습니다.

그러나 기본 설정을 유지하려면 다음 옵션을 사용하여 yum repolist 를 사용하여 문제를 해결할 수 있습니다.

```
--setopt=*.skip_if_unavailable=True
```

(BZ#1697472)

6.7.3. 서브스크립션 관리

syspurpose 애드온은 subscription-manager attach --auto 출력에 아무 영향을 미치지 않습니다.

Red Hat Enterprise Linux 8에서는 syspurpose 명령줄 툴의 4가지 속성(role,usage, service_level_agreement, addons)이 추가되었습니다. 현재는 role,usage 및 service_level_agreement 만 subscription-manager attach --auto 명령을 실행하는 출력에 영향을 미칩니다. addons 인수에 값을 설정하려는 사용자는 자동 연결된 서브스크립션에 어떤 영향을 미치지 않습니다.

(BZ#1687900)

6.7.4. 쉘 및 명령행 툴

Wayland 프로토콜을 사용하는 애플리케이션은 원격 디스플레이 서버로 전달할 수 없습니다.

Red Hat Enterprise Linux 8.1에서 대부분의 애플리케이션은 기본적으로 X11 프로토콜 대신 Wayland 프로토콜을 사용합니다. 결과적으로 ssh 서버는 Wayland 프로토콜을 사용하는 애플리케이션을 전달할 수 없지만 X11 프로토콜을 사용하는 애플리케이션을 원격 디스플레이 서버로 전달할 수 있습니다.

이 문제를 해결하려면 애플리케이션을 시작하기 전에 환경 변수 GDK_BACKEND=x11 을 설정합니다. 그 결과 애플리케이션을 원격 디스플레이 서버로 전달할 수 있습니다.

(BZ#1686892)

systemd-resolved.service 가 부팅 시 시작되지 않음

systemd 확인 서비스가 부팅 시 시작되지 않는 경우가 있습니다. 이 경우 다음 명령을 사용하여 부팅이 완료된 후 서비스를 수동으로 다시 시작합니다.

```
# systemctl start systemd-resolved
```

그러나 부팅 시 systemd-resolved 가 실패해도 다른 서비스에는 영향을 미치지 않습니다.

(BZ#1640802)

6.7.5. 인프라 서비스

dnsmasq의 DNSSEC 지원

dnsmasq 패키지에서는 DNSSEC(Domain Name System Security Extensions) 지원을 도입하여 루트 서버에서 받은 호스트 이름 정보를 확인합니다.

dnsmasq의 DNSSEC 검증은 FIPS 140-2와 호환되지 않습니다. FIPS(Federal Information Processing Standard) 시스템에서 dnsmasq에서 DNSSEC를 활성화하지 말고 localhost에서 준수 검증 확인자를 전달자로 사용합니다.

(BZ#1549507)

6.7.6. 보안

redhat-support-tool 이 FUTURE 암호화 정책에서 작동하지 않음

고객 포털 API의 인증서에서 사용하는 암호화 키가 FUTURE 시스템 전체 암호화 정책의 요구 사항을 충족하지 않으므로 redhat-support-tool 유틸리티는 현재 이 정책 수준에서 작동하지 않습니다. 이 문제를 해결하려면 고객 포털 API에 연결하는 동안 DEFAULT 암호화 정책을 사용하십시오.

(BZ#1802026)

/etc/selinux/config 에서 SELINUX=disabled 가 제대로 작동하지 않음

/etc/selinux/config 에서 SELINUX=disabled 옵션을 사용하여 SELinux를 비활성화하면 커널이 SELinux가 활성화된 상태로 부팅되고 부팅 프로세스 후반부에서 비활성화 모드로 전환됩니다. 이로 인해 메모리 누수와 경쟁 조건이 발생할 수 있으므로 커널 패닉도 발생할 수 있습니다. 이 문제를 해결하려면 시나리오가 실제로 SELinux 제목을 완전히 비활성화해야 하는 경우 SELinux 제목 사용의 부팅 시 SELinux 모드 변경 섹션에 설명된 대로 커널 명령줄에 selinux=0 매개 변수를 추가하여 SELinux를 비활성화합니다.

(JIRA:RHELPLAN-34199)

libselinux-python 은 모듈을 통해서만 사용할 수 있습니다

libselinux-python 패키지에는 SELinux 애플리케이션 개발을 위한 Python 2 바인딩만 포함되어 있으며 이전 버전과의 호환성에 사용됩니다. 이러한 이유로 libselinux-python 은 dnf install libselinux-python 명령을 통해 기본 RHEL 8 리포지토리에서 더 이상 사용할 수 없습니다.

이 문제를 해결하려면 libselinux-python 및 python27 모듈을 둘 다 활성화하고 다음 명령을 사용하여 libselinux-python 패키지와 해당 종속성을 설치합니다.

```
# dnf module enable libselinux-python
# dnf install libselinux-python
```

또는 단일 명령으로 설치 프로파일을 사용하여 libselinux-python 을 설치합니다.

```
# dnf module install libselinux-python:2.8/common
```

결과적으로 해당 모듈을 사용하여 libselinux-python 을 설치할 수 있습니다.

(BZ#1666328)

udica 는 --env container=podman으로 시작되는 경우에만 UBI 8 컨테이너를처리합니다.

Red Hat Universal Base Image 8(UBI 8) 컨테이너는 컨테이너 환경 변수를 podman 값이 아닌 oci 값으로 설정합니다. 이렇게 하면 udica 툴에서 컨테이너 JSON(JavaScript Object Notation) 파일을 분석하지 못합니다.

이 문제를 해결하려면 --env container=podman 매개변수와 함께 podman 명령을 사용하여 UBI 8 컨테이너를 시작합니다. 결과적으로 udica 는 설명된 해결 방법을 사용하는 경우에만 UBI 8 컨테이너에 대한 SELinux 정책을 생성할 수 있습니다.

(BZ#1763210)

rpm-plugin-selinux 패키지를 제거하면 시스템에서 모든 selinux-policy 패키지가 제거됩니다.

rpm-plugin-selinux 패키지를 제거하면 시스템에서 SELinux가 비활성화됩니다. 또한 시스템에서 모든 selinux-policy 패키지를 제거합니다. 그런 다음 rpm-plugin-selinux 패키지를 반복적으로 설치한 후 selinux-policy- targeted 정책이 시스템에 있는 경우에도 selinux-policy- minimum SELinux 정책을 설치합니다. 그러나 반복적으로 설치하면 정책 변경 사항을 고려하여 SELinux 구성 파일이 업데이트되지 않습니다. 결과적으로 rpm-plugin-selinux 패키지를 다시 설치해도 SELinux가 비활성화됩니다.

이 문제를 해결하려면 다음을 수행합니다.

1. umount /sys/fs/selinux/ 명령을 입력합니다.
2. 누락된 selinux-policy-targeted 패키지를 수동으로 설치합니다.
3. 정책이 SELINUX=enforcing 과 같도록 /etc/selinux/config 파일을 편집합니다.
4. load_policy -i 명령을 입력합니다.

결과적으로 SELinux가 활성화되어 이전과 동일한 정책을 실행합니다.

(BZ#1641631)

SELinux는 corosync에서 만든 공유 메모리 파일에서 newfstatat() 를 호출하도록 systemd-journal-gatewayd 를 방지합니다.

SELinux 정책에는 systemd-journal-gatewayd 데몬이 corosync 서비스에서 생성한 파일에 액세스할 수 있도록 하는 규칙이 포함되지 않습니다. 그 결과 SELinux는 systemd-journal-gatewayd 를 거부하여 corosync 에서 만든 공유 메모리 파일에 newfstatat() 함수를 호출합니다.

이 문제를 해결하려면 설명된 시나리오를 활성화하는 allow 규칙을 사용하여 로컬 정책 모듈을 생성합니다. SELinux 정책 *allow* 및 *dontaudit* 규칙 생성에 대한 자세한 내용은 audit2allow(1) 도움말 페이지를 참조하십시오. 이전 해결방법으로 인해 systemd-journal-gatewayd는 강제 모드에서 SELinux 를 사용하여 생성된 공유 메모리 파일에서 함수를 호출할 수 있습니다.

(BZ#1746398)

성능에 대한 기본 로깅 설정의 부정적인 영향

기본 로깅 환경 설정은 rsyslog 를 사용하여 systemd-journald를 실행할 때 4GB 메모리를 사용하거나 rate- limit 값을 조정하는 작업이 복잡할 수 있습니다.

자세한 내용은 성능 및 완화 기술 자료에 대한 RHEL 기본 로깅 설정의 부정적인 영향을 참조하십시오.

(JIRA:RHELPLAN-10431)

config.enabled 가 포함된 rsyslog 출력의 매개 변수가 알 수 없는 오류

rsyslog 출력에서는 config.enabled 지시문을 사용하여 구성 처리 오류에서 예기치 않은 버그가 발생합니다. 결과적으로 include() 문을 제외하고 config.enabled 지시문을 사용하는 동안 매개 변수가 알 수 없는 오류가 표시됩니다.

이 문제를 해결하려면 config.enabled=on 을 설정하거나 include() 문을 사용하십시오.

(BZ#1659383)

특정 rsyslog 우선 순위 문자열이 올바르게 작동하지 않음

암호화를 세밀하게 제어할 수 있는 imtcp 에 대한 GnuTLS 우선순위 문자열 지원은 완료되지 않습니다. 결과적으로, rsyslog 에서 다음 우선 순위 문자열이 제대로 작동하지 않습니다 :

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+DHE-RSA:+AES-256-GCM:+SIGN-RSA-
SHA384:+COMP-ALL:+GROUP-ALL
```

이 문제를 해결하려면 우선 순위 문자열이 올바르게 작동하는 경우에만 사용하십시오.

```
NONE:+VERS-ALL:-VERS-TLS1.3:+MAC-ALL:+ECDHE-RSA:+AES-128-CBC:+SIGN-RSA-SHA1:+COMP-ALL:+GROUP-ALL
```

따라서 현재 구성을 올바르게 작동하는 문자열로 제한해야 합니다.

(BZ#1679512)

SHA-1 서명이 있는 서버에 대한 연결이 GnuTLS에서 작동하지 않음

인증서의 SHA-1 서명은 GnuTLS 보안 통신 라이브러리에서 안전하지 않은 것으로 거부됩니다. 결과적으로 GnuTLS를 TLS 백엔드로 사용하는 애플리케이션은 이러한 인증서를 제공하는 피어에 TLS 연결을 설정할 수 없습니다. 이 동작은 다른 시스템 암호화 라이브러리와 일치하지 않습니다. 이 문제를 해결하려면 SHA-256 또는 더 강력한 해시로 서명된 인증서를 사용하거나 LEGACY 정책으로 전환하도록 서버를 업그레이드합니다.

(BZ#1628553)

TLS 1.3이 FIPS 모드에서 NSS에서 작동하지 않음

FIPS 모드에서 작동하는 시스템에서는 TLS 1.3이 지원되지 않습니다. 따라서 상호 운용성에 TLS 1.3이 필요한 연결은 FIPS 모드에서 작동하는 시스템에서 작동하지 않습니다.

연결을 활성화하려면 시스템의 FIPS 모드를 비활성화하거나 피어에서 TLS 1.2 지원을 활성화합니다.

(BZ#1724250)

OpenSSL 에서 원시 RSA 또는 RSA-PSS 서명을 지원하지 않는 PKCS #11 토큰을 잘못 처리합니다.

OpenSSL 라이브러리는 PKCS #11 토큰의 키 관련 기능을 탐지하지 않습니다. 결과적으로 원시 RSA 또는 RSA-PSS 서명을 지원하지 않는 토큰으로 서명이 생성되면 TLS 연결 설정에 실패합니다.

이 문제를 해결하려면 /etc/pki/tls/openssl .cnf 파일의 crypto_policy 섹션 끝에.include 행 뒤에 다음 행을 추가하십시오.

```
SignatureAlgorithms =
RSA+SHA256:RSA+SHA512:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA512:ECDSA+SHA384
MaxProtocol = TLSv1.2
```

따라서 설명된 시나리오에서 **TLS** 연결을 설정할 수 있습니다.

(**BZ#1685470**)

OpenSSL TLS 라이브러리는 **PKCS#11** 토큰이 원시 **RSA** 또는 **RSA -PSS** 서명 생성을 지원하는지 탐지하지 않습니다.

TLS-1.3 프로토콜에는 **RSA-PSS** 서명 지원이 필요합니다. **PKCS#11** 토큰이 원시 **RSA** 또는 **RSA -PSS** 서명을 지원하지 않는 경우, **OpenSSL TLS** 라이브러리를 사용하는 서버 애플리케이션이 **PKCS#11** 토큰에 보유하는 경우 **RSA** 키로 작동하지 않습니다. 결과적으로 **TLS** 통신이 실패합니다.

이 문제를 해결하려면 **TLS-1.2** 버전을 사용 가능한 최고 **TLS** 프로토콜 버전으로 사용하도록 서버 또는 클라이언트를 구성합니다.

(**BZ#1681178**)

OpenSSL은 **TLS 1.3**의 **CertificateRequest** 메시지에 잘못된 형식의 **status_request** 확장을 생성합니다.

status_request 확장 및 클라이언트 인증서 기반 인증을 지원하는 경우 **OpenSSL** 서버는 **CertificateRequest** 메시지에 잘못된 형식의 **status_request** 확장을 전송합니다. 이러한 경우 **OpenSSL**은 **RFC 8446** 프로토콜을 준수하는 구현과 상호 운용되지 않습니다. 그 결과 **'CertificateRequest'** 메시지의 확장을 올바르게 확인하는 클라이언트는 **OpenSSL** 서버와의 연결이 중단됩니다. 이 문제를 해결하려면 연결 측에서 **TLS 1.3** 프로토콜에 대한 지원을 비활성화하거나 **OpenSSL** 서버에서 **status_request** 에 대한 지원을 비활성화합니다. 이렇게 하면 서버가 잘못된 형식의 메시지를 보내지 못합니다.

(**BZ#1749068**)

ssh-keyscan 은 **FIPS** 모드에서 **RSA** 키를 검색할 수 없습니다

FIPS 모드에서 **RSA** 서명에 대해 **SHA-1** 알고리즘이 비활성화되어 **ssh-keyscan** 유틸리티가 해당 모드에서 작동하는 서버의 **RSA** 키를 검색하지 못하게 합니다.

이 문제를 해결하려면 대신 **ECDSA** 키를 사용하거나 서버의 **/etc/ssh/ssh_host_rsa_key.pub** 파일에서 키를 로컬로 검색합니다.

(BZ#1744108)

감사 규칙의 SCAP-security-guide PCI-DSS 수정이 제대로 작동하지 않음

scap-security-guide 패키지에는 다음 시나리오 중 하나가 될 수 있는 수정 및 검사가 조합되어 있습니다.

- 감사 규칙의 잘못된 수정 적용
- 통과된 규칙이 실패한 것으로 표시되는 오탐을 포함하는 검사 평가

결과적으로 RHEL 8.1 설치 프로세스 중에 설치된 시스템을 스캔하면 일부 감사 규칙이 실패하거나 오류로 보고됩니다.

이 문제를 해결하려면 RHEL-8.1 해결방법의 지침에 따라 scap-security-guide PCI-DSS 프로파일 지식 베이스 문서로 수정 및 스캔 하십시오.

(BZ#1754919)

SSG의 특정 상호 의존 규칙 세트는 실패할 수 있습니다.

규칙 및 해당 종속 항목의 정의되지 않은 순서로 인해 벤치마크의 SCAP 보안 가이드 (SSG) 규칙 수정이 실패할 수 있습니다. 예를 들어, 한 규칙이 구성 요소를 설치하고 다른 규칙이 동일한 구성 요소를 구성하는 경우와 같이 두 개 이상의 규칙을 특정 순서로 실행해야 하는 경우 해당 규칙을 잘못된 순서로 실행하고 수정을 통해 오류를 보고할 수 있습니다. 이 문제를 해결하려면 수정을 두 번 실행하고 두 번째는 종속 규칙을 수정합니다.

(BZ#1750755)

컨테이너 보안 및 준수 검사를 위한 유틸리티를 사용할 수 없음

Red Hat Enterprise Linux 7에서 oscap-docker 유틸리티는 Atomic 기술을 기반으로 한 Docker 컨테이너 스캔에 사용할 수 있었습니다. Red Hat Enterprise Linux 8에서는 Docker 및 Atomic 관련 OpenSCAP 명령을 사용할 수 없습니다.

이 문제를 해결하려면 고객 포털의 RHEL 8 문서의 컨테이너 스캔을 위한 OpenSCAP 사용을 참조하십시오. 따라서 현재 RHEL 8의 컨테이너 보안 및 준수 스캔을 위해 지원되지 않으며 제한된 방법만 사용

할 수 있습니다.

(BZ#1642373)

OpenSCAP 는 가상 머신 및 컨테이너의 오프라인 스캔을 제공하지 않습니다.

OpenSCAP 코드베이스를 리팩토링하면 특정 **RPM** 프로브가 오프라인 모드에서 **VM** 및 컨테이너 파일 시스템을 스캔하지 못했습니다. 따라서 **openscap-utils** 패키지인 **oscap- vm** 및 **oscap- chroot** 에서 다음 도구가 제거되었습니다. 또한 **openscap-containers** 패키지가 완전히 제거되었습니다.

(BZ#1618489)

OpenSCAP rpmverifypackage가 올바르게 작동하지 않음

chdir 및 **chroot** 시스템 호출은 **rpmverifypackage** 프로브에 의해 두 번 호출됩니다. 그 결과, 사용자 지정 **OVAL(Open Vulnerability and Assessment Language)** 콘텐츠로 **OpenSCAP** 스캔 중에 프로브를 사용할 때 오류가 발생합니다.

이 문제를 해결하려면 **rpmverifypackage_test OVAL** 테스트를 콘텐츠에서 사용하지 마십시오.또는 **rpmverifypackage_test**가 사용되지 않은 **scap-security-guide** 패키지에서만 콘텐츠를 사용하십시오.

(BZ#1646197)

SCAP Workbench가 사용자 정의 프로파일에서 결과를 기반으로 한 수정을 생성하지 못함

SCAP Workbench 툴을 사용하여 사용자 정의된 프로파일에서 결과 기반 수정 역할을 생성하려고 할 때 다음과 같은 오류가 발생합니다.

```
Error generating remediation role .../remediation.sh: Exit code of oscap was 1: [output truncated]
```

이 문제를 해결하려면 **--tailoring-file** 옵션과 함께 **oscap** 명령을 사용하십시오.

(BZ#1640715)

OSCAP Anaconda 애드온은 모든 패키지를 텍스트 모드에 설치하지 않음

OSCAP Anaconda Addon 플러그인은 설치가 텍스트 모드에서 실행 중인 경우 시스템 설치 프로그

램에서 설치에 대해 선택한 패키지 목록을 수정할 수 없습니다. 결과적으로 Kickstart를 사용하여 보안 정책 프로필을 지정하고 설치가 텍스트 모드로 실행되는 경우 보안 정책에 필요한 추가 패키지는 설치 중에 설치되지 않습니다.

이 문제를 해결하려면 그래픽 모드에서 설치를 실행하거나 Kickstart 파일의 %packages 섹션에 있는 보안 정책의 보안 정책에서 필요한 모든 패키지를 지정합니다.

결과적으로 보안 정책 프로필에 필요한 패키지는 설명된 해결 방법 중 하나가 없으면 RHEL 설치 중에 설치되지 않으며 설치된 시스템은 지정된 보안 정책 프로필을 준수하지 않습니다.

(BZ#1674001)

OSCAP Anaconda 애드온 이 사용자 지정 프로파일을 올바르게 처리하지 않음

OSCAP Anaconda 애드온 플러그인은 별도의 파일의 사용자 지정으로 보안 프로필을 올바르게 처리하지 않습니다. 따라서 해당 Kickstart 섹션에서 적절하게 지정하는 경우에도 RHEL 그래픽 설치에서 사용자 지정된 프로필을 사용할 수 없습니다.

이 문제를 해결하려면 원래 DS에서 단일 SCAP 데이터 스트림 생성 및 맞춤형 파일 지식 베이스 문서의 지침을 따르십시오. 이 해결방법은 RHEL 그래픽 설치에서 사용자 지정 SCAP 프로필을 사용할 수 있습니다.

(BZ#1691305)

6.7.7. 네트워킹

arptables 의 자세한 출력 형식이 RHEL 7의 유틸리티 형식과 일치합니다.

RHEL 8에서 iptables-arptables 패키지는 arptables 유틸리티의 nftables기반 교체 기능을 제공합니다. 이전에는 RHEL 7에서 arptables 의 자세한 출력을 쉼표로만 구분한 반면 RHEL 7에서 arptables 는 설명된 출력을 공백과 쉼표로 구분했습니다. 결과적으로 arptables -v -L 명령의 출력을 구문 분석하는 RHEL 7에서 생성된 스크립트를 사용한 경우 이러한 스크립트를 조정해야 했습니다. 이 비호환성은 수정되었습니다. 결과적으로 RHEL 8.1 의 arptables 도 공백 및 쉼표로 카운터 값을 구분합니다.

(BZ#1676968)

nftables이 다차원 IP 집합 유형을 지원하지 않음

nftables 패킷 필터링 프레임워크가 연결 및 간격이 있는 집합 유형을 지원하지 않습니다. 그 결과,

hash:net,port와 같은 다차원 IP 집합 유형을 nftables와 함께 사용할 수 없습니다.

이 문제를 해결하려면 다차원 IP 집합 유형이 필요한 경우 iptables 프레임워크를 ipset 툴과 함께 사용하십시오.

(BZ#1593711)

GRO를 비활성화할 때 IPsec 오프로딩 중에 IPsec 네트워크 트래픽이 실패합니다

장치에서 GRO(Generic Receive Offload)를 비활성화하면 IPsec 오프로딩이 작동하지 않습니다. IPsec 오프로딩이 네트워크 인터페이스에 구성되어 있고 해당 장치에서 GRO가 비활성화되면 IPsec 네트워크 트래픽이 실패합니다.

이 문제를 해결하려면 장치에서 GRO를 사용하도록 유지합니다.

(BZ#1649647)

6.7.8. 커널

부팅 시 i40iw 모듈이 자동으로 로드되지 않음

많은 i40e NIC에서 iWarp를 지원하지 않고 i40iw 모듈이 일시 중지/재개를 완전히 지원하지 않기 때문에 이 모듈이 기본적으로 자동 로드되지 않으므로 일시 중지/재개 동작이 제대로 작동하지 않게 됩니다. 이 문제를 해결하려면 수동으로 /lib/udev/rules.d/90-rdma-hw-modules.rules 파일을 편집하여 i40iw의 자동 로드를 활성화해야 합니다.

또한 동일한 시스템에 i40e 장치와 함께 설치된 다른 RDMA 장치가 있는 경우 비 i40e RDMA 장치는 rdma 서비스를 트리거하여 i40iw 모듈을 포함하여 활성화된 모든 RDMA 스택 모듈을 로드합니다.

(BZ#1623712)

fadump 를 사용할 때 네트워크 인터페이스의 이름이 kdump-<interface-name> 으로 변경됩니다.

펌웨어 지원 덤프(fadump)를 사용하여 vmcore를 캡처하여 SSH 또는 NFS 프로토콜을 사용하여 원격 머신에 저장하는 경우, & lt;interface-name>이 일반인 경우 네트워크 인터페이스의 이름이 kdump-& lt;interface-name> 으로 변경됩니다(예: *eth# 또는 net#). 이 문제는 초기 RAM 디스크(initrd)의 vmcore 캡처 스크립트를 네트워크 인터페이스 이름에 kdump- 접두사를 추가하여 영구적인 명명을 보안

하기 때문에 발생합니다. 동일한 initrd 도 일반 부팅에도 사용되므로 프로덕션 커널의 인터페이스 이름도 변경됩니다.

(BZ#1745507)

부팅 프로세스 중 많은 양의 영구 메모리 경험이 있는 시스템

메모리 초기화가 직렬화되므로 많은 양의 영구 메모리가 있는 시스템은 부팅하는 데 시간이 오래 걸립니다. 결과적으로 /etc/fstab 파일에 영구 메모리 파일 시스템이 나열된 경우 장치를 사용할 수 있을 때까지 기다리는 동안 시스템이 시간 초과될 수 있습니다. 이 문제를 해결하려면 /etc/systemd/system.conf 파일에서 DefaultTimeoutStartSec 옵션을 충분히 큰 값으로 구성하십시오.

(BZ#1666538)

KSM이 NUMA 메모리 정책을 무시하는 경우가 있음

merge_across_nodes=1 매개 변수를 사용하여 KSM(커널 공유 메모리) 기능을 활성화하면 KSM은 mbind() 함수에서 설정한 메모리 정책을 무시하고 일부 메모리 영역의 페이지를 정책과 일치하지 않는 NUMA(Non-Uniform Memory Access) 노드에 병합할 수 있습니다.

이 문제를 해결하려면 QEMU와 함께 NUMA 메모리 바인딩을 사용하는 경우 KSM을 비활성화하거나 merge_across_nodes 매개변수를 0 으로 설정합니다. 결과적으로 KVM VM에 대해 구성된 NUMA 메모리 정책이 예상대로 작동되게 됩니다.

(BZ#1153521)

fadump 가 활성화된 경우 부팅 시 시스템이 긴급 모드로 전환됩니다.

systemd 관리자가 마운트 정보를 가져오지 못하고 마운트할 LV 파티션을 구성하지 못하기 때문에 initramfs 스키마에서 fadump (kdump)또는 dracut squash 모듈이 활성화된 경우 시스템이 긴급 모드로 들어갑니다. 이 문제를 해결하려면 다음 커널 명령줄 parameter rd.lvm.lv=<VG>/<LV> 를 추가하여 실패한 LV 파티션을 적절하게 검색하고 마운트합니다. 따라서 설명된 시나리오에서 시스템이 성공적으로 부팅됩니다.

(BZ#1750278)

kdump 커널 명령줄에서 irqpoll 을 사용하면 vmcore 생성에 실패합니다.

AWS(Amazon Web Services) 클라우드 플랫폼에서 실행되는 64비트 ARM 아키텍처에서 nvme 드라이버의 기존 기본 문제로 인해 첫 번째 커널에 irqpoll kdump 명령줄 인수를 제공하면 vmcore 생성이

실패합니다. 결과적으로 커널 충돌 후 /var/crash/ 디렉토리에 vmcore가 덤프되지 않습니다. 이 문제를 해결하려면 다음을 수행합니다.

1. /etc/sysconfig/kdump 파일의 KDUMP_COMMANDLINE_REMOVE 키에 irqpoll 을 추가합니다.

2. systemctl restart kdump 명령을 실행하여 kdump 서비스를 다시 시작합니다.

결과적으로 첫 번째 커널이 올바르게 부팅되고 vmcore가 커널 충돌 시 캡처될 것으로 예상됩니다.

(BZ#1654962)

RHEL 8의 크래시 캡처 환경에서 커널을 부팅하지 못했습니다.

디버그 커널의 메모리 수요 특성으로 인해 디버그 커널이 사용 중이고 커널 패닉이 트리거되면 문제가 발생합니다. 결과적으로 디버그 커널은 캡처 커널로 부팅할 수 없으며 대신 스택 추적이 생성됩니다. 이 문제를 해결하려면 크래시 커널 메모리를 적절하게 늘립니다. 결과적으로 디버그 커널이 크래시 캡처 환경에서 성공적으로 부팅됩니다.

(BZ#1659609)

softirq 변경으로 인해 로드가 많은 경우 localhost 인터페이스에서 UDP 패킷이 삭제될 수 있습니다.

서비스 거부(DOS) 영향을 줄이기 위해 Linux 커널 소프트웨어 인터럽트(softirq) 처리의 변경이 수행됩니다. 결과적으로 localhost 인터페이스가 많은 로드에서 UDP(User Datagram Protocol) 패킷을 삭제하는 상황이 발생합니다.

이 문제를 해결하려면 네트워크 장치 백로그 버퍼의 크기를 6000 값으로 늘립니다.

```
echo 6000 > /proc/sys/net/core/netdev_max_backlog
```

Red Hat 테스트에서 이 값은 패킷 손실을 방지하기에 충분했습니다. 더 많이 로드되는 시스템에는 더 큰 백로그 값이 필요할 수 있습니다. 향상된 백로그는 localhost 인터페이스에서 잠재적으로 대기 시간을 증가시키는 영향을 미칩니다.

결과적으로 버퍼를 늘리고 더 많은 패킷이 처리 대기하도록 허용하므로 localhost 패킷이 삭제될 가능성이 줄어듭니다.

(BZ#1779337)

6.7.9. 하드웨어 활성화

경우에 따라 HP NMI 워치독은 크래시 덤프를 생성하지 않습니다.

HP NMI 워치독의 hpwdt 드라이버는 perfmon 드라이버에서 NMI를 대신 사용했기 때문에 HPE 워치독 타이머에서 생성한 NMI(마스크 가능 인터럽트)를 요청할 수 없는 경우가 있습니다. 결과적으로 경우에 따라 hpwdt 는 패닉을 호출하여 크래시 덤프를 생성할 수 없습니다.

(BZ#1602962)

QL41000 카드로 구성된 테스트 시스템에 RHEL 8.1을 설치하면 커널 패닉이 발생합니다.

QL41000 카드로 구성된 테스트 시스템에 RHEL 8.1을 설치하는 동안 시스템은 at 000000000000003c 카드의 커널 NULL 포인터 역참조를 처리할 수 없습니다. 결과적으로 커널 패닉 오류가 발생합니다. 이 문제에 대한 해결 방법은 없습니다.

(BZ#1743456)

cxgb4 드라이버로 인해 kdump 커널에서 충돌이 발생합니다.

vmcore 파일에 정보를 저장하려는 동안 kdump 커널이 충돌합니다. 결과적으로 cxgb4 드라이버는 kdump 커널이 나중에 분석을 위해 코어를 저장하지 못하게 합니다. 이 문제를 해결하려면 코어 파일을 저장할 수 있도록 kdump 커널 명령줄에 "novmcoredd" 매개변수를 추가합니다.

(BZ#1708456)

6.7.10. 파일 시스템 및 스토리지

특정 SCSI 드라이버에서 과도한 양의 메모리를 사용하는 경우가 있습니다.

특정 SCSI 드라이버는 RHEL 7보다 많은 양의 메모리를 사용합니다. HBA(파이버 채널 호스트 버스 어댑터)에서 vPort 생성과 같은 경우에 따라 시스템 구성에 따라 메모리 사용량이 과도하게 사용될 수 있습니다.

메모리 사용량 증가는 블록 계층의 메모리 사전 할당으로 인해 발생합니다. 다중 대기열 블록 장치 스

케줄링(BLK-MQ) 및 멀티 큐 SCSI 스택(SCSI-MQ) 모두 RHEL 8의 각 I/O 요청에 대해 메모리를 사전 할당하므로 메모리 사용량이 증가합니다.

(BZ#1698297)

UDS가 다시 빌드를 완료할 때까지 VDO는 일시 중단할 수 없습니다.

불명확한 시스템 종료 후 VDO(가상 데이터 최적화 도구) 볼륨이 시작되면 UDS(Universal Deduplication Service) 인덱스를 다시 빌드합니다. UDS 인덱스가 다시 빌드되는 동안 dmsetup suspend 명령을 사용하여 VDO 볼륨을 일시 중지하려고 하면 일시 중지 명령이 응답하지 않을 수 있습니다. 명령은 다시 빌드가 완료된 후에만 완료됩니다.

응답하지 않는 것은 큰 UDS 인덱스가 있는 VDO 볼륨에서만 확인할 수 있으므로 다시 빌드하는 데 시간이 더 오래 걸립니다.

(BZ#1737639)

NFS 4.0 패치를 통해 개방형 워크로드에서 성능이 저하될 수 있습니다.

이전 버전에서는 경우에 따라 NFS open 작업이 서버에서 파일이 제거되거나 이름이 변경된 사실을 간과할 수 있는 버그가 수정되었습니다. 그러나 많은 오픈 작업이 필요한 워크로드에서 수정으로 인해 성능이 저하될 수 있습니다. 이 문제를 해결하기 위해 NFS 버전 4.1 이상을 사용하는 데 도움이 될 수 있습니다. 이 경우 더 많은 경우 클라이언트에 위임을 부여하여 클라이언트가 로컬에서 빠르고 안전하게 오픈 작업을 수행할 수 있습니다.

(BZ#1748451)

6.7.11. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

Nginx 는 하드웨어 보안 토큰에서 서버 인증서를 로드할 수 없습니다.

nginx 웹 서버는 PKCS#11 모듈에서 직접 하드웨어 보안 토큰에서 TLS 개인 키를 로드하는 기능을 지원합니다. 그러나 현재 PKCS#11 URI를 통해 하드웨어 보안 토큰에서 서버 인증서를 로드할 수 없습니다. 이 문제를 해결하려면 파일 시스템에 서버 인증서를 저장하십시오.

(BZ#1668717)

php- opcache가 PHP 7.2와 함께 설치되면 PHP- fpm 으로 SELinux AVC가 거부됩니다.

php-opcache 패키지가 설치되면 FastCGI Process Manager(php-fpm)로 인해 SELinux AVC 거부가 발생합니다. 이 문제를 해결하려면 /etc/php.d/10-opcache.ini 파일의 기본 구성을 다음으로 변경합니다.

```
opcache.huge_code_pages=0
```

이 문제는 php :7.3 스트림이 아닌 php:7.2 스트림에만 영향을 미칩니다.

(BZ#1670386)

6.7.12. 컴파일러 및 개발 도구

ltrace 툴이 함수 호출을 보고하지 않음

모든 RHEL 구성 요소에 적용된 바이너리 강화 기능이 개선되었으므로 ltrace 툴은 RHEL 구성 요소의 바이너리 파일에서 함수 호출을 더 이상 감지할 수 없습니다. 따라서 이러한 바이너리 파일에 사용될 때 감지된 모든 호출을 보고하지 않으므로 ltrace 출력이 비어 있습니다. 현재 해결방법은 없습니다.

참고로 ltrace는 해당 강화 플래그없이 구축된 사용자 정의 바이너리 파일에서 호출을 올바르게 보고할 수 있습니다.

(BZ#1618748)

6.7.13. IdM (Identity Management)

GSSAPI 인증을 사용할 때 만료된 계정을 가진 AD 사용자는 로그인할 수 있습니다.

SSSD에서 계정이 만료되었는지 확인하는 데 사용하는 accountExpires 속성이 기본적으로 글로벌 카탈로그에 복제되지 않았는지 확인합니다. 결과적으로 GSSAPI 인증을 사용하는 경우 만료된 계정이 있는 사용자는 로그인할 수 있습니다. 이 문제를 해결하기 위해 sssd.conf 파일에 ad_enable_gc=False 를 지정하여 글로벌 카탈로그 지원을 비활성화할 수 있습니다. 이 설정을 사용하면 GSSAPI 인증을 사용하는 경우 만료된 계정의 사용자가 액세스가 거부됩니다.

SSSD는 이 시나리오에서 각 LDAP 서버에 개별적으로 연결되므로 연결 수를 늘릴 수 있습니다.

(BZ#1081046)

cert-fix 유틸리티를 --agent-uid pkidbuser 옵션과 함께 사용하면 인증서 시스템이 중단됩니다.

cert-fix 유틸리티를 --agent-uid pkidbuser 옵션과 함께 사용하면 인증서 시스템의 LDAP 구성이 손상됩니다. 결과적으로 인증서 시스템이 불안정해질 수 있으며 시스템을 복구하려면 수동 단계가 필요합니다.

(BZ#1729215)

/etc/nsswitch.conf 를 변경하려면 수동 시스템 재부팅이 필요합니다

/etc/nsswitch.conf 파일을 변경하는 경우, 예를 들어 authselect select profile_id 명령을 실행하려면 모든 관련 프로세스에서 업데이트된 /etc/nsswitch.conf 파일을 사용하도록 시스템을 재부팅해야 합니다. 시스템 재부팅이 불가능한 경우 시스템을 Active Directory(System Security Services Daemon) 또는 winbind 에 조인하는 서비스를 다시 시작합니다.

(BZ#1657295)

IdM에서 AD 신뢰 지원을 활성화할 때 필수 DNS 레코드에 대한 정보가 표시되지 않습니다

외부 DNS 관리를 통한 Red Hat Enterprise Linux IdM(Identity Management) 설치에 대한 AD(Active Directory) 신뢰성을 활성화하면 필수 DNS 레코드에 대한 정보가 표시되지 않습니다. AD에 대한 포리스트 신뢰는 필수 DNS 레코드가 추가될 때까지 성공하지 못합니다. 이 문제를 해결하려면 'ipa dns-update-system-records --dry-run' 명령을 실행하여 IdM에 필요한 모든 DNS 레코드 목록을 가져옵니다. IdM 도메인의 외부 DNS가 필요한 DNS 레코드를 정의하는 경우 포레스트 신뢰를 AD로 설정할 수 있습니다.

(BZ#1665051)

SSSD에서 로컬 사용자에 대해 잘못된 LDAP 그룹 멤버십 반환

SSSD(시스템 보안 서비스 데몬)에서 로컬 파일의 사용자를 제공하는 경우 파일 프로바이더에 다른 도메인의 그룹 멤버십이 포함되지 않습니다. 그 결과 로컬 사용자가 LDAP 그룹의 멤버인 경우 id local_user 명령은 사용자의 LDAP 그룹 멤버십을 반환하지 않습니다. 이 문제를 해결하려면 시스템이 /etc/nsswitch.conf 파일에서 사용자 그룹 구성원을 찾고 있는 데이터베이스 순서를 되돌리거나 sss 파일을 파일 sss로 교체 하거나 암시적 파일 도메인을 추가하여 암시적 파일 도메인을 비활성화합니다.

```
enable_files_domain=False
```

/etc/ sssd/sssd.conf 파일의 [sssd] 섹션에 추가합니다.

그 결과 id local_user 는 로컬 사용자에 대해 올바른 LDAP 그룹 멤버십을 반환합니다.

(BZ#1652562)

systemd-user 의 기본 PAM 설정이 RHEL 8에서 변경되어 SSSD 동작에 영향을 줄 수 있습니다.

Red Hat Enterprise Linux 8에서는 PAM(Pluggable Authentication Module) 스택이 변경되었습니다. 예를 들어 systemd 사용자 세션은 이제 systemd-user PAM 서비스를 사용하여 PAM 대화를 시작합니다. 이제 이 서비스에는 pam_sss.so 인터페이스가 포함될 수 있는 system-auth PAM 서비스가 재귀적으로 포함됩니다. 즉, SSSD 액세스 제어는 항상 호출됩니다.

RHEL 8 시스템에 대한 액세스 제어 규칙을 설계할 때 변경 사항에 유의하십시오. 예를 들어 systemd-user 서비스를 허용된 서비스 목록에 추가할 수 있습니다.

IPA HBAC 또는 AD GPO와 같은 일부 액세스 제어 메커니즘의 경우 systemd-user 서비스가 기본적으로 허용된 서비스 목록에 추가되어 작업을 수행할 필요가 없습니다.

(BZ#1669407)

SSSD가 동일한 우선 순위로 여러 인증서 일치 규칙을 올바르게 처리하지 않음

지정된 인증서가 여러 인증서 일치 규칙과 동일한 우선 순위의 규칙과 일치하면 SSSD(System Security Services Daemon)는 규칙 중 하나만 사용합니다. 이 문제를 해결하려면 LDAP 필터가 | (또는) 운영자와 연결된 개별 규칙의 필터로 구성된 단일 인증서 일치 규칙을 사용합니다. 인증서 일치 규칙의 예는 sss-certamp(5) 도움말 페이지를 참조하십시오.

(BZ#1447945)

여러 도메인을 정의할 때 auto_private_group = hybrid로 프라이빗 그룹을 만들 수 없습니다.

여러 도메인이 정의되어 있고 첫 번째 도메인이 아닌 다른 도메인에서 하이브리드 옵션을 사용하는 경우 auto_private_group = 하이브리드 옵션을 사용하여 프라이빗 그룹을 만들 수 없습니다. 암시적 파일 도메인이 sssd.conf' 파일의 AD 또는 LDAP 도메인과 함께 정의되어 있고 'MPG_HYBRID로 표시되지 않는 경우, SSSD는 uid=gid를 가진 사용자의 개인 그룹을 생성하지 못하고 이 gid 그룹이 AD 또는 LDAP에 존재하지 않습니다.

sssd_nss 응답자는 첫 번째 도메인에서만 auto_private_groups 옵션 값을 확인합니다. 결과적으로 RHEL 8의 기본 설정이 포함된 여러 도메인이 구성된 설정에서는 auto_private_group 옵션이 적용되지 않습니다.

이 문제를 해결하려면 sssd. conf 의 sssd 섹션에 enable_files_domain = false 를 설정합니다. 결과

적으로 enable_files_domain 옵션이 false로 설정된 경우 sssd는 활성 도메인 목록을 시작할 때 id_provider=files 가 있는 도메인을 추가하지 않으므로 이 버그가 발생하지 않습니다.

(BZ#1754871)

python-ply 는 FIPS와 호환되지 않습니다

python-ply 패키지의 ✓CC 모듈은 MD5 해싱 알고리즘을 사용하여 CC 서명의 지문을 생성합니다. 그러나 FIPS 모드에서는 비보안 컨텍스트에서만 허용되는 MD5 사용을 차단합니다. 결과적으로 python-ply는 FIPS와 호환되지 않습니다. FIPS 모드의 시스템에서 ply.yacc.yacc() 에 대한 모든 호출이 실패하고 오류 메시지가 표시됩니다.

```
"UnboundLocalError: local variable 'sig' referenced before assignment"
```

이 문제는 python-pycparser 및 python-cffi 의 일부 사용 사례에 영향을 미칩니다. 이 문제를 해결하려면 /usr/lib/python3.6/site-packages/ply/yacc.py 파일의 2966행을 수정하고 sig = md5()를 sig = md5 (usedforsecurity=False) 로 바꿉니다. 결과적으로 FIPS 모드에서 python-ply 를 사용할 수 있습니다.

(BZ#1747490)

6.7.14. 데스크탑

Wayland 세션의 제한 사항

Red Hat Enterprise Linux 8에서는 GNOME 환경과 GDM(GNOME Display Manager)이 이전 주요 RHEL에서 사용된 X11 세션 대신 Wayland 를 기본 세션 유형으로 사용합니다.

다음 기능은 현재 사용할 수 없거나 Wayland 에서 예상대로 작동하지 않습니다 :

- 멀티-GPU 설정은 Wayland에서 지원되지 않습니다.
- xrandr 과 같은 X11 구성 유틸리티는 해상도, 회전 및 레이아웃 처리에 대한 다양한 접근 방식으로 인해 Wayland 에서 작동하지 않습니다. GNOME 설정을 사용하여 디스플레이 기능을 구성할 수 있습니다.
- 화면 녹화 및 원격 데스크탑에서는 Wayland 에서 포털 API를 지원하는 애플리케이션이 필요합니다. 특정 레거시 애플리케이션은 포털 API를 지원하지 않습니다.

- Wayland 에서는 포인터 접근성을 사용할 수 없습니다.
- 클립보드 관리자는 사용할 수 없습니다.
- Wayland 의 GNOME Shell은 대부분의 레거시 X11 응용 프로그램에서 발행된 키보드 그랩을 무시합니다. /org/gnome/mutter/wayland/xwayland-grab-access-rules GSettings 키를 사용하여 X11 애플리케이션에서 키보드 그랩을 발행할 수 있습니다. 기본적으로 Wayland 의 GNOME 쉘을 사용하면 다음 응용 프로그램이 키보드 그랩을 실행할 수 있습니다.
  - GNOME 박스
  - vinagre
  - Xephyr
  - virt-manager, virt-viewer, and remote-viewer
  - vncviewer
- 게스트 VM(가상 시스템) 내의 Wayland 에는 안정성과 성능 문제가 있습니다. VM에서 실행되는 경우 RHEL은 자동으로 X11 세션으로 돌아갑니다.

X11 GNOME 세션을 사용한 RHEL 7 시스템에서 RHEL 8로 업그레이드하는 경우 시스템은 계속 X11 을 사용합니다. 다음 그래픽 드라이버를 사용하는 경우 시스템에서 X11 로 자동 대체합니다.

- 독점적 NVIDIA 드라이버
- cirrus 드라이버

- mga 드라이버
- aspeed 드라이버

Wayland 사용을 수동으로 비활성화할 수 있습니다.

- GDM에서 Wayland 를 비활성화하려면 /etc/gdm/custom.conf 파일에 WaylandEnable=false 옵션을 설정합니다.
- GNOME 세션에서 Wayland 를 비활성화하려면 로그인 이름을 입력한 후 로그인 화면의 메뉴로 legacy X11 옵션을 선택합니다.

Wayland에 관한 자세한 내용은 https://wayland.freedesktop.org/를 참조하십시오.

(BZ#1797409)

드래그 앤 드롭이 데스크탑과 응용 프로그램 간에 작동하지 않음

gnome-shell-extensions 패키지의 버그로 인해 현재 드래그 앤 드롭 기능이 데스크탑과 애플리케이션 간에 작동하지 않습니다. 이 기능에 대한 지원은 향후 릴리스에서 다시 추가될 예정입니다.

(BZ#1717947)

소프트웨어 리포지토리에서 flatpak 리포지토리를 비활성화할 수 없습니다.

현재 GNOME 소프트웨어 유틸리티의 Software Repositories(소프트웨어 리포지토리) 도구에서 flatpak 리포지토리를 비활성화하거나 제거할 수 없습니다.

(BZ#1668760)

Generation 2 RHEL 8 가상 머신이 Hyper-V Server 2016 호스트에서 부팅되지 않는 경우가 있습니다.

Microsoft Hyper-V Server 2016 호스트에서 실행되는 VM(가상 머신)에서 RHEL 8을 게스트 운영 체제로 사용하는 경우, 경우에 따라 VM이 부팅되지 않고 GRUB 부팅 메뉴로 돌아갑니다. 또한 Hyper-V 이

벤트 로그에 다음 오류가 기록됩니다.

```
The guest operating system reported that it failed with the following error code: 0x1E
```

이 오류는 **Hyper-V** 호스트의 **UEFI** 펌웨어 버그로 인해 발생합니다. 이 문제를 해결하려면 **Hyper-V Server 2019**를 호스트로 사용합니다.

(BZ#1583445)

소프트웨어 렌더러를 사용할 때 **Wayland**의 **GNOME** 쉘이 느리게 작동합니다.

소프트웨어 렌더를 사용하는 경우 **GNOME Shell**은 **Wayland Compositor(Wayland**의 **GNOME Shell)**로 화면 렌더링에캐시 가능한 프레임버퍼를 사용하지 않습니다. 그 결과 **Wayland**의 **GNOME** 쉘이 느립니다. 이 문제를 해결하려면 **GDM(GNOME Display Manager)** 로그인 화면으로 이동하여 대신 **X11** 프로토콜을 사용하는 세션으로 전환합니다. 결과적으로 캐시 가능한 메모리를 사용하는 **Xorg** 디스플레이 서버가 사용되었으며 설명된 상황에서 **Xorg** 쉘 은 **Wayland**의 **GNOME** 쉘에 비해 더 빠르게 수행됩니다.

(BZ#1737553)

시스템 충돌로 인해 **fadump** 설정이 손실될 수 있습니다.

이 문제는 펌웨어 지원 덤프**(fadump)**가 활성화된 시스템에서 확인되며 부팅 파티션은 **XFS**와 같은 저널링 파일 시스템에 있습니다. 시스템 충돌로 인해 부트 로더가 덤프 캡처 지원이 활성화되어 있지 않은 이전 **initrd** 를 로드할 수 있습니다. 결과적으로 시스템이 **vmcore** 파일을 캡처하지 않아 **fadump** 구성이 손실됩니다.

이 문제를 해결하려면 다음을 수행합니다.

- **/boot** 가 별도의 파티션인 경우 다음을 수행하십시오.

  1. **kdump** 서비스 다시 시작

  2. **root** 사용자로 다음 명령을 실행하거나 **CAP_SYS_ADMIN** 권한이 있는 사용자 계정을 사용합니다.

     ```
     # fsfreeze -f
     # fsfreeze -u
     ```

- /boot 가 별도의 파티션이 아닌 경우 시스템을 재부팅합니다.

(BZ#1723501)

ldap_id_use_start_tls 옵션에 기본값을 사용할 때 발생할 수 있는 위험

TLS없이 ldap:// 를 ID 조회에 사용하는 경우 공격 벡터가 발생할 위험이 있습니다. 특히 MITM(Man-in-the-middle) 공격으로 공격자는 LDAP 검색에 반환된 오브젝트의 UID 또는 GID를 변경하여 사용자를 가장할 수 있습니다.

현재 TLS를 적용하는 SSSD 구성 옵션인 ldap_id_use_start_tls 는 기본값은 false 입니다. 설정이 신뢰할 수 있는 환경에서 작동하고 id_provider = ldap 에 대해 암호화되지 않은 통신을 안전하게 사용할 수 있는지 결정합니다. 참고 id_provider = ad 및 id_provider = ipa 는 SASL 및 GSSAPI로 보호되는 암호화된 연결을 사용하므로 영향을 받지 않습니다.

암호화되지 않은 통신을 사용하는 것이 안전하지 않은 경우 /etc/sssd/sssd.conf 파일에서 ldap_id_use_start_tls 옵션을 true 로 설정하여 TLS를 적용합니다. 기본 동작은 RHEL의 향후 릴리스에서 변경될 예정입니다.

(JIRA:RHELPLAN-155168)

6.7.15. 그래픽 인프라

Radeon이 하드웨어를 올바르게 재설정하지 못했습니다

현재 radeon 커널 드라이버는 kexec 컨텍스트에서 하드웨어를 올바르게 재설정하지 않습니다. 대신, radeon 이 종료되어 나머지 kdump 서비스가 실패합니다.

이 문제를 해결하려면 /etc/kdump.conf 파일에 다음 행을 추가하여 kdump 의 radeon 을 블랙리스트로 지정합니다.

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

시스템과 kdump 를 다시 시작합니다. kdump 를 시작한 후 force_rebuild 1 행이 구성 파일에서 제거될 수 있습니다.

이 시나리오에서는 **kdump** 중에 그래픽을 사용할 수 없지만 **kdump** 가 성공적으로 작동합니다.

(BZ#1694705)

6.7.16. 웹 콘솔

권한이 없는 사용자는 서브스크립션 페이지에 액세스할 수 있습니다.

관리자가 아닌 사용자가 웹 콘솔의 서브스크립션 페이지로 이동하면 웹 콘솔에 일반 오류 메시지 **"Cockpit was unexpected internal error"**가 표시됩니다.

이 문제를 해결하려면 권한 있는 사용자로 웹 콘솔에 로그인하고 **Reuse my password for privileged tasks**(권한 있는 작업에 내 암호 재사용) 확인란을 선택해야 합니다.

(BZ#1674337)

6.7.17. 가상화

cloud-init 를 사용하여 **Microsoft Azure**에 가상 머신 프로비저닝 실패

현재 **Microsoft Azure** 플랫폼에서 **RHEL 8** 가상 시스템(**VM**)을 프로비저닝하는 데 **cloud-init** 유틸리티를 사용할 수 없습니다. 이 문제를 해결하려면 다음 방법 중 하나를 사용하십시오.

- **cloud-init** 대신 **WALinuxAgent** 패키지를 사용하여 **Microsoft Azure**에 **VM**을 프로비저닝합니다.
- **/etc/NetworkManager/NetworkManager.conf** 파일의 **[main]** 섹션에 다음 설정을 추가합니다.

```
[main]
dhcp=dhclient
```

(BZ#1641190)

경우에 따라 **RHEL 7** 호스트의 **RHEL 8** 가상 머신은 더 높은 해상도로 볼 수 없습니다.

현재 **RHEL 7** 호스트 시스템에서 실행 중인 **RHEL 8** 가상 머신(**VM**)을 사용하는 경우, **kiosk** 모드에서

애플리케이션을 실행하는 것과 같은 VM의 그래픽 출력을 표시하는 특정 방법을 사용할 수 없습니다. 더 큰 해상도를 사용할 수는 없습니다. 결과적으로 이러한 방법을 사용하는 VM을 표시하는 것은 호스트 하드웨어가 높은 해상도를 지원하는 경우에도 최대 1.0x1200의 해상도에서만 작동합니다.

(BZ#1635295)

Windows Server 2019 호스트의 RHEL 8 가상 머신의 낮은 GUI 디스플레이 성능

Windows Server 2019 호스트에서 그래픽 모드에서 RHEL 8을 게스트 운영 체제로 사용하는 경우 GUI 디스플레이 성능이 낮고 현재 게스트의 콘솔 출력에 연결하는 데 예상보다 훨씬 오래 걸립니다.

이는 Windows 2019 호스트에서 알려진 문제이며 Microsoft가 수정 사항을 보류하고 있습니다. 이 문제를 해결하려면 SSH를 사용하여 게스트에 연결하거나 호스트로 Windows Server 2016을 사용합니다.

(BZ#1706541)

RHEL 가상 머신 설치에 실패하는 경우가 있음

특정 상황에서 virt-install 유틸리티를 사용하여 생성된 RHEL 7 및 RHEL 8 가상 머신은 --location 옵션을 사용하는 경우 부팅되지 않습니다.

이 문제를 해결하려면 대신 --extra-args 옵션을 사용하고 네트워크에서 연결할 수 있는 설치 트리를 지정합니다. 예를 들면 다음과 같습니다.

```
--extra-args="inst.repo=https://some/url/tree/path"
```

이렇게 하면 RHEL 설치 프로그램이 설치 파일을 올바르게 찾을 수 있습니다.

(BZ#1677019)

Wayland를 사용하는 가상 머신의 여러 모니터를 QXL에서는 표시할 수 없습니다.

remote-viewer 유틸리티를 사용하여 Wayland 디스플레이 서버를 사용하는 VM(가상 시스템)의 모니터를 두 개 이상 *표시하면 VM이 응답하지 않고 표시* 상태 메시지가 무기한 표시됩니다.

이 문제를 해결하려면 Wayland를 사용하는 VM의 GPU 장치로 qxl 대신 virtio-gpu 를 사용합니다.

(BZ#1642887)

virsh iface-* 명령이 일관되게 작동하지 않음

현재 virsh iface- start 및 virsh iface- destroy와 같은 virsh iface- * 명령은 구성 종속성으로 인해 실패하는 경우가 많습니다. 따라서 호스트 네트워크 연결을 구성하고 관리하는 데 virsh iface-* 명령을 사용하지 않는 것이 좋습니다. 대신 NetworkManager 프로그램과 관련 관리 애플리케이션을 사용합니다.

(BZ#1664592)

cloud-init 를 사용하여 ESXi VM을 사용자 지정하고 VM을 재부팅하면 IP 설정이 손실되고 VM이 부팅 속도가 매우 느립니다.

현재 cloud-init 서비스를 사용하여 VMware ESXi 하이퍼바이저에서 실행되는 VM(가상 시스템)을 고정 IP를 사용하도록 수정한 다음 VM을 복제하는 경우, 경우에 따라 복제된 새 VM이 재부팅하는 데 시간이 오래 걸립니다. 이로 인해 cloud-init 가 VM의 정적 IP를 DHCP로 다시 작성한 다음 사용 가능한 데이터 소스를 검색합니다.

이 문제를 해결하려면 VM을 처음 부팅한 후 cloud-init 를 설치 제거할 수 있습니다. 그 결과 이후의 재부팅 속도가 느려지지 않습니다.

(BZ#1666961, BZ#1706482)

RHEL 8 가상 머신은 Witherspoon 호스트에서 부팅할 수 없는 경우가 있습니다.

경우에 따라 DD2.2 또는 DD2.3 CPU를 사용하는 *HPC 호스트(Witherspoon이라고도 함)용 Power9 S922LC* 에서 pseries-rhel7.6.0-sxxm 시스템 유형을 사용하는 RHEL 8 가상 머신(VM)에서 부팅되지 않는 경우가 있습니다.

이러한 VM을 부팅하려고 하면 다음과 같은 오류 메시지가 생성됩니다.

```
qemu-kvm: Requested safe indirect branch capability level not supported by kvm
```

이 문제를 해결하려면 다음과 같이 가상 머신의 XML 구성을 구성합니다.

```
<domain type='qemu' xmlns:qemu='http://libvirt.org/schemas/domain/qemu/1.0'>
  <qemu:commandline>
    <qemu:arg value='-machine'/>
```

```
  <qemu:arg value='cap-ibs=workaround'/>
</qemu:commandline>
```

(BZ#1732726, BZ#1751054)

IBM POWER 가상 머신이 메모리 0 NUMA 노드에서 제대로 작동하지 않음

현재 RHEL 8 호스트에서 실행 중인 IBM POWER 가상 머신(VM)이 제로메모리(memory='0')를 사용하는 NUMA 노드로 구성된 경우 VM은 부팅할 수 없습니다. 따라서 RHEL 8에서 제로 메모리 NUMA 노드가 있는 IBM POWER VM을 사용하지 않는 것이 좋습니다.

(BZ#1651474)

RHEL 7-ALT 호스트에서 RHEL 8로 POWER9 게스트 마이그레이션에 실패

현재 POWER9 가상 머신을 RHEL 7-ALT 호스트 시스템에서 RHEL 8로 마이그레이션하는 것은 "마이그레이션 상태: active" 상태로 응답하지 않습니다.

이 문제를 해결하려면 RHEL 7-ALT 호스트에서 THP(투명한 대규모 페이지)를 비활성화하여 마이그레이션을 성공적으로 완료할 수 있습니다.

(BZ#1741436)

AMD EPYC에서 호스트 패스스루 모드를 사용할 때 VM에서 SMT CPU 토폴로지를 감지하지 않습니다.

AMD EPYC 호스트에서 CPU 호스트 패스스루 모드로 부팅되는 VM(가상 머신)이 부팅되면 CPU O EXT CPU 기능 플래그가 표시되지 않습니다. 결과적으로 VM은 코어당 여러 스레드가 있는 가상 CPU 토폴로지를 탐지할 수 없습니다. 이 문제를 해결하려면 호스트 통과 대신 EPYC CPU 모델로 VM을 부팅합니다.

(BZ#1740002)

여러 virtio-blk 디스크를 사용할 때 가상 머신이 시작되지 않는 경우가 있습니다.

VM(가상 시스템)에 다수의 virtio-blk 장치를 추가하면 플랫폼에서 사용 가능한 인터럽트 벡터 수가 소진될 수 있습니다. 이 경우 VM의 게스트 OS가 부팅되지 않고 dracut-initqueue[392]를 표시합니다. 경고: 부팅할 수 없습니다 오류.

(BZ#1719687)

7장. 컨테이너 관련 주요 변경 사항

RHEL(Red Hat Enterprise Linux) 8.1에서 컨테이너 이미지 집합을 사용할 수 있습니다. 주요 변경 사항은 다음과 같습니다.

- 루트리스 컨테이너는 RHEL 8.1에서 완벽하게 지원됩니다.

  루트리스(rootless) 컨테이너는 관리자 권한 없이 일반 시스템 사용자가 생성 및 관리하는 컨테이너입니다. 이를 통해 사용자는 컨테이너 레지스트리에 대한 자격 증명과 같은 항목을 포함하여 ID를 유지 관리할 수 있습니다.

  podman 및 buildah 명령을 사용하여 rootless 컨테이너를 사용해 볼 수 있습니다. 자세한 내용은 다음을 참조하십시오.

  - rootless 컨테이너의 경우 다음과 같이 루트리스 컨테이너 설정을 참조하십시오.
  - Buildah 의 경우 Buildah로 컨테이너 이미지 빌드를 참조하십시오.
  - podman 은 Building, running, and managing containers를 참조하십시오.

- toolbox RPM 패키지는 RHEL 8.1에서 완벽하게 지원됩니다.

  toolbox 명령은 Red Hat CoreOS와 같은 컨테이너 지향 운영 체제와 함께 자주 사용되는 유틸리티입니다. toolbox 를 사용하면 호스트 시스템에 이러한 툴을 설치할 필요 없이 사용할 대규모 문제 해결 툴 세트가 포함된 컨테이너를 시작하여 호스트 운영 체제의 문제를 해결하고 디버깅할 수 있습니다.

  toolbox 명령을 실행하면 수정하거나 해당 호스트와 작업하기 위해 호스트에 대한 루트 액세스 권한을 제공하는 rhel-tools 컨테이너가 시작됩니다.

- runlabels를 사용하여 컨테이너 실행 관련 새 문서 를 참조하십시오.

- podman 패키지가 업스트림 버전 1.4.2로 업그레이드되었습니다. RHEL 8.0에서 사용된 버전 1.0.0 이후 podman 에 추가된 기능에 대한 자세한 내용은 Github의 최신podman 릴리스에 대한

설명을 참조하십시오.

8장. 국제화

8.1. RED HAT ENTERPRISE LINUX 8 국제 언어

Red Hat Enterprise Linux 8은 사용자의 요구 사항에 따라 다양한 언어의 설치와 언어 변경을 지원합니다.

- 동아시아 언어 - 일본어, 한국어, 중국어 간체, 중국어 번체.
- 유럽 언어 - 영어, 독일어, 스페인어, 프랑스어, 이탈리아어, 포르투갈어, 러시아어.

다음 표에는 다양한 주요 언어에 제공되는 글꼴 및 입력 방법이 나열되어 있습니다.

언어	기본 글꼴 (Font Package)	입력 방법
영어	dejavu-sans-fonts	
프랑스어	dejavu-sans-fonts	
독일어	dejavu-sans-fonts	
이탈리아어	dejavu-sans-fonts	
러시아어	dejavu-sans-fonts	
스페인어	dejavu-sans-fonts	
포르투갈어	dejavu-sans-fonts	
중국어 간체	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
중국어 번체	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
일본어	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkkc
한국어	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	IBus-hangul, libhangu

8.2. RHEL 8 국제화의 주요 변경 사항

RHEL 8에서는 RHEL 7에 비해 국제화에 다음과 같은 변경 사항이 추가되었습니다.

- 유니코드 11 컴퓨팅 업계 표준에 대한 지원이 추가되었습니다.
- 국제화는 여러 패키지로 배포되므로 설치 공간을 더 적게 설치할 수 있습니다. 자세한 내용은 langpacks 사용을 참조하십시오.
- 여러 로케일의 glibc 패키지 업데이트가 이제 CLDR(Common Locale Data Repository)과 동기화됩니다.

부록 A. 구성 요소별 티켓 목록

구성 요소	티켓
NetworkManager-libreswan	BZ#1697329
anaconda	BZ#1628653, BZ#1673901, BZ#1671047,BZ#1689909,BZ#1689194, BZ#1584145, BZ#1637472, BZ#1696609, BZ#1672405, BZ#1687747, BZ#1745064, BZ#1659400, BZ#1655523
audit	BZ#1730382
authselect	BZ#1657295
bcc	BZ#1667043
binutils	BZ#1618748, BZ#1644391, BZ#1525406, BZ#1659437
bpftrace	BZ#1687802
Chrony	BZ#1685469
cloud-init	BZ#1641190, BZ#1666961
cockpit-appstream	BZ#1658847
cockpit	BZ#1631905, BZ#1678956, BZ#1657752, BZ#1678473, BZ#1666722
Corosync	BZ#1693491
criu	BZ#1689746
crypto-policies	BZ#1678661, BZ#1660839
cryptsetup	BZ#1676622
distribution	BZ#1685191, BZ#1657927
dnf-plugins-core	BZ#1722093
dnsmasq	BZ#1549507
dyninst	BZ#1648441
elfutils	BZ#1683705
정규 스크립트	BZ#1664366

구성 요소	티켓
fapolicyd	BZ#1673323
freeradius	BZ#1685546
frr	BZ#1657029
gcc-toolset-9	BZ#1685482
gcc	BZ#1680182
gdb	BZ#1669953, BZ#1187581
gdm	BZ#1678627
glibc	BZ#1663035, BZ#1701605, BZ#1651283, BZ#1577438
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1704360
gnome-software	BZ#1668760
gnutls	BZ#1628553
grub2	BZ#1583445, BZ#1723501
initial-setup	BZ#1676439
ipa	BZ#1665051, JIRA:RHELPLAN-15036, BZ#1664719, BZ#1664718, BZ#1719767
ipset	BZ#1683711, BZ#1683713, BZ#1649090
iptables	BZ#1658734, BZ#1676968
kernel-rt	BZ#1678887

구성 요소	티켓
kernel	BZ#1647723, BZ#1656787, BZ#1649087, BZ#1721386, BZ#1564427, BZ#1686755, BZ#1664969, BZ#1714111, BZ#1712272, BZ#1646810, BZ#1728519, BZ#1721961, BZ#1654962, BZ#1635295, BZ#1706541, BZ#1666538, BZ#1685894, BZ#1643980, BZ#1602962, BZ#1697310, BZ#1593711, BZ#1649647, BZ#1153521, BZ#1694705, BZ#1698297, BZ#1348508, BZ#1748451, BZ#1743456, BZ#1708456, BZ#1710480, BZ#1634343, BZ#1652222, BZ#1687459, BZ#1571628, BZ#1571534, BZ#1685552, BZ#1685427, BZ#1663281, BZ#1664359, BZ#1677215, BZ#1659399, BZ#1665717, BZ#1581898, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1401552, BZ#1495358, BZ#1633143, BZ#1503672, BZ#1505999, BZ#1570255, BZ#1696451, BZ#1665295, BZ#1658840, BZ#1660627, BZ#1569610
kexec-tools	BZ#1662911, BZ#1750278, BZ#1520209, BZ#1710288
keycloak-httpd-client-install	BZ#1553890
kmod-kvdo	BZ#1696492, BZ#1737639
kpatch	BZ#1763780
libcacard	BZ#1615840
libdnf	BZ#1697472
libgnome-keyring	BZ#1607766
libselinux-python-2.8-module	BZ#1666328
libsemanage	BZ#1672638
libssh	BZ#1610883
libstoragemgmt	BZ#1626415
libvirt	BZ#1664592, BZ#1526548, BZ#1528684
linuxptp	BZ#1677217, BZ#1685467
lorax	BZ#1663950, BZ#1709594, BZ#1689140
lvm2	BZ#1649086
mariadb-10.3-module	BZ#1657053

구성 요소	티켓
mutter	BZ#1737553
nfs-utils	BZ#1668026, BZ#1592011
nginx	BZ#1668717, BZ#1690292
nmstate	BZ#1674456
nss	BZ#1724250, BZ#1645153
openmpi	BZ#1717289
openscap	BZ#1642373, BZ#1618489, BZ#1646197, BZ#1718826, BZ#1709429
openssh	BZ#1683295, BZ#1671262, BZ#1651763, BZ#1744108, BZ#1691045
openssl	BZ#1685470, BZ#1681178, BZ#1749068
oscap-anaconda-addon	BZ#1674001, BZ#1691305
pacemaker	BZ#1715426
pcp	BZ#1685302
pcs	BZ#1619620
perl-IO-Socket-SSL	BZ#1632600
perl-Net-SSLeay	BZ#1632597
perl-Socket	BZ#1699793
php-7.2-module	BZ#1670386
php	BZ#1653109
pki-core	BZ#1695302, BZ#1673296, BZ#1729215
pykickstart	BZ#1637872
python-ply	BZ#1747490
python-wheel	BZ#1731526

구성 요소	티켓
python3	BZ#1731424
qemu-kvm	BZ#1619884, BZ#1689216, BZ#1651474, BZ#1740002, BZ#1719687, BZ#1651994
redhat-support-tool	BZ#1688274
rhel-system-roles-sap	BZ#1660832
rhel-system-roles	BZ#1691966
rng-tools	BZ#1692435
rpm	BZ#1688849
rsyslog	JIRA:RHELPLAN-10431, BZ#1659383, BZ#1679512, BZ#1614181
rt-tests	BZ#1686494, BZ#1707505, BZ#1666351
ruby-2.6-module	BZ#1672575
s390utils	BZ#1750326
samba	BZ#1638001, JIRA:RHELPLAN-13195
scap-security-guide	BZ#1741455, BZ#1754919, BZ#1750755, BZ#1718839
scap-workbench	BZ#1640715
selinux-policy	BZ#1673269, BZ#1671241, BZ#1683642, BZ#1641631, BZ#1746398, BZ#1673107, BZ#1684103, BZ#1673056
setools	BZ#1672631
setup	BZ#1663556
squashfs-tools	BZ#1716278
sssd	BZ#1448094, BZ#1081046, BZ#1657665,BZ#1652562,BZ#1669407, BZ#1447945, BZ#1382750, BZ#1754871
subscription-manager	BZ#1674337
systemd	BZ#1658691, BZ#1686892, BZ#1640802

구성 요소	티켓
systemtap	BZ#1675740
tpm2-abrmd-selinux	BZ#1642000
tpm2-tools	BZ#1664498
tuned	BZ#1685585
udica	BZ#1763210, BZ#1673643
valgrind	BZ#1683715
vdo	BZ#1669534
virt-manager	BZ#1677019
virtio-win	BZ#1223668
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1687489, BZ#1698565
기타	BZ#1640697, BZ#1623712, BZ#1745507, BZ#1659609, BZ#1697896, BZ#1732726, JIRA:RHELPLAN-2542, JIRA:RHELPLAN-13066, JIRA:RHELPLAN-13074, BZ#1731502, BZ#1649493, BZ#1718422, JIRA:RHELPLAN-7109, JIRA:RHELPLAN-13068, JIRA:RHELPLAN-13960, JIRA:RHELPLAN-13649, JIRA:RHELPLAN-12811, BZ#1766186, BZ#1741531, BZ#1721683, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1699825, JIRA:RHELPLAN-14047, BZ#1769727, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057,BZ#1748980

부록 B. 개정 내역

0.4-0

2023년 11월 10일 Gabriela Fialová (gfialova@redhat.com)

- RHEL 문서의 피드백 제공에서 모듈을 업데이트했습니다.

0.3-0

2023년 11월 7일 Gabriela Fialová (gfialova@redhat.com)

- 손상된 링크를 수정합니다.

0.2-9

Fri Oct 13 2023, Gabriela Fialová (gfialova@redhat.com)

- 기술 프리뷰 JIRA:RHELDOCS-16861 (컨테이너)이 추가되었습니다.

0.2-8

2023년 4월 27일, Gabriela Fialov al (gfialova@redhat.com)

- 알려진 문제 JIRA:RHELPLAN-155168 (Identity Management)이 추가되었습니다.

0.2-7

2022년 4월 29일, Lenka ECDHEpaanchorková (lspackova@redhat.com)

- 더 이상 사용되지 않는 기능 소개가 업데이트되었습니다.
- BZ#1605216 의 고정 오타.
- 손상된 링크가 수정되었습니다.

0.2-6

2021년 12월 23일 목요일, 기니카 -파파산라(lspackova@redhat.com)

- **soft-RoCE 드라이버인 rdma_rxe 에 대한 정보가 기술 프리뷰 BZ#1605216 및 더 이상 사용되지 않는 기능 BZ#1878207 (커널)에 추가되었습니다.**

0.2-5

2021년 8월 19일 목요일, Lucie Maás¢(lmanasko@redhat.com)

- **YUM/DNF를 사용한 패키지 관리가 배포 장에 추가되었습니다.**

0.2-4

2021년 5월 21일 금요일, 메카 -파파산라(lspackova@redhat.com)

- **개요에서 OS 변환에 대한 업데이트된 정보입니다.**

0.2-3

2021년 4월 6일 화요일, 메카 -파파산라(lspackova@redhat.com)

- **지원되는 아키텍처 목록 개선.**

0.2-2

2021년 2월 25일, 커널카 -파파산라(lspackova@redhat.com)

- **고정 CentOS Linux 이름.**

0.2-1

2021년 2월 4일 목요일, Lucie Maás¢(lmanasko@redhat.com)

- **알려진 문제(가상화) 추가.**

0.2-0

2021년 1월 28일 목요일, Lucie Maás¢(lmanasko@redhat.com)

- 새 기능 장 업데이트.
- 기술 프리뷰 장 업데이트.

0.1-9

2020년 12월 10일, Lenka pa¢á(lspackova@redhat.com)

- 새 기능(ID 관리)에 SSSD의 AD GPO 처리에 대한 정보가 추가되었습니다.

0.1-8

2020년 12월 01일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- fapolicyd (Security)와 관련된 버그 수정을 추가했습니다.

0.1-7

2020년 10월 30일 금요일, Barbka pa¢á(lspackova@redhat.com)

- Repositories(리포지토리) 섹션에 업데이트된 애플리케이션 스트림 설명.

0.1-6

2020년 9월 15일, Jaroslav Klech(jklech@redhat.com)

- 커널 섹션에 알려진 문제가 추가되었습니다.

0.1-5

2020년 4월 28일 화요일, 기니카 -파파산라(lspackova@redhat.com)

- 개요의 즉각적 업그레이드에 대한 업데이트된 정보.

0.1-4

2020년 4월 9일 목요일, 기니카 -파파산라(lspackova@redhat.com)

- 두 가지 알려진 문제(보안)가 추가되었습니다.
- 모듈 설치를 위한 통합 명령.

0.1-3

2020년 3월 31일 화요일, Lenka pa¢á(lspackova@redhat.com)

- pcs와 관련된 새 기능이 추가되었습니다 .

0.1-2

2020년 3월 27일 금요일, Lucie Maœás¢(lmanasko@redhat.com)

- 기술 프리뷰 설명을 올바른 장에 잘못 배치했습니다.

0.1-1

2020년 3월 20일 금요일, Lenka pa¢á(lspackova@redhat.com)

- jmc:rhel8 모듈을 설치하기 위한 명령을 업데이트했습니다.

0.1-0

2020년 3월 12일, Lenka pa¢á(lspackova@redhat.com)

- RHEL 시스템 역할에 대한 업데이트된 정보.

0.0-9

2020년 3월 6일 금요일, Jaroslav Klech(jklech@redhat.com)

- 외부 커널 매개 변수 및 새 드라이버에 중요한 변경 사항 제공.

0.0-8

2020년 2월 12일, Jaroslav Klech(jklech@redhat.com)

- 아키텍처에 대한 전체 커널 버전 및 새 기능 장 제공.

0.0-7

2020년 2월 4일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- Red Hat Enterprise Linux 8.1.1 릴리스 노트.

0.0-6

2020년 1월 23일 목요일, Lucie Maásá(lmanasko@redhat.com)

- 기술 프리뷰 섹션 업데이트.

0.0-5

2019년 12월 20일 금요일, Lucie Maœás¢(lmanasko@redhat.com)

- rhel-system-roles-sap 에 대한 참고 사항을 버전 1.1.1(시스템 역할)으로 다시 지정합니다.
- subscription-manager 가 이제 역할, 사용량 및 추가 기능 값(서브스크립션 관리)을 보고한다는 참고 사항이 추가되었습니다.
- eBPF(Extended Berkeley Packet Filter)(Kernel)와 관련된 메모가 업데이트되었습니다.

0.0-4

2019년 12월 3일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- **fadump** (커널)와 관련된 알려진 문제가 추가되었습니다.

0.0-3

2019년 11월 26일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- 버그 수정 섹션이 업데이트되었습니다.
- 기술 프리뷰 섹션 업데이트.
- **irqpoll** (커널)과 관련된 알려진 문제가 추가되었습니다.

0.0-2

2019년 11월 14일 목요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- **TIPC**가 이제 완전한 지원을 제공한다는 참고 사항이 추가되었습니다.
- 이제 **x86_64** 아키텍처에서만 **bcc-tool** 이 지원된다는 참고 사항이 추가되었습니다.
- 커널, **kpatch** 의 실시간 패치에 대한 정보로 업데이트된 개요.
- 기술 프리뷰 섹션 업데이트.

0.0-1

2019년 11월 5일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- **Red Hat Enterprise Linux 8.1** 릴리스 노트.

0.0-0

2019년 7월 24일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- **Red Hat Enterprise Linux 8.1 베타 릴리스 노트 릴리스.**