



Red Hat Enterprise Linux 8

8.3 릴리스 노트

Red Hat Enterprise Linux 8.3 릴리스 정보

Red Hat Enterprise Linux 8 8.3 릴리스 노트

Red Hat Enterprise Linux 8.3 릴리스 정보

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

법적 공지

Copyright © 2022 | You need to change the HOLDER entity in the en-US/8.3_Release_Notes.ent file |.

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 8.3에서 구현된 개선 사항 및 추가 사항에 대해 개략적으로 설명하고 이 릴리스의 알려진 문제와 주요 버그 수정, 기술 프리뷰, 사용되지 않는 기능 및 기타 세부 정보를 문서화합니다.

차례

RED HAT 문서에 관한 피드백 제공	5
1장. 개요	6
설치 프로그램 및 이미지 생성	6
에지용 RHEL	6
인프라 서비스	6
보안	6
동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버	6
컴파일러 툴 세트	7
IdM (Identity Management)	7
웹 콘솔	7
가상화	7
데스크탑 및 그래픽	7
즉각적 업그레이드 및 OS 변환	7
OpenJDK 11 사용 가능	8
추가 리소스	8
Red Hat Customer Portal 랩	9
2장. 아키텍처	10
3장. RHEL 8의 콘텐츠 배포	11
3.1. 설치	11
3.2. 리포지토리	11
3.3. APPLICATION STREAMS	11
3.4. YUM/DNF를 사용한 패키지 관리	12
4장. RHEL 8.3.1 릴리스	13
4.1. 새로운 기능	13
5장. RHEL 8.3.0 릴리스	17
5.1. 새로운 기능	17
5.1.1. 설치 프로그램 및 이미지 생성	17
5.1.2. 에지용 RHEL	18
5.1.3. 소프트웨어 관리	19
5.1.4. 셸 및 명령행 툴	20
5.1.5. 인프라 서비스	21
5.1.6. 보안	24
5.1.7. 네트워킹	32
5.1.8. 커널	34
5.1.9. 파일 시스템 및 스토리지	37
5.1.10. 고가용성 및 클러스터	39
5.1.11. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버	42
5.1.12. 컴파일러 및 개발 도구	51
5.1.13. IdM (Identity Management)	60
5.1.14. 데스크탑	70
5.1.15. 그래픽 인프라	72
5.1.16. 웹 콘솔	74
5.1.17. Red Hat Enterprise Linux 시스템 역할	75
5.1.18. 가상화	78
5.1.19. 클라우드 환경의 RHEL	87
5.1.20. 컨테이너	87
5.2. 외부 커널 매개변수로 중요한 변경	88

새 커널 매개변수	88
업데이트된 커널 매개변수	91
새로운 /proc/sys/fs 매개변수	96
5.3. 장치 드라이버	97
5.3.1. 새 드라이버	97
네트워크 드라이버	97
그래픽 드라이버 및 기타 드라이버	97
5.3.2. 업데이트된 드라이버	99
네트워크 드라이버 업데이트	99
스토리지 드라이버 업데이트	100
그래픽 및 기타 드라이버 업데이트	100
5.4. 버그 수정	101
5.4.1. 설치 프로그램 및 이미지 생성	101
5.4.2. 소프트웨어 관리	103
5.4.3. 셸 및 명령행 툴	103
5.4.4. 보안	104
5.4.5. 네트워킹	107
5.4.6. 커널	108
5.4.7. 고가용성 및 클러스터	111
5.4.8. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버	112
5.4.9. 컴파일러 및 개발 도구	112
5.4.10. IdM (Identity Management)	116
5.4.11. 그래픽 인프라	119
5.4.12. 가상화	120
5.4.13. 컨테이너	120
5.5. 기술 프리뷰	121
5.5.1. 네트워킹	121
5.5.2. 커널	123
5.5.3. 파일 시스템 및 스토리지	125
5.5.4. 고가용성 및 클러스터	128
5.5.5. IdM (Identity Management)	130
5.5.6. 데스크탑	131
5.5.7. 그래픽 인프라	131
5.5.8. Red Hat Enterprise Linux 시스템 역할	132
5.5.9. 가상화	133
5.5.10. 컨테이너	135
5.6. 사용되지 않는 기능	136
5.6.1. 설치 프로그램 및 이미지 생성	137
5.6.2. 소프트웨어 관리	138
5.6.3. 셸 및 명령행 툴	139
5.6.4. 인프라 서비스	139
5.6.5. 보안	140
5.6.6. 네트워킹	141
5.6.7. 커널	142
5.6.8. 파일 시스템 및 스토리지	142
5.6.9. IdM (Identity Management)	144
5.6.10. 데스크탑	146
5.6.11. 그래픽 인프라	146
5.6.12. 웹 콘솔	147
5.6.13. Red Hat Enterprise Linux 시스템 역할	147
5.6.14. 가상화	147
5.6.15. 컨테이너	148
5.6.16. 사용되지 않는 패키지	148

5.7. 확인된 문제	150
5.7.1. 설치 프로그램 및 이미지 생성	150
5.7.2. 서브스크립션 관리	155
5.7.3. 인프라 서비스	156
5.7.4. 보안	156
5.7.5. 네트워킹	164
5.7.6. 커널	165
5.7.7. 파일 시스템 및 스토리지	172
5.7.8. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버	174
5.7.9. IdM (Identity Management)	175
5.7.10. 데스크탑	177
5.7.11. 그래픽 인프라	178
5.7.12. 웹 콘솔	181
5.7.13. Red Hat Enterprise Linux 시스템 역할	181
5.7.14. 가상화	182
5.7.15. 클라우드 환경의 RHEL	184
5.7.16. 지원 관련 기능	185
5.7.17. 컨테이너	186
6장. 국제화	187
6.1. RED HAT ENTERPRISE LINUX 8 국제 언어	187
6.2. RHEL 8 국제화의 주요 변경 사항	188
부록 A. 구성 요소별 티켓 목록	189
부록 B. 개정 내역	197

RED HAT 문서에 관한 피드백 제공

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

- 특정 문구에 대해 간단한 의견을 남기려면 문서가 Multi-page HTML 형식으로 되어 있는지 확인하십시오. 주석 처리하려는 텍스트 부분을 강조 표시합니다. 그런 다음 강조 표시된 텍스트 아래에 표시되는 **피드백 추가** 팝업을 클릭하고 표시된 지침을 따릅니다.
- 보다 상세하게 피드백을 제출하려면 다음과 같이 Bugzilla 티켓을 생성하십시오.
 1. [Bugzilla](#) 웹 사이트로 이동하십시오.
 2. Component로 **Documentation**을 선택하십시오.
 3. **Description** 필드에 문서 개선을 위한 제안 사항을 기입하십시오. 관련된 문서의 해당 부분 링크를 알려주십시오.
 4. **Submit Bug**를 클릭하십시오.

1장. 개요

설치 프로그램 및 이미지 생성

RHEL 8.3에서는 설치를 시작하기 전에 루트 암호를 구성하고 사용자 계정을 만들 수 있습니다. 이전에는 설치 프로세스를 시작한 후 루트 암호를 구성하고 사용자 계정을 생성했습니다. 더 안정적인 백엔드를 기반으로 사용자 지정 이미지를 만들고 RHEL 웹 콘솔을 통해 이미지를 클라우드로 내보낼 수도 있습니다.

에지용 RHEL

RHEL 8.3에서는 에지 서버에 **RHEL**을 원격으로 설치하기 위한 **RHEL for Edge** 도입. RHEL for Edge는 이미지 빌더를 사용하여 구성할 수 있는 rpm-ostree 이미지입니다. Kickstart 파일을 사용하여 이미지를 설치한 다음 이미지 업데이트를 포함하고 이미지를 이전 기능 상태로 롤백하도록 이미지를 관리할 수 있습니다.

에지 주요 강조 표시는 다음과 같습니다.

- Atomic 업그레이드: 각 업데이트의 상태가 알려져 장치를 재부팅할 때까지 변경 사항이 표시되지 않습니다.
- 복원력을 보장하기 위한 맞춤형 상태 점검 및 지능형 롤백.
- 애플리케이션 업데이트에서 핵심 OS 업데이트를 분리하고 다양한 버전의 애플리케이션을 테스트 및 배포할 수 있는 컨테이너 중심 워크플로.
- 대역폭이 낮은 환경에 최적화된 OTA 페이로드.

자세한 내용은 [5.1.2절. "에지용 RHEL"](#)의 내용을 참조하십시오.

인프라 서비스

Tuned 시스템 튜닝 툴은 버전 2.13으로 변경되어 아키텍처 종속 튜닝 및 여러 include 지시문 지원이 추가되었습니다.

보안

RHEL 8.3은 **Clevis** 및 **Tang** 을 사용하여 PBD(Policy-Based Decryption) 솔루션의 자동화된 배포를 위한 Ansible 역할을 제공하며, 이 **rhel-system-roles** 패키지에는 **Rsyslog** 를 통해 RHEL 로그에 대한 Ansible 역할도 포함되어 있습니다.

scap-security-guide 패키지는 0.1.50 버전으로 업데이트되었으며 **OpenSCAP** 은 버전 1.3.3로 다시 기반합니다. 이러한 업데이트에서는 CIS RHEL 7 벤치마크 v2.2.0에 맞는 프로파일과 노스캐롤라이나 의료 기관에서 요구하는 HIPAA(Health Insurance Portability and Accountability Act)에 맞는 프로필을 포함하여 대폭적인 개선을 제공합니다.

이번 업데이트를 통해 **SCAP Workbench** 툴을 사용하여 맞춤형 프로필에서 결과 기반 수정 역할을 생성할 수 있습니다.

USBGuard 프레임워크는 이제 자체 SELinux 정책을 제공하며, GUI에서 데스크탑 사용자에게 알리고 버전 0.0.8에는 기타 여러 개선 사항 및 버그 수정이 포함되어 있습니다.

동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

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

- nginx 1.18
- Node.js 14
- Perl 5.30

- PHP 7.4
- Ruby 2.7

RHEL 8.3에서 다음 구성 요소가 업데이트되었습니다.

- Git 에서 버전 2.27 사이
- 버전 4.11 로 Squid

자세한 내용은 [5.1.11절. "동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버"](#) 를 참조하십시오.

컴파일러 툴 세트

RHEL 8.3에서 다음 컴파일러 툴 세트가 업데이트되었습니다.

- GCC 툴 세트 10
- LLVM Toolset 10.0.1
- 북마크 툴 세트 1.45.2
- Go Toolset 1.14.7

자세한 내용은 [5.1.12절. "컴파일러 및 개발 도구"](#) 를 참조하십시오.

IdM (Identity Management)

RHEL 8에서는 AD(Active Directory) 도메인 간 기본 암호화 유형인 Rivest Cipher 4(RC4) 암호화 제품군이 더 이상 사용되지 않습니다. 호환성을 위해 이 업데이트에서는 더 이상 사용되지 않는 RC4 암호화 유형에 대한 지원을 활성화하기 위해 새로운 암호화 하위 정책 **AD-SUPPORT** 가 도입되었습니다. 새 하위 정책을 통해 RC4를 RHEL IdM(Identity Management) 및 SSSD Active Directory 통합 솔루션과 함께 사용할 수 있습니다.

자세한 내용은 [5.1.13절. "IdM \(Identity Management\)"](#) 를 참조하십시오.

웹 콘솔

웹 콘솔은 사용자 세션 내부에서 관리 액세스와 제한된 액세스를 전환하는 옵션을 제공합니다.

가상화

IBM Z 하드웨어에서 호스팅되는 VM(가상 시스템)은 이제 IBM Secure Execution 기능을 사용할 수 있습니다. 이로 인해 호스트가 손상되면 VM이 공격에 취약하고 신뢰할 수 없는 호스트가 VM에서 정보를 얻지 못하도록 합니다. 또한 이제 DASD 장치를 IBM Z의 VM에 할당할 수 있습니다.

데스크탑 및 그래픽

이제 IBM Z 시스템에서 GNOME 데스크탑을 사용할 수 있습니다.

DRM (Direct Rendering Manager) 커널 그래픽 하위 시스템은 업스트림 Linux 커널 버전 5.6으로 업데이트되었습니다. 이 버전은 새 GPU 및 APU에 대한 지원과 다양한 드라이버 업데이트를 포함하여 이전 버전에 비해 여러 가지 개선 사항을 제공합니다.

자세한 내용은 [5.1.14절. "데스크탑"](#) 및 [5.1.15절. "그래픽 인프라"](#) 을 참조하십시오.

즉각적 업그레이드 및 OS 변환

RHEL 7에서 RHEL 8으로의 즉각적 업그레이드

현재 지원되는 즉각적 업그레이드 경로는 다음과 같습니다.

- 64비트 Intel, IBM POWER 8(little endian) 및 IBM Z 아키텍처의 RHEL 7.8에서 RHEL 8.2로

- 커널 버전 4.14가 필요한 아키텍처의 RHEL 7.6에서 RHEL 8.2로: IBM POWER 9(little endian) 및 IBM Z(Structure A)
- SAP HANA가 있는 시스템의 RHEL 7.7에서 RHEL 8.2까지.

RHEL 8.2로 업그레이드한 후에도 시스템이 계속 지원되도록하려면 최신 RHEL 8.3 버전으로 업데이트하거나 RHEL 8.2 EUS (Extended Update Support) 리포지토리를 활성화하십시오. SAP HANA가 있는 시스템에서 RHEL 8.2 Update Services for SAP Solutions(E4S) 리포지토리를 활성화합니다.

자세한 내용은 [Red Hat Enterprise Linux에 대한 지원 내부 업그레이드 경로를](#) 참조하십시오. 즉각적 업그레이드를 수행하는 방법은 [RHEL 7에서 RHEL 8로 업그레이드를](#) 참조하십시오.

주요 개선 사항은 다음과 같습니다.

- **LeApp**은 이제 true/false 질문을 생성하여 사용자 입력을 지원하여 업그레이드 진행 방법을 결정합니다.
- 이제 Satellite 웹 UI를 사용하여 여러 호스트를 동시에 업그레이드할 수 있습니다.
- 이제 RHUI(Red Hat Update Infrastructure)를 사용하여 AWS 및 Microsoft Azure의 온디맨드 인스턴스에 대해 즉각적 업그레이드가 지원됩니다.
- [RHBA-2021:0569](#) 권고가 릴리스되면서 **Leapp** 사전 업그레이드 보고서에 대한 사용자 지정 스크립트를 생성할 수 있습니다. 자세한 내용은 [Red Hat Enterprise Linux 사전 업그레이드 보고서 워크플로 자동화](#)를 참조하십시오.

RHEL 6에서 RHEL 8로 즉각적 업그레이드

RHEL 6.10에서 RHEL 8.2로 업그레이드하려면 [RHEL 6에서 RHEL 8로 업그레이드하는](#) 방법에 대한 지침을 따르십시오.

다른 Linux 배포판에서 RHEL로 변환

CentOS Linux 8 또는 Oracle Linux 8을 사용하는 경우 Red Hat에서 지원하는 **Convert2 RHEL** 유틸리티를 사용하여 운영 체제를 RHEL 8로 변환할 수 있습니다. 자세한 내용은 [RPM 기반 Linux 배포판에서 RHEL로 변환을](#) 참조하십시오.

CentOS Linux 또는 Oracle Linux, 즉 6 또는 7의 이전 버전을 사용하는 경우 운영 체제를 RHEL로 변환한 다음 RHEL 8로 인플레이스 업그레이드를 수행할 수 있습니다. CentOS Linux 6 및 Oracle Linux 6 변환에서는 지원되지 않는 **Convert2 RHEL** 유틸리티를 사용합니다. 지원되지 않는 변환에 대한 자세한 내용은 [CentOS Linux 6 또는 Oracle Linux 6에서 RHEL 6으로 변환하는](#) 방법을 참조하십시오.

Red Hat이 다른 Linux 배포판에서 RHEL로의 변환을 지원하는 방법에 대한 자세한 내용은 [Convert2 RHEL 지원 정책 문서](#)를 참조하십시오.

OpenJDK 11 사용 가능

새로운 버전의 OpenJDK(Open Java Development Kit)가 출시되었습니다. 이 릴리스에 도입된 기능과 기존 기능의 변경 사항에 대한 자세한 내용은 [OpenJDK 기능을](#) 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 **라이프사이클**에 대한 정보는 [Red Hat Enterprise Linux 라이프 사이클](#) 문서를 참조하십시오.

- [패키지 매니페스트](#) 문서는 RHEL 8의 [패키지 목록](#)을 제공합니다.
- RHEL 7과 RHEL 8의 주요 차이점은 RHEL 8 [채택을 고려한 것으로 설명되어 있습니다](#).
- RHEL 7에서 RHEL 8로 즉각적 업그레이드를 수행하는 방법에 대한 지침은 [RHEL 7에서 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 틀입니다. 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](#)
- [킵스타트 생성기](#)
- [킵스타트 킵스타트](#)
- [Red Hat Enterprise Linux Upgrade Helper](#)
- [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 8.3은 다음 아키텍처를 지원하는 커널 버전 4.18.0-240과 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. RHEL 8의 콘텐츠 배포

3.1. 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 방법](#)은 [표준 RHEL 8](#) 설치 문서를 참조하십시오. 자동화된 Kickstart 설치 및 기타 고급 주제는 [고급 RHEL 8 설치](#) 문서를 참조하십시오.

3.2. 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 매니페스트](#)를 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, 모듈이라는 RPM 형식 또는 소프트웨어 컬렉션으로 사용할 수 있습니다. AppStream에서 사용할 수 있는 패키지 목록은 [패키지 매니페스트](#)를 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 매니페스트](#)를 참조하십시오.

3.3. 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 사용할 가능한 모듈 목록은 [패키지 매니페스트](#)를 참조하십시오.

3.4. 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](#)

4장. RHEL 8.3.1 릴리스

Red Hat은 마이너 릴리스 (8.Y)마다 분기별로 Red Hat Enterprise Linux 8 콘텐츠를 제공합니다. 분기 별 릴리스는 세 번째 숫자 (8.Y.1)로 번호가 매겨집니다. RHEL 8.3.1 릴리스의 새로운 기능은 다음과 같습니다.

4.1. 새로운 기능

여러 데스크탑 응용 프로그램을 위한 flatpak 패키지

Flatpak은 그래픽 애플리케이션을 컨테이너로 실행하는 시스템입니다. Flatpak을 사용하면 호스트 운영 체제와 독립적으로 애플리케이션을 설치하고 업데이트할 수 있습니다.

이번 업데이트에서는 Red Hat Container Catalog에서 다음 애플리케이션의 Flatpak 컨테이너 이미지를 제공합니다.

애플리케이션 이름	flatpak 컨테이너 ID
Firefox	org.mozilla.firefox
GIMP	org.gimp.GIMP
Inkscape	org.inkscape.Inkscape
Thunderpod	org.mozilla.Thunderbird

Red Hat Container Catalog에서 사용할 수 있는 Flatpak 컨테이너를 설치하려면 다음 절차를 따르십시오.

1. 최신 버전의 Flatpak 클라이언트가 시스템에 설치되어 있는지 확인합니다.

```
# yum update flatpak
```

2. RHEL Flatpak 리포지토리를 활성화합니다.

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

3. RHEL 계정의 인증 정보를 제공합니다.

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

기본적으로 Podman은 사용자가 로그아웃할 때까지만 자격 증명을 저장합니다.

4. 선택 사항: 인증 정보를 영구적으로 저장합니다.

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

5. Flatpak 컨테이너 이미지를 설치합니다.

```
$ flatpak install rhel container-id
```

(JIRA:RHELPLAN-30958,
[BZ#1920689](#),[BZ#1921179](#),[BZ#1921802](#),[BZ#1916412](#),[BZ#1921812](#),[BZ#1920604](#))

jboss Toolset을 버전 1.47.0으로 다시 설정

capsule Toolset이 1.47.0 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 컴파일 시간 평가 함수 **const fn** 이 개선되어 이제 제어 흐름 기능(예: **while** 및 **match**) 을 사용할 수 있습니다.
- 이제 새로운 **#[track_caller]** 주석을 함수에 배치할 수 있습니다. 주석이 추가된 함수의 패닉이 호출자를 소스로 보고합니다.
- pvc Standard Library는 이제 모든 길이 배열에 대한 특성을 일반적으로 구현합니다. 이전에는 배열에 대한 많은 특성 구현이 0에서 32 사이의 길이로 채워졌습니다.

사용법에 대한 자세한 지침은 사용 설명서 [를 참조하십시오](#).

(BZ#1883839)

Logging System Role이 출력에 속성 기반 필터를 지원

이번 업데이트를 통해 파일 출력, 전달 출력 및 로깅 시스템 역할의 **remote_files** 출력에 속성 기반 필터가 추가되었습니다. 이 기능은 기본 **rsyslog** 하위 역할에서 제공하며 로깅 RHEL 시스템 역할을 통해 구성할 수 있습니다. 결과적으로 사용자는 호스트 이름, 태그 및 메시지 자체와 같은 속성으로 로그 메시지를 필터링하는 기능이 로그를 관리하는 데 유용할 수 있습니다.

(BZ#1889492)

로깅 RHEL 시스템 역할에서 **rsyslog** 동작 지원

이번 개선된 기능을 통해 **rsyslog** 는 Red Hat Virtualization에서 메시지를 수신하고 **elasticsearch** 에 메시지를 전달합니다.

(BZ#1889893)

ubi8/pause 컨테이너 이미지를 사용할 수 있습니다.

Podman은 이제 **k8s.gcr.io/pause** 컨테이너 이미지 대신 **ubi8/ pause** 를 사용하여 포드의 네트워크 네임스페이스 정보를 보유합니다.

(BZ#1690785)

Podman을 버전 2.1으로 업데이트

Podman 유틸리티가 버전 2.1으로 업데이트되었습니다. 주요 개선 사항은 다음과 같습니다.

- 변경 사항:
 - Podman을 2.2.1(2.0.5)로 업데이트, Buildah에서 1.19(1.15.1), Skopeo에서 1.2.1(1.1.1)으로 업데이트, Udrca에서 0.2.3(0.2.2)으로 업데이트, CRIU에서 3.15(0.3.4)로 업데이트
 - Docker 호환 볼륨 API 끝점 (Create, Inspect, List, Remove, Prune) 사용 가능
 - 컨테이너의 systemd 장치 파일을 생성하기 위한 API 끝점 추가
 - **podman play kube** 명령에 컨테이너의 CPU 및 메모리 제한 설정을 지원합니다.

- **podman play kube** 명령에서 는 volumes라는 Podman을 사용하여 영구 볼륨 클레임을 지원 합니다.
- **podman play kube** 명령에서 **--configmap** 옵션을 통해 Kubernetes configmaps 지원
- 단축 별칭에 대한 실험적 지원이 추가되었습니다. 기본적으로 활성화되지 않지만 환경 변수 **CONTAINERS_SHORT_NAME_ALIASING** 을 on on으로 설정하여 켤 수 있습니다. 자세한 내용은 [Podman의 컨테이너 이미지 단축 이름](#)을 참조하십시오.
- 새로운 **podman image** 명령이 추가되었습니다. 이를 통해 이미지를 읽기 전용으로 마운트하여 컨테이너를 생성하지 않고도 콘텐츠를 검사할 수 있습니다.
- **podman save** 및 **podman load** 명령은 여러 이미지가 포함된 아카이브를 생성하고 로드할 수 있습니다.
- 이제 네트워크 오류로 인해 가져오기가 실패하면 Podman에서 이미지 가져오기를 최대 3번 다시 시도합니다.
- 버그 수정:
 - cgroup v1 시스템의 컨테이너에서 systemd를 실행하지 못하는 버그 수정

Buildah 도구가 버전 1.19로 업데이트되었습니다. 주요 개선 사항은 다음과 같습니다.

- 변경 사항:
 - **buildah inspect** 명령은 매니페스트 검사를 지원
 - **buildah push** 명령은 매니페스트 목록 및 다이제스트 푸시를 지원합니다.
 - **--manifest** 플래그 지원 추가
 - 아키텍처 및 OS를 선택하려면 **--arch** 및 **--os** 및 **--variant** 옵션이 추가되었습니다.
 - 사용자가 stdin을 컨테이너에 지정할 수 있음
 - from 이 **--from** 옵션을 사용하여 재정의되도록 허용
 - alternate **.docker ignore** 플래그를 사용하기 위해 추가된 **--ignore file** 플래그
 - 짧은 이름 별칭
 - **buildah pull** 명령에 **--policy** 옵션 추가
 - **buildah mount** 명령을 수정하여 ID가 아닌 컨테이너 이름을 표시
 - 개선된 buildah 완료
 - **--timestamp** 대신 **--controllt-timestamp** 플래그를 사용하십시오.
 - 복사를 위해 파이프 사용
 - **buildah bud** 명령에 **--ct-timestamp** 플래그 추가
 - 컨테이너에 VFS 추가 이미지 저장소 추가
 - 마운트 옵션에서 "ro"에 별칭으로 "readonly" 허용

- Buildah, 버드: 병렬 실행을 위한 **--jobs=N** 옵션 지원

Skopeo 툴이 버전 1.2.1로 업데이트되었습니다. 주요 개선 사항은 다음과 같습니다.

- 변경 사항:
 - Travis를 통해 업스트림 및 안정적인 skopeo 이미지에 대한 다중 아키텍처 빌드 추가
 - 동기화된 다이제스트에 대한 지원 추가
 - 복사 **--all** 을 에뮬레이션하기 위해 **--all** 동기화 플래그가 추가되었습니다
 - **skopeo inspect** 명령에 **--format** 옵션 추가

Udica 툴이 0.2.3 버전으로 업데이트되었습니다. 주요 개선 사항은 다음과 같습니다.

- 변경 사항:
 - 호스트 포트가 아닌 컨테이너 포트 활성화
 - **--version** 옵션 추가

CRIU 툴이 버전 3.15로 업데이트되었습니다. 주요 개선 사항은 다음과 같습니다.

- 변경 사항:
 - 초기 cgroup2 지원
 - 합법적인 swrk API 및 이를 통해 fds를 상속할 수 있는 기능 추가
 - 외부 바인딩 마운트 및 tasks-to-cgroups 바인딩
 - **ibcriu.so** (RPC 래퍼) 및 플러그인

(JIRA:RHELPLAN-55998)

5장. RHEL 8.3.0 릴리스

5.1. 새로운 기능

이 부분에서는 Red Hat Enterprise Linux 8.3에 도입된 새로운 기능 및 주요 개선 사항에 대해 설명합니다.

5.1.1. 설치 프로그램 및 이미지 생성

Anaconda가 버전 33.16으로 업데이트

이 릴리스에서 Anaconda는 버전 33.16으로 업데이트되었습니다. 이 버전은 이전 버전에 비해 다음과 같은 주요 개선사항을 제공합니다.

- 이제 설치 프로그램에 정적 IPv6 주소가 여러 줄에 표시되고 더 이상 창의 크기를 조정하지 않습니다.
- 이제 설치 프로그램에 지원되는 NVDIMM 장치 섹터 크기가 표시됩니다.
- 설치된 시스템에 IPv6 정적 구성이 있는 호스트 이름이 올바르게 구성됩니다.
- 이제 디스크 암호화 암호에서 ASCII가 아닌 문자를 사용할 수 있습니다.
- 설치 프로그램에는 /boot, /tmp 및 /var/local 및 /var/www를 제외한 모든 /var 및 /usr 마운트 지점에서 새 파일 시스템을 만드는 적절한 권장 사항이 표시됩니다.
- 이제 설치 프로그램에서 키보드 레이아웃을 올바르게 확인하고 키보드 키(ALT+SHIFT)를 사용하여 다양한 레이아웃과 언어를 전환할 때 키보드 레이아웃 화면의 상태를 변경하지 않습니다.
- 기존 RAID1 파티션이 있는 시스템에서 더 이상 복구 모드가 실패하지 않습니다.
- 이제 **Manual Partitioning** (수동 파티셔닝) 화면에서 컨테이너의 LUKS 버전을 변경할 수 있습니다.
- **btrfs-progs** 패키지 없이 설치 프로그램이 설치를 성공적으로 완료합니다.
- 이제 설치 프로그램에서 암호화된 컨테이너에 기본 LUKS2 버전을 사용합니다.
- Kickstart 파일이 **ignoredisk** (논리 볼륨 그룹) 목록에 PV(논리 볼륨 그룹)를 배치하면 설치 프로그램이 더 이상 충돌하지 않습니다.
- 시스템 루트의 새 마운트 경로 **/mnt/sysroot** 가 도입되었습니다. 이 경로는 대상 시스템의 /를 마운트하는 데 사용됩니다. 일반적으로 물리적 루트와 시스템 루트는 동일하므로 **/mnt/sysroot** 는 **/mnt/sysimage** 와 동일한 파일 시스템에 연결됩니다. 유일한 예외는 배포를 기반으로 시스템 루트가 변경되는 rpm-ostree 시스템입니다. 그런 다음 **/mnt/sysroot** 가 **/mnt/sysimage** 의 하위 디렉토리에 연결됩니다. chroot에 **/mnt/sysroot** 를 사용하는 것이 좋습니다.

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

RHEL 설치 프로그램의 GUI 변경 사항

RHEL 설치 프로그램에는 Installation Summary(설치 요약) 창의 다음 사용자 설정이 포함됩니다.

- 루트 암호
- 사용자 생성

이 변경으로 설치를 시작하기 전에 루트 암호를 구성하고 사용자 계정을 만들 수 있습니다. 이전에는 설치 프로세스를 시작한 후 루트 암호를 구성하고 사용자 계정을 생성했습니다.

루트 암호는 시스템 관리 작업에 사용되는 관리자(수퍼유저 또는 루트라고도 함) 계정에 로그인하는 데 사용됩니다. 사용자 이름은 명령줄에서 로그인하는 데 사용됩니다. 그래픽 환경을 설치하는 경우 그래픽 로그인 관리자는 전체 이름을 사용합니다. 자세한 내용은 [표준 RHEL 설치 문서 수행](#)을 참조하십시오.

(JIRA:RHELPLAN-40469)

이미지 빌더 백엔드 **osbuild-composer** 가 **lorax-composer**를 대체합니다.

osbuild-composer 백엔드는 **lorax-composer** 를 대체합니다. 새 서비스는 이미지 빌드를 위한 REST API를 제공합니다. 결과적으로 사용자는 보다 안정적인 백엔드와 보다 예측 가능한 출력 이미지를 활용할 수 있습니다.

(BZ#1836211)

Image Builder **osbuild-composer** 는 이미지 유형 세트를 지원합니다.

osbuild-composer 백엔드 교체를 통해 이번에는 **osbuild-composer** 에서 지원되는 다음 이미지 유형 세트가 지원됩니다.

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

다음 출력은 이번에는 지원되지 않습니다.

- ext4-filesystem
- partitioned-disk
- Ping Cloud
- Google GCE

(JIRA:RHELPLAN-42617)

Image Builder 는 GUI를 통해 클라우드에 대한 푸시 지원

이 향상된 기능을 통해 사용자는 GUI 이미지 빌더를 통해 **Azure** 및 **AWS** 서비스 클라우드로 푸시하는 옵션을 선택할 수 있습니다. 결과적으로 사용자는 더 쉬운 업로드 및 인스턴스화를 통해 이점을 얻을 수 있습니다.

(JIRA:RHELPLAN-30878)

5.1.2. 에지용 RHEL

에지 이미지용 RHEL 소개

이번 릴리스에서는 이제 에지 서버에 대한 사용자 지정 RHEL 이미지를 만들 수 있습니다.

Image Builder를 사용하여 에지 이미지의 RHEL을 생성한 다음 RHEL 설치 프로그램을 사용하여 AMD 및 Intel 64비트 시스템에 배포할 수 있습니다. Image Builder는, **tar** 파일에 **rhel-edge-commit** 로 에지 이미지의 RHEL을 생성합니다.

RHEL for Edge 이미지는 에지 서버에 RHEL을 원격으로 설치하기 위한 시스템 패키지가 포함된 **rpm-ostree** 이미지입니다.

시스템 패키지에는 다음이 포함됩니다.

- 기본 OS 패키지
- 컨테이너 엔진으로 Podman

이미지를 사용자 지정하여 요구 사항에 따라 OS 콘텐츠를 구성하고 물리적 및 가상 시스템에 배포할 수 있습니다.

에지용 RHEL 이미지를 사용하면 다음을 수행할 수 있습니다.

- Atomic 업그레이드: 각 업데이트의 상태가 알려져 장치를 재부팅할 때까지 변경 사항이 표시되지 않습니다.
- 업그레이드에 실패한 경우 Greenboot 및 지능적 롤백을 사용한 사용자 정의 상태 점검.
- 애플리케이션 업데이트에서 핵심 OS 업데이트를 분리하고 다양한 버전의 애플리케이션을 테스트 및 배포할 수 있는 컨테이너 중심 워크플로.
- 대역폭이 낮은 환경에 최적화된 OTA 페이로드.
- Greenboot를 사용한 사용자 정의 상태 점검을 통해 복원력을 확보합니다.

에지 이미지의 RHEL 구성, 설치 및 관리에 대한 자세한 내용은 엣지 이미지의 [RHEL 구성, 설치 및 관리](#)를 참조하십시오.

(JIRA:RHELPLAN-56676)

5.1.3. 소프트웨어 관리

최상의 **dnf** 구성 옵션의 기본값이 **True** 에서 **False**로 변경되었습니다.

이번 업데이트를 통해 원래 **dnf** 동작을 유지하기 위해 기본 구성 파일에서 최상의 **dnf** 구성 옵션의 값이 **True** 로 설정되었습니다. 결과적으로 기본 구성 파일을 사용하는 사용자의 경우 동작은 변경되지 않습니다.

고유한 구성 파일을 제공하는 경우 원래 동작을 유지하기 위해 **best=True** 옵션이 있는지 확인합니다.

(BZ#1832869)

dnf reposync 명령의 새로운 **--norepopath** 옵션을 사용할 수 있습니다.

이전에는 **reposync** 명령에서 기본적으로 다운로드한 각 리포지토리의 **--download-path** 디렉터리에 하위 디렉터리를 생성했습니다. 이번 업데이트를 통해 **--norepopath** 옵션이 도입되었으며 **reposync** 는 하위 디렉터리를 생성하지 않습니다. 결과적으로 리포지토리가 **--download-path** 에 지정된 디렉터리로 직접 다운로드됩니다. 이 옵션은 **YUM v3** 에도 있습니다.

(BZ#1842285)

libdnf 플러그인을 활성화 및 비활성화하는 기능

이전에는 서브스크립션 검사가 RHEL 버전의 **libdnf** 플러그인으로 하드 코딩되었습니다. 이번 업데이트를 통해 **microdnf** 유틸리티는 **libdnf** 플러그인을 활성화 및 비활성화할 수 있으며 이제 서브스크립션 검사를 DNF와 동일한 방식으로 비활성화할 수 있습니다. 서브스크립션 확인을 비활성화하려면 **--disableplugin=subscription-manager** 명령을 사용합니다. 모든 플러그인을 비활성화하려면 **--noplugins** 명령을 사용합니다.

([BZ#1781126](#))

5.1.4. 셸 및 명령행 툴

자동 업데이트

RHEL 8.3에는 **ReaR**(Relax-and- Recovery) 유틸리티에 대한 여러 업데이트가 도입되었습니다. 주요 변경 사항은 다음과 같습니다.

- 외부 백업 소프트웨어로 타사 CDM(Rubrik Cloud Data Management) 지원이 추가되었습니다. 이를 사용하려면 구성 파일의 **BACKUP** 옵션을 **CDM** 으로 설정합니다.
- IBM POWER에서 4GB보다 큰 파일로 복구 이미지를 생성하면 little endian 아키텍처가 활성화되었습니다.
- **ReaR** 에 의해 생성된 디스크 레이아웃에는 더 이상 Rancher 2 장치 iSCSI 장치 및 파일 시스템에 대한 항목이 포함되지 않습니다.

([BZ#1743303](#))

smartmontools 버전 7.1으로 다시 기반

smartmontools 패키지가 버전 7.1으로 업그레이드되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 드라이브 데이터베이스에 HDD, SSD 및 USB 추가.
- JSON 출력 모드를 활성화하기 위한 새로운 옵션 **-j** 및 **--json**.
- 일부 SAS SSD의 불완전한 로그 하위 페이지 응답에 대한 해결방법.
- **READ CAPACITY** 명령 처리 개선.
- 로그 페이지의 디코딩에 대한 다양한 개선 사항.

([BZ#1671154](#))

opencryptoki 가 3.14.0 버전으로 업데이트

opencryptoki 패키지가 버전 3.14.0으로 업그레이드되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- EP11 암호화 서비스 개선 사항:
 - Dilithium 지원
 - Edwards-curve 전자 서명 알고리즘 (EdDSA) 지원
 - 비SHA1 해시 및 마스크 생성 기능(MGF)을 포함하는 Rivest-Shamir-Adleman 최적의 비대칭 암호화 패딩(RSA-OAEP) 지원

- 프로세스 및 스레드 잠금 강화
- 향상된 **btree** 및 오브젝트 잠금
- 새로운 IBM Z 하드웨어 z15 지원
- 신뢰할 수 있는 플랫폼 모듈(TPM), ICA(IBM 암호화 아키텍처) 및 통합 암호화 서비스 기능을 위한 여러 토큰 인스턴스 지원
- **openCryptoki** 토큰 저장소에 토큰 키를 나열하는 새로운 도구 **p11sak** 을 추가했습니다.
- 토큰 리포지토리를 FIPS 호환 암호화로 마이그레이션하는 유틸리티 추가
- 고정 **pkcsep11_migrate** 도구
- ICSF 소프트웨어의 마이너 수정

(BZ#1780293)

Gpgme 가 1.13.1 버전으로 업데이트.

gpgme 패키지가 업스트림 버전 1.13.1으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 새로운 컨텍스트 플래그 **no-symkey-cache** (GnuPG 2.2.7 이상에서 사용 시), **request-origin** (GnuPG 2.2.6 이상에서 사용 시), **auto-key-locate** 및 **trust-model** 이 도입되었습니다.
- 웹 브라우저용 기본 메시징 서버로 새 도구 **gpgme-json** 이 추가되었습니다. 현재 공개 키 암호화 및 암호 해독이 지원됩니다.
- 숨겨진 수신자 옵션을 포함한 직접 키 사양을 지원하고 파일에서 키를 가져오는 새로운 암호화 API가 도입되었습니다. 또한 하위 키를 사용할 수 있습니다.

(BZ#1829822)

5.1.5. 인프라 서비스

PowerTOP 버전 2.12로 업데이트

powertop 패키지가 버전 2.12로 업그레이드되었습니다. 이전에 사용 가능한 버전 2.11에 대한 주요 변경 사항은 다음과 같습니다.

- SATA 링크 PM의 경우 장치 인터페이스 전원 관리(DIPM) 사용.
- Intel®t Lake 모바일 및 데스크탑 시스템, Skylake 서버 및 Atom 기반 Treᄁ 아키텍처(Jasper Lake) 지원.

(BZ#1783110)

버전 2.14.0으로 재구성

tuned 패키지가 업스트림 버전 2.14.0으로 업그레이드되었습니다. 주요 개선 사항은 다음과 같습니다.

- **optimize-serial-console** 프로필이 도입되었습니다.
- 로드된 프로파일에 대한 지원이 추가되었습니다.
- **irqbalance** 설정을 처리하기 위한 **irqbalance** 플러그인이 추가되었습니다.

- ThunderX 및 AMD 기반 플랫폼을 위한 아키텍처별 튜닝이 추가되었습니다.
- CPU 선호도 설정에 대해 **cgroups-v1** 을 지원하도록 스케줄러 플러그인이 확장되었습니다.

([BZ#1792264](#))

tcpdump 가 버전 4.9.3으로 업데이트

tcpdump 유틸리티가 CVE(Common Vulnerabilities and Exposures)를 수정하기 위해 버전 4.9.3으로 업데이트되었습니다.

([BZ#1804063](#))

libpcap 버전 1.9.1로 업데이트

libpcap 패키지가 CVE(Common Vulnerabilities and Exposures)를 수정하기 위해 버전 1.9.1로 업데이트되었습니다.

([BZ#1806422](#))

iperf3 에서 클라이언트 측의 **sctp** 옵션 지원

이 향상된 기능을 통해 사용자는 네트워크 처리량을 테스트하는 클라이언트 측에서 TCP(Transmission Control Protocol) 대신 SCTP(Stream Control Transmission Protocol)를 사용할 수 있습니다.

iperf3 에 대한 다음 옵션은 이제 테스트의 클라이언트 측에서 사용할 수 있습니다.

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

자세한 내용은 **iperf3** 도움말 페이지의 **클라이언트 특정 옵션**을 참조하십시오.

([BZ#1665142](#))

iperf3 에서 **SSL**지원

이 향상된 기능을 통해 사용자는 클라이언트와 서버 간에 RSA 인증을 사용하여 서버에 대한 연결을 합법적인 클라이언트로만 제한할 수 있습니다.

이제 서버 측에서 **iperf3** 에 대한 다음 옵션을 사용할 수 있습니다.

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

iperf3 에 대한 다음 옵션은 이제 클라이언트 통신 측에서 사용할 수 있습니다.

- **--username**
- **--rsa-public-key-path**

([BZ#1700497](#))

9.11.20으로 다시 기반 연결

bind 패키지가 버전 9.11.20으로 업그레이드되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 여러 경쟁 조건을 수정하여 많은 CPU 코어를 사용하는 시스템의 신뢰성 향상.
- 자세한 오류 보고: **dig** 및 기타 도구가 이제 EED(Extended DNS Error) 옵션이 있는 경우 출력할 수 있습니다.
- AXFR(Inbound DNS Zone Transfer Protocol) 전송의 메시지 ID가 확인되고 일치하지 않는 경우 기록됩니다.

(BZ#1818785)

printk 값을 줄여서 I/O를 직렬 콘솔로 줄이는 새로운 optimize-serial-console TuneD 프로파일

이번 업데이트를 통해 새로운 **optimize-serial-console** TuneD 프로필을 사용할 수 있습니다. 일부 시나리오에서는 커널 드라이버가 많은 양의 I/O 작업을 직렬 콘솔에 보낼 수 있습니다. 이러한 동작으로 인해 I/O가 직렬 콘솔에 기록되는 동안 일시적으로 응답하지 않을 수 있습니다. **optimize-serial-console** 프로파일은 **printk** 값을 기본값 7 4 1 7에서 4 4 1로 줄여 이 I/O를 줄입니다. 시스템에서 이러한 변경을 수행하려는 직렬 콘솔이 있는 사용자는 다음과 같이 시스템을 재설정할 수 있습니다.

```
# tuned-adm profile throughput-performance optimize-serial-console
```

결과적으로 사용자는 재부팅 시 지속되는 출력 값이 낮으므로 시스템이 중단될 가능성이 줄어듭니다.

이 TuneD 프로파일은 디버깅 정보를 제거하여 직렬 콘솔에 기록된 I/O의 양을 줄입니다. 이 디버깅 정보를 수집해야 하는 경우 이 프로파일은 활성화되지 않고 출력 값이 7 4 1 7로 설정되어 있는지 확인해야 합니다. **printk** run 값을 확인하려면 다음을 실행합니다.

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

(BZ#1840689)

AMD 기반 플랫폼에 대한 새로운 TuneD 프로파일 추가

RHEL 8.3에서는 AMD 기반 플랫폼에 대한 튜닝을 포함하도록 **throughput-performance** TuneD 프로파일 이 업데이트되었습니다. 매개 변수를 수동으로 변경할 필요가 없으며 **AMD** 시스템에서 튜닝이 자동으로 적용됩니다. **AMD Epyc** 및 **authenticate** 시스템은 기본 **throughput-performance** 프로파일에서 다음 매개 변수를 변경합니다.

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

이번 개선된 기능을 통해 시스템 성능이 ~5% 향상되었습니다.

(BZ#1746957)

Memcached 가 버전 1.5.22로 업데이트

memcached 패키지가 버전 1.5.22로 업그레이드되었습니다. 이전 버전에 대한 주요 변경 사항은 다음과 같습니다.

- TLS가 활성화되어 있습니다.
- **-o inline_ascii_response** 옵션이 제거되었습니다.
- ASCII 프로토콜의 인증 모드와 함께 **-Y [authfile]** 옵션이 추가되었습니다.
- **Memcached** 는 이제 다시 시작할 때 캐시를 복구할 수 있습니다.

- 새로운 실험적 메타 명령이 추가되었습니다.
- 다양한 성능 향상.

([BZ#1809536](#))

5.1.6. 보안

Cyrus SASL 은 **SASL /GSSAPI** 및 **SASL/ GSS-SPNEGO** 플러그인으로 채널 바인딩을 지원합니다.

이번 업데이트에서는 **SASL/GSSAPI** 및 **SASL/ GSS-SPNEGO** 플러그인으로 채널 바인딩에 대한 지원이 추가되었습니다. 그 결과, **openldap** 라이브러리에서 이 기능을 사용하면 **Cyrus SASL** 이 LDAP 연결에 대한 필수 채널 바인딩을 도입하는 Microsoft Active Directory 및 Microsoft Windows 시스템과의 호환성을 유지할 수 있습니다.

([BZ#1817054](#))

Libreswan이 3.32로 다시 기반

이번 업데이트를 통해 Libreswan은 여러 가지 새로운 기능과 버그 수정이 포함된 업스트림 버전 3.32로 업데이트되었습니다. 주요 기능은 다음과 같습니다.

- Libreswan에는 더 이상 별도의 FIPS 140-2 인증이 필요하지 않습니다.
- Libreswan은 RFC 8247의 암호화 권장 사항을 구현하고 SHA-1 및 RSA-PKCS v1.5에서 SHA-2 및 RSA-PSS로 기본 설정을 변경합니다.
- Libreswan은 방화벽 규칙 작성을 간소화하는 XFRMi 가상 ipsecXX 인터페이스를 지원합니다.
- 전체 메시 암호화 네트워크에서 충돌 및 재부팅된 노드를 복구하는 기능이 향상되었습니다.

([BZ#1820206](#))

libssh 라이브러리가 4.4.4 버전으로 업데이트되었습니다.

SSH 프로토콜을 구현하는 **libssh** 라이브러리가 4.8.4 버전으로 업그레이드되었습니다.

이번 업데이트에는 다음과 같은 버그 수정 및 개선 사항이 포함되어 있습니다.

- PEM 파일에 **Ed25519** 키에 대한 지원이 추가되었습니다.
- **diffie-hellman-group14-sha256** 키 교환 알고리즘에 대한 지원이 추가되었습니다.
- **libssh** 클라이언트 구성 파일의 **Match** 키워드에 **localuser** 에 대한 지원이 추가되었습니다.
- 일치 기준 키워드 인수가 대소문자를 구분합니다(키 입력은 대소문자를 구분하지 않지만 키워드 인수는 대소문자를 구분합니다)
- 고정 CVE-2019-14889 및 CVE-2020-1730.
- 알려진 호스트 파일에 제공된 경로 문자열에 누락된 디렉터리를 재귀적으로 생성하는 기능이 추가되었습니다.
- 주석과 선행 공백이 있는 PEM 파일에 **OpenSSH** 키 지원이 추가되었습니다.
- **libssh** 서버 구성에서 **OpenSSH** 서버 구성이 제거되었습니다.

([BZ#1804797](#))

GNUTLS 가 3.6.14로 다시 기반

gnutls 패키지는 업스트림 버전 3.6.14로 업데이트되었습니다. 이 버전은 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- **Gnutls** 에서 잘못된 문자 또는 포맷이 포함된 **Time** 필드가 포함된 인증서를 거부합니다.
- **Gnutls** 는 이제 신뢰할 수 있는 CA 인증서에 최소 키 크기가 있는지 확인합니다.
- 암호화된 개인 키를 표시할 때 **certtool** 유틸리티에는 더 이상 일반 텍스트 설명이 포함되지 않습니다.
- **gnutls** 를 사용하는 서버는 이제 OCSP-stapling 지원을 알립니다.
- **gnutls** 를 사용하는 클라이언트는 이제 요청 시에만 OCSP 스테이플을 보냅니다.

([BZ#1789392](#))

Gnutls FIPS DH 검사는 이제 NIST SP 800-56A 개정을 따릅니다. 3

gnutls 패키지의 이번 업데이트에서는 NIST 특수 발행 800-56A 버전 3, 섹션 5.7.1.1 및 5.7.1.2, 2단계에 필요한 검사를 제공합니다. 향후 FIPS 140-2 인증에는 변경이 필요합니다. 결과적으로 **gnutls** 는 FIPS 모드에서 작동할 때 Diffie-Hellman 키 교환 중에 RFC 7919 및 RFC 3526에서 2048비트 또는 더 큰 매개변수만 허용합니다.

([BZ#1849079](#))

Gnutls 는 이제 NIST SP 800-56A rev 3에 따라 검증을 수행합니다.

이 **gnutls** 패키지 업데이트는 NIST 특수 발행 800-56A 버전 3, 5.6.2.2.2 및 5.6.2.1.3 2단계에 필요한 검사를 추가합니다. 또한 향후 FIPS 140-2 인증을 위해 **gnutls** 를 준비합니다. 결과적으로 **gnutls** 는 FIPS 모드에서 작동할 때 Diffie-Hellman 키 교환 중에 생성 및 수신된 공개 키에 대한 추가 검증 단계를 수행합니다.

([BZ#1855803](#))

update-crypto-policies 및 fips-mode-setup 이 crypto-policies-scripts로 이동

이전에 **crypto-policies** 패키지에 포함된 **update-crypto-policies** 및 **fips-mode-setup** 스크립트가 이제 별도의 RPM 하위 패키지 **crypto-policies-scripts** 로 이동되었습니다. 패키지는 일반 설치에 대한 Recommends 종속성을 통해 자동으로 설치됩니다. 이를 통해 **ubi8/ubi-minimal** 이미지가 활성화되어 Python 언어 인터프리터가 포함되지 않아 이미지 크기가 줄어듭니다.

([BZ#1832743](#))

OpenSC가 버전 0.20.0으로 업데이트

opensc 패키지는 여러 버그 및 보안 문제를 처리하는 버전 0.20.0으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 이번 업데이트를 통해 **CVE-2019-6502**, **CVE-2019-15946**, **CVE-2019-15945**, **CVE-2019-19480**, **CVE-2019-19481** 및 **CVE-2019-19479** 보안 문제가 수정되었습니다.
- OpenSC 모듈은 이제 **C_WrapKey** 및 **C_UnwrapKey** 함수를 지원합니다.
- 이제 이 기능을 사용하여 카드 리더의 삽입 및 제거를 탐지할 수 있습니다.
- **pkcs11-tool** 유틸리티는 이제 **CKA_ALLOWED_MECHANISMS** 특성을 지원합니다.
- 이번 업데이트에서는 **OsEID** 카드를 기본 감지할 수 있습니다.

- OpenPGP Card v3에서는 ECC(**Elliptic Curve Cryptography**)를 지원합니다.
- 이제 PKCS#11 URI가 ellipsis를 사용하여 리더 이름을 잘립니다.

([BZ#1810660](#))

S tunnel 이 5.56 버전으로 업데이트

이번 업데이트를 통해 **stunnel** 암호화 래퍼는 여러 가지 새로운 기능과 버그 수정을 포함하는 업스트림 버전 5.56으로 다시 기반했습니다. 주요 기능은 다음과 같습니다.

- 새로운 티켓 **KeySecret** 및 티켓 **MacSecret** 옵션은 발급된 세션 티켓의 기밀성 및 무결성 보호를 제어합니다. 이러한 옵션을 사용하면 클러스터의 다른 노드에서 세션을 다시 시작할 수 있습니다.
- OpenSSL 1.1.0 이상에서 타원 곡선 목록을 제어하는 새로운 곡선 **옵션**.
- 허용된 TLS 1.3 암호화 정책 목록을 제어하는 새로운 **ciphersuites** 옵션.
- OpenSSL 1.1.0 이상에 **sslVersion**, **sslVersionMin** 및 **sslVersionMax** 가 추가되었습니다.

([BZ#1808365](#))

libkcapi 가 버전 1.2.0으로 업데이트

libkcapi 패키지는 부 변경 사항이 포함된 업스트림 버전 1.2.0으로 다시 기반했습니다.

([BZ#1683123](#))

setools 가 4.3.0으로 다시 기반

SELinux 정책 분석을 용이하게 하는 툴 모음인 **setools** 패키지가 버전 4.3.0으로 업그레이드되었습니다.

이번 업데이트에는 다음과 같은 버그 수정 및 개선 사항이 포함되어 있습니다.

- TE(type Enforcement) 규칙에 대한 수정된 **sediff** 방법으로 메모리 및 런타임 문제가 크게 줄어 듭니다.
- **infiniband** 컨텍스트 지원 추가 to **seinfo**, **sediff** 및 **apol**.
- 온라인 문서를 표시하는 데 사용되는 Qt 도우미 도구의 위치에 대한 **apol** 구성이 추가되었습니다.
- 다음과 관련된 해결 **sediff** 문제 :
 - 요청되지 않은 경우 표시되는 속성 헤더입니다.
 - **type_transition** 파일의 이름 비교.
- 맵 소켓 **sendto** 정보 흐름 방향에 대한 고정된 권한.
- **TypeAttribute** 클래스에 추가된 메서드로 전체 Python 컬렉션이 되도록 합니다.
- 이제 **Genfscon** 은 **libsepol** 에서 삭제된 고정 값을 사용하는 대신 클래스를 조회합니다.

setools 패키지에는 다음 패키지가 필요합니다.

- **setools-console**
- **setools-console-analyses**

- **setools-gui**

(BZ#1820079)

개별 CephFS 파일 및 디렉터리에 SELinux 레이블이 있을 수 있음

Ceph 파일 시스템(CephFS)은 최근에 SELinux 레이블을 확장된 파일 속성에 저장하도록 활성화했습니다. 이전에는 CephFS 볼륨의 모든 파일에 하나의 공통 레이블 **system_u:object_r:cephfs_t:s0**로 레이블이 지정되었습니다. 이번 개선된 기능을 통해 개별 파일의 레이블을 변경할 수 있으며 SELinux는 전환 규칙에 따라 새로 생성된 파일의 레이블을 정의합니다. 이전에 레이블이 없는 파일에는 명시적으로 변경될 때까지 **system_u:object_r:cephfs_t:s0** 레이블이 있습니다.

(BZ#1823764)

OpenSCAP 을 버전 1.3.3로 업데이트

openscap 패키지가 업스트림 버전 1.3.3로 업그레이드되어 이전 버전에 대해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- CLI(명령줄 인터페이스)를 사용하여 맞춤형 파일을 생성할 수 있는 **autotailor** 스크립트가 추가되었습니다.
- 시간대 부분을 XCCDF(Extensible Configuration Checklist Description Format) TestResult 시작 및 종료 타임스탬프에 추가
- **yamfilecontent** 독립 프로브를 초안 구현으로 추가했습니다.
- XCCDF에서 **urn:xccdf:fix:script:kubernetes** 수정 유형을 도입했습니다.
- **machineconfig** 수정을 생성하는 기능이 추가되었습니다.
- **oscap-podman** 툴에서 모호한 검사 대상을 감지할 수 있습니다.
- **rpmverifyfile** 프로브는 이제 **/bin** 디렉토리에서 파일을 확인할 수 있습니다.
- 복잡한 regexes가 **textfilecontent58** 프로브에서 실행될 때 수정된 충돌.
- XCCDF 보고서의 평가 특성은 **system_info** 프로브의 OVAL 엔터티와 일치합니다.
- **textfilecontent58** 프로브의 오프라인 모드에서 일치하는 고정 파일 경로 패턴입니다.
- **systemdunitdependency** 프로브에서 고정된 무한 재귀.

(BZ#1829761)

SCAP Security Guide는 CIS RHEL 8 벤치마크 v1.0.0과 일치하는 프로파일을 제공합니다.

이번 업데이트를 통해 **scap-security-guide** 패키지는 CIS Red Hat Enterprise Linux 8 벤치마크 v1.0.0에 맞는 프로필을 제공합니다. 이 프로필을 사용하면 CIS(Center for Internet Security)의 지침을 사용하여 시스템 구성을 강화할 수 있습니다. 결과적으로 CIS Ansible 플레이북 및 CIS SCAP 프로필을 사용하여 CIS로 RHEL 8 시스템을 구성하고 자동화할 수 있습니다.

CIS 프로필의 **rpm_verify_permissions** 규칙이 제대로 작동하지 않습니다.

(BZ#1760734)

scap-security-guide 에서 HIPAA를 구현하는 프로파일 제공

scap-security-guide 패키지 업데이트는 RHEL 8 보안 준수 콘텐츠에 HIPAA(Health Insurance Portability and Accountability Act) 프로필을 추가합니다. 이 프로필은 [HIPAA 개인 정보 보호 규칙](#) 웹 사이트에 설명된 권장 사항을 구현합니다.

HIPAA 보안 규칙(HIPAA Security Rule)은 미국 국가 표준에 따라 생성, 수신, 사용 또는 관리되는 개인 의료 정보를 관리합니다. 보안 규칙에서는 전자 보호 의료 정보의 기밀성, 무결성 및 보안을 보장하기 위해 적절한 관리, 물리적 및 기술 보호 조치가 필요합니다.

([BZ#1832760](#))

scap-security-guide 가 0.1.50으로 업데이트

Linux 시스템에 대한 최신 보안 정책 세트를 포함하는 **scap-security-guide** 패키지가 0.1.50 버전으로 업그레이드되었습니다.

이 업데이트에는 버그 수정 및 개선 사항이 포함되어 있습니다. 특히 다음과 같습니다.

- Ansible 콘텐츠가 개선되었습니다. 수많은 규칙에는 처음으로 Ansible 해결이 포함되고 버그 수정을 해결하기 위해 다른 규칙이 업데이트되었습니다.
- RHEL7 시스템 스캔을 위한 **scap-security-guide** 콘텐츠 수정 및 개선 사항:
 - **scap-security-guide** 패키지는 이제 CIS RHEL 7 벤치마크 v2.2.0에 맞는 프로필을 제공합니다. CIS 프로필의 **rpm_verify_permissions** 규칙이 제대로 작동하지 않습니다. CIS 프로필에서 **rpm_verify_permissions**가 실패하는 것을 확인합니다.
 - SCAP 보안 가이드 프로필은 이제 시작하지 않아야 하는 서비스를 올바르게 비활성화하고 마스킹합니다.
 - **scap-security-guide** 패키지의 **audit_rules_privileged_commands** 규칙이 권한 있는 명령에 대해 올바르게 작동합니다.
 - **scap-security-guide** 패키지에서 **dconf_gnome_login_banner_text** 규칙을 수정해도 더 이상 잘못 실패하지 않습니다.

([BZ#1815007](#))

SCAP Workbench 가 맞춤형 프로파일에서 결과 기반 수정을 생성할 수 있음

이번 업데이트를 통해 **SCAP Workbench** 툴을 사용하여 맞춤형 프로파일에서 결과 기반 수정 역할을 생성할 수 있습니다.

([BZ#1640715](#))

새로운 Ansible 역할은 Clevis 클라이언트의 자동화된 배포를 제공합니다.

이번 **rhel-system-roles** 패키지 업데이트에서는 **nbde_client** RHEL 시스템 역할이 도입되었습니다. 이 Ansible 역할을 사용하면 자동화된 방식으로 여러 Clevis 클라이언트를 배포할 수 있습니다.

([BZ#1716040](#))

새로운 Ansible 역할에서 Tang 서버를 설정할 수 있음

이 향상된 기능을 통해 새로운 **nbde_server** 시스템 역할을 사용하여 자동화된 디스크 암호화 솔루션의 일부로 Tang 서버를 배포하고 관리할 수 있습니다. **rhel-system-roles** 패키지에 포함된 **nbde_server** Ansible 역할은 다음 기능을 지원합니다.

- Tang 키 순환

- Tang 키 배포 및 백업

자세한 내용은 [Tang 서버 키](#) 순환을 참조하십시오.

(BZ#1716039)

Clevis 가 버전 13으로 다시 기반

clevis 패키지는 여러 버그 수정 및 개선 사항을 제공하는 버전 13으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- **Clevis luks unlock** 는 비대화형 모드에서 키 파일이 있는 장치에서 사용할 수 있습니다.
- **Clevis encrypt tpm2** 는 입력이 JSON 배열로 제공되는 경우 **pcr_ids** 필드를 구문 분석합니다.
- **clevis-luks-unbind(1)** 도움말 페이지는 더 이상 LUKS v1만 참조하지 않습니다.
- 지정된 암호가 올바르지 않으면 **Clevis luks bind** 가 비활성 슬롯에 더 이상 기록되지 않습니다.
- **Clevis luks**는 현재 바인딩 되어 있지 않은 영어 로케일을 사용하는 동안 바인딩됩니다.
- **tpm2-tools** 4.x에 대한 지원이 추가되었습니다.

(BZ#1818780)

Clevis luks edit 를 통해 특정 고정 구성을 편집할 수 있습니다.

이번 **clevis** 패키지 업데이트에서는 새로운 **clevis luks edit** 하위 명령을 도입하여 특정 고정 구성을 편집할 수 있습니다. 예를 들어 TPM2 구성에서 Tang 서버의 URL 주소와 **pcr_ids** 매개 변수를 변경할 수 있습니다. 새 **sss** 고정을 추가 및 제거하고 **sss** pin의 임계값을 변경할 수도 있습니다 .

(BZ#1436735)

Clevis luks bind -y 에서 자동 바인딩 허용

이 향상된 기능을 통해 Clevis는 **-y** 매개변수를 사용한 자동화된 바인딩을 지원합니다. 이제 **-y** 옵션을 **clevis luks bind** 명령과 함께 사용하면 **yes** 를 사용하여 후속 프롬프트에 자동으로 답변할 수 있습니다. 예를 들어 Tang 쌍을 사용할 때 더 이상 Tang 키를 수동으로 신뢰할 필요가 없습니다.

(BZ#1819767)

fapolicyd 버전 1.0으로 업데이트

fapolicyd 패키지는 여러 버그 수정 및 개선 사항을 제공하는 버전 1.0으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 여러 스레드 동기화 문제가 해결되었습니다.
- 데이터베이스 크기 및 로드 시간 감소로 성능 향상.
- 신뢰 백엔드를 사용자 지정하기 위해 **fapolicyd.conf** 파일의 **fapolicyd** 패키지에 대한 새 **trust** 옵션이 추가되었습니다. 신뢰할 수 있는 모든 파일, 바이너리 및 스크립트를 새 **/etc/fapolicyd/fapolicyd.trust** 파일에 추가할 수 있습니다.
- CLI를 사용하여 **fapolicyd.trust** 파일을 관리할 수 있습니다.
- CLI를 사용하여 데이터베이스를 정리하거나 덤프할 수 있습니다.

- **fapolicyd** 패키지는 스크립트를 더 효과적으로 디코딩하기 위해 매직 데이터베이스를 재정의합니다. CLI는 재정의에 따라 `file` 명령과 유사한 파일의 MIME 유형을 출력합니다.
- **/etc/fapolicyd/fapolicyd.rules** 파일은 값 그룹을 특성 값으로 지원합니다.
- **fapolicyd** 데몬에는 **audit/sylog** 이벤트 형식을 설정하는 **syslog_format** 옵션이 있습니다.

(BZ#1817413)

fapolicyd는 이제 **fapolicyd -selinux**에 자체 SELinux 정책을 제공합니다.

이번 개선된 기능을 통해 **fapolicyd** 프레임워크에서 자체 SELinux 보안 정책을 제공합니다. 데몬은 **fapolicyd_t** 도메인 아래에 제한되며 정책은 **fapolicyd-selinux** 하위 패키지를 통해 설치됩니다.

(BZ#1714529)

usbguard는 버전 0.2.8로 업데이트

usbguard 패키지는 여러 버그 수정 및 개선 사항을 제공하는 버전 0.2.8로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- **/etc/usbguard/usbguard-daemon.conf** 파일의 **HidePII=true|false** 매개 변수는 이제 감사 항목에서 식별 가능한 정보를 숨길 수 있습니다.
- **/etc/usbguard/usbguard-daemon.conf** 파일의 **AuthorizedDefault=keep|none|all|internal** 매개 변수는 컨트롤러 장치의 권한 부여 상태를 미리 정의할 수 있습니다.
- 새로운 **with-connect-type** 규칙 속성을 사용하여 사용자는 이제 장치의 연결 유형을 구분할 수 있습니다.
- 사용자는 이제 **-t** 옵션을 사용하여 임시 규칙을 추가할 수 있습니다. 임시 규칙은 데몬이 다시 시작될 때까지 메모리에 유지됩니다.
- **usbguard list-rules**는 이제 특정 속성에 따라 규칙을 필터링할 수 있습니다.
- **usbguard generate-policy**에서 이제 특정 장치에 대한 정책을 생성할 수 있습니다.
- **usbguard allow|block|reject** 명령은 이제 규칙 문자열을 처리할 수 있으며 지정된 규칙 문자열과 일치하는 각 장치에 대상이 적용됩니다.
- 새 하위 패키지 **usbguard-notifier** 및 **usbguard-selinux**가 포함됩니다.

(BZ#1738590)

usbguard는 기업 데스크탑 사용자를 위해 많은 개선 사항을 제공합니다.

이 외에도 USBGuard 프로젝트에는 회사 데스크탑 사용자의 사용 편의성을 향상시키기 위한 개선 사항 및 버그 수정이 포함되어 있습니다. 중요한 변경 사항은 다음과 같습니다.

- **/etc/usbguard/rules.conf** 규칙 파일을 정리하기 위해 사용자는 **RuleFolder=/etc/usbguard/rules.d/** 디렉터리에 여러 구성 파일을 정의할 수 있습니다. 기본적으로 **RuleFolder**는 **/etc/usbguard-daemon.conf** 파일에 지정됩니다.
- **usbguard-notifier** 도구는 이제 GUI 알림을 제공합니다. 장치는 장치를 연결하거나 연결할 때마다 사용자에게 알리고 장치를 허용, 차단 또는 거부할 수 있는지 여부를 알립니다.
- **usbguard-daemon**에서 **#**로 시작하는 행을 구문 분석하지 않으므로 이제 구성 파일에 주석을 포함할 수 있습니다.

(BZ#1667395)

usbguard는 이제 **usbguard-selinux**에 자체 SELinux 정책을 제공합니다.

이 향상된 기능을 통해 **USBGuard** 프레임워크에서 자체 SELinux 보안 정책을 제공합니다. 데몬은 **usbguard_t** 도메인 아래에 제한되며 정책은 **usbguard-selinux** 하위 패키지를 통해 설치됩니다.

(BZ#1683567)

libcap 의 기능 지원

이번 업데이트를 통해 사용자는 로그인 시 주변 기능을 부여할 수 있으며 적절하게 구성된 프로세스에 대해 루트 액세스 권한이 없어도 방지할 수 있습니다.

(BZ#1487388)

libseccomp 라이브러리가 버전 2.4.3으로 업데이트되었습니다.

seccomp 시스템 호출 필터링 메커니즘에 인터페이스를 제공하는 **libseccomp** 라이브러리가 버전 2.4.3으로 업그레이드되었습니다.

이번 업데이트에서는 다양한 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- Linux v5.4-rc4의 **syscall** 테이블을 업데이트했습니다.
- 존재하지 않는 시스템 호출에 대한 **__NR_x** 값을 더 이상 정의하지 않습니다.
- **_SNR_x** 는 이제 내부적으로 사용됩니다.
- 추가된 **_SNR_ppoll** 을 정의합니다.
- s390/s390x shm* 시스템 호출에서 멀티플렉싱 문제를 해결했습니다.
- **libseccomp** 툴 컴파일에서 **static** 플래그를 제거했습니다.
- 추가 지원 for **io-uring** 관련 시스템 호출.
- v2.4.0 릴리스에 도입된 Python 모듈 이름 지정 문제를 수정했습니다. 모듈의 이름은 이전에 **seccomp** 로 지정됩니다.
- **scmp_bpf_sim** 툴에서 **clang** 으로 식별되는 잠재적인 메모리 누수를 수정했습니다.

(BZ#1770693)

omamqp1 모듈 지원

이번 업데이트를 통해 **AMQP 1.0** 프로토콜은 버스의 대상으로 메시지 전송을 지원합니다. 이전에는 Openstack에서 **AMQP1** 프로토콜을 통신 표준으로 사용했으며 이 프로토콜은 이제 AMQP 메시지에 메시지를 기록할 수 있습니다. 이번 업데이트에서는 메시지를 기록하고 버스의 대상으로 전송하는 **ma mqp1** 출력 모드를 제공하는 **rsyslog-mamqp1** 하위 패키지가 도입되었습니다.

(BZ#1713427)

OpenSCAP이 원격 콘텐츠 압축

이번 업데이트를 통해 OpenSCAP은 원격 콘텐츠를 전송하는 데 **gzip** 압축을 사용합니다. 가장 일반적인 원격 콘텐츠 유형은 텍스트 기반 CVE 피드로, 시간이 지남에 따라 크기가 증가하고 일반적으로 모든 스캔에 대해 다운로드해야 합니다. **gzip** 압축은 압축되지 않은 콘텐츠에 필요한 대역폭의 10%로 줄어듭니다.

결과적으로 스캔한 시스템과 원격 콘텐츠를 호스팅하는 서버 간에 전체 체인의 대역폭 요구 사항이 줄어 듭니다.

(BZ#1855708)

SCAP Security Guide는 이제 **NIST-800-171**과 일치하는 프로파일을 제공합니다.

이번 업데이트를 통해 **scap-security-guide** 패키지는 NIST-800-171 표준에 맞는 프로파일을 제공합니다. 프로파일을 사용하면 비유형 정보 시스템에서 CUI(Controlled Unclassified Information)를 보호하기 위한 보안 요구 사항에 따라 시스템 구성을 강화할 수 있습니다. 따라서 NIST-800-171 표준에 맞게 시스템을 보다 쉽게 구성할 수 있습니다.

(BZ#1762962)

5.1.7. 네트워킹

IPv4 및 IPv6 연결 추적 모듈이 the nf_conntrack 모듈에 병합되었습니다.

이번 개선된 기능은 the **nf_conntrack_ipv4** 및 **nf_conntrack_ipv6** Netfilter 연결 추적 모듈을 the **nf_conntrack**로 병합합니다. 이러한 변경으로 인해 주소 제품군별 모듈의 블랙리스트를 RHEL 8.3에서 더 이상 작동하지 않으며 the **nf_conntrack** 모듈만 블랙리스트하여 IPv4 및 IPv6 프로토콜에 대한 연결 추적 지원을 비활성화할 수 있습니다.

(BZ#1822085)

Firewalld가 버전로 업데이트 된 버전 지정.2

firewalld 패키지가 업스트림 버전 4.6.2로 업그레이드되어 이전 버전에 비해 여러 버그 수정이 제공됩니다. 자세한 내용은 [firewalld.2 릴리스 정보를 참조하십시오](#).

(BZ#1809636)

NetworkManager가 버전 1.26.0으로 업데이트

NetworkManager 패키지가 업스트림 버전 1.26.0으로 업그레이드되어 이전 버전에 비해 여러 개선 사항 및 버그 수정이 제공됩니다.

- NetworkManager는 장치 비활성화 시 자동 협상, 속도 및 이중화 설정을 원래 값으로 재설정합니다.
- 이전 활성화에 실패하면 Wi-Fi 프로파일 자동으로 연결됩니다. 즉, 초기 네트워크에 자동 연결하지 않으면 더 이상 자동 일치가 차단되지 않습니다. 부작용은 이전에 차단되었던 기존의 Wi-Fi 프로파일이 자동으로 연결된다는 것입니다.
- **nm-settings-nmcli(5)** 및 **nm-settings-dbus(5)** 도움말 페이지가 추가되었습니다.
- 여러 브리지 매개 변수에 대한 지원이 추가되었습니다.
- VRF(가상 라우팅 및 전달) 인터페이스에 대한 지원이 추가되었습니다. 자세한 내용은 [다양한 인터페이스에서 동일한 IP 주소를 영구적으로 재사용하는 것을 참조하십시오](#).
- Wi-Fi 네트워크에 대한 기회 OWE(가상화 모드) 지원이 추가되었습니다.
- NetworkManager는 [RFC 3021](#)에 따라 IPv4 포인트 투 포인트 링크에서 31비트 접두사를 지원합니다.
- **nmcli** 유틸리티는 **nmcli connection modify <connection_name> remove <setting>** 명령을 사용하여 설정을 제거하는 기능을 지원합니다.

- 마스터 장치가 누락된 경우 NetworkManager는 슬레이브 장치를 더 이상 생성하고 활성화하지 않습니다.

주요 변경 사항에 대한 자세한 내용은 업스트림 릴리스 노트를 참조하십시오.

- [NetworkManager 1.26.0](#)
- [NetworkManager 1.24.0](#)

(BZ#1814746)

XDP는 조건부 지원

Red Hat은 다음 모든 조건이 적용되는 경우에만 eXpress Data Path(XDP) 기능을 지원합니다.

- AMD 또는 Intel 64비트 아키텍처에서 XDP 프로그램을 로드합니다.
- **libxdp** 라이브러리를 사용하여 프로그램을 커널로 로드합니다.
- XDP 프로그램은 다음 반환 코드 중 하나를 사용합니다. **XDP_ABORTED**, **XDP_DROP** 또는 **XDP_PASS**
- XDP 프로그램은 XDP 하드웨어 오프로딩을 사용하지 않습니다

지원되지 않는 XDP 기능에 대한 자세한 내용은 [기술 프리뷰로 사용 가능한 XDP 기능 개요](#)를 참조하십시오.

(BZ#1889736)

XDP-tools 는 부분적으로 지원됨

커널 eXpress Data Path(XDP) 기능에 대한 사용자 공간 지원 유틸리티가 포함된 **xdp-tools** 패키지는 이제 AMD 및 Intel 64비트 아키텍처에서 지원됩니다. 여기에는 **libxdp** 라이브러리, XDP 프로그램 로드를 위한 **xdp-loader** 유틸리티, 패킷 필터링을 위한 **xdp-filter** 예제 프로그램이 포함됩니다. XDP가 활성화된 네트워크 인터페이스에서 패킷을 캡처하기 위한 **xdpdump** 유틸리티는 여전히 기술 프리뷰입니다.

(BZ#1820670)

기본적으로 **dracut** 유틸리티는 초기 RAM 디스크에서 NetworkManager를 사용합니다.

이전에는 **dracut** 유틸리티에서 쉘 스크립트를 사용하여 초기 RAM 디스크 **initrd**의 네트워킹을 관리했습니다. 이 경우 문제가 발생할 수 있습니다. 예를 들어 RAM 디스크의 스크립트가 IP 주소를 이미 요청했다 라도 NetworkManager는 다른 DHCP 요청을 전송하여 시간 초과가 발생할 수 있습니다.

이번 업데이트를 통해 기본적으로 **dracut**은 초기 RAM 디스크에서 NetworkManager를 사용하고 시스템이 문제가 발생하지 않도록 합니다. 이전 구현으로 다시 전환하고 RAM 디스크 이미지를 재생성하려면 다음 명령을 사용하십시오.

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

(BZ#1626348)

커널 명령줄의 네트워크 구성이 ip 매개변수 아래에 통합되었습니다

커널 명령줄에서 네트워크 구성을 설정하는 **ipv6**, **넷마스크**, **게이트웨이** 및 **호스트 이름** 매개 변수가 **ip** 매개 변수 아래에 통합되었습니다. **ip** 매개 변수는 다음과 같은 다양한 형식을 허용합니다.

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

이 매개변수에서 허용하는 개별 필드 및 기타 형식에 대한 자세한 내용은 **dracut.cmdline(7)** 도움말 페이지의 **ip** 매개변수 설명을 참조하십시오.

RHEL 8에서는 **ipv6**, **넷마스크**, **게이트웨이** 및 **호스트 이름** 매개 변수를 더 이상 사용할 수 없습니다.

(BZ#1905138)

5.1.8. 커널

RHEL 8.3의 커널 버전

Red Hat Enterprise Linux 8.3은 커널 버전 4.18.0-240과 함께 배포됩니다.

(BZ#1839151)

RHEL 8.3에 대한 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.

eBPF 바이트코드는 먼저 커널로 로드된 다음 확인, 실시간 컴파일만 사용하여 네이티브 시스템 코드로 코드 변환한 다음 가상 시스템에서 코드를 실행합니다.

Red Hat은 **eBPF** 가상 시스템을 활용하는 다양한 구성 요소를 제공합니다. 각 구성 요소는 다른 개발 단계에 있으므로 현재 모든 구성 요소가 완전히 지원되지는 않습니다. RHEL 8.3에서는 다음 **eBPF** 구성 요소가 지원됩니다.

- **eBPF**를 사용하여 Linux 운영 체제의 I/O 분석, 네트워킹 및 모니터링을 위한 툴을 제공하는 **BCC(BPF Compiler Collection)** 툴 패키지
- **BCC 라이브러리**는 **BCC** 툴 패키지에서 제공되는 툴과 유사한 툴을 개발할 수 있도록 합니다.
- 커널 네트워크 데이터 경로 내에서 프로그래밍 가능한 패킷 처리를 가능하게 하는 **tc(트래픽 제어)** 기능을 위한 **eBPF**입니다.
- 커널 네트워킹 스택이 처리하기 전에 수신된 패킷에 대한 액세스를 제공하는 **eXpress Data Path(XDP)** 기능은 특정 조건에서 지원됩니다. 자세한 내용은 Release Notes의 **네트워킹** 섹션을 참조하십시오.
- **libbpf** 패키지는 **bpf trace** 및 **bpf/xdp** 개발과 같은 **bpf** 관련 애플리케이션에 중요합니다. 자세한 내용은 전용 릴리스 노트 **libbpf**를 참조하십시오.
- **XDP** 기능에 대한 사용자 공간 지원 유틸리티가 포함된 **xdp-tools** 패키지는 이제 AMD 및 Intel 64 비트 아키텍처에서 지원됩니다. 여기에는 **libxdp** 라이브러리, XDP 프로그램 로드를 위한 **xdp-loader** 유틸리티, 패킷 필터링을 위한 **xdp-filter** 예제 프로그램이 포함됩니다. XDP가 활성화된 네트워크 인터페이스에서 패킷을 캡처하기 위한 **xdpdump** 유틸리티는 여전히 지원되지 않는 기술 프리뷰입니다. 자세한 내용은 릴리스 정보의 **네트워킹** 섹션을 참조하십시오.

특정 구성 요소가 지원되는 것으로 표시되지 않는 한 다른 **eBPF** 구성 요소는 기술 프리뷰로 사용할 수 있습니다.

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

- **bpftrace** 추적 언어
- 사용자 공간에 **eXpress Data Path(XDP)** 경로를 연결하는 **AF_XDP** 소켓

기술 프리뷰 구성 요소에 대한 자세한 내용은 [기술 프리뷰](#)를 참조하십시오.

(BZ#1780124)

Cornelis Networks -Path Architecture (OPA) 호스트 소프트웨어

Red Hat Enterprise Linux 8.3에서 OPA(OPA-Path Architecture) 호스트 소프트웨어가 완벽하게 지원됩니다. 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.

œ-Path Architecture 설치에 대한 자세한 내용은 [Intel®œ-Path Fabric Software](#) Release Notes 파일을 참조하십시오.

(BZ#1893174)

TSX 는 기본적으로 비활성화되어 있습니다

RHEL 8.3부터는 이제 OS 보안을 개선하기 위해 기본적으로 **Intel® TSX(Transactional Synchronization Extensions)** 기술이 비활성화되었습니다. 변경 사항은 **TSX** 비활성화를 지원하는 CPU에 적용됩니다. 여기에는 2세대 Intel® Xeon® Scalable Processors(이전 명칭: Intel® C620 시리즈가 포함된 Cascade Lake)가 포함됩니다.

애플리케이션이 **TSX** 를 사용하지 않는 사용자의 경우 변경 사항은 2차 Generation Intel® Xeon® Scalable Processors의 **TSX** 비동기 중단(TAA) 완화의 기본 성능 저하를 제거합니다.

또한 변경 사항은 Linux 5.4 이후 **TSX** 가 기본적으로 비활성화된 업스트림과 RHEL 커널 동작을 조정합니다.

TSX 를 활성화하려면 **tsx=on** 매개 변수를 커널 명령줄에 추가합니다.

(BZ#1828642)

RHEL 8.3에서 페이지 소유자 추적 기능을 지원

이번 업데이트를 통해 페이지 소유자 추적 기능을 사용하여 페이지 할당 수준에서 커널 메모리 사용량을 관찰할 수 있습니다.

페이지 추적기를 활성화하려면 다음 단계를 실행하십시오.

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

결과적으로 페이지 소유자 추적기가 커널 메모리 사용량을 추적하여 커널 메모리 누수를 디버그하고 많은 메모리를 사용하는 드라이버를 탐지하는 데 도움이 됩니다.

(BZ#1825414)

AMD EPYC™ 7003 시리즈 프로세서용 EDAC 지원

이번 개선된 기능으로 AMD EPYC™ 7003 시리즈 프로세서에 대한 오류 감지 및 수정(EDAC) 장치 지원을 제공합니다. 이전에는 AMD EPYC™ 7003 시리즈 프로세서를 기반으로 하는 시스템에서 수정(CE) 및 수정되지 않은(UE) 메모리 오류가 보고되지 않았었습니다. 이번 업데이트를 통해 이제 EDAC를 사용하여 이러한 오류가 보고됩니다.

(BZ#1735611)

perf 툴로 샘플그래픽 지원

이번 업데이트를 통해 **perf** 명령줄 툴에서 화살표를 지원하여 시스템 성능을 그래픽으로 표시합니다. **perf** 데이터는 유사한 스택 역추적이 있는 샘플로 그룹화됩니다. 결과적으로 이 데이터는 계산으로 많이 사용되는 코드 영역을 보다 쉽게 식별할 수 있도록 시각적 표현으로 변환됩니다. **perf** 툴을 사용하여 표시를 생성하려면 다음 명령을 실행합니다.

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

참고: 표시기를 생성하려면 **js-d3-flame-graph** rpm을 설치합니다.

(BZ#1281843)

/dev/random 및 **/dev/urandom** 은 Kernel API DRBG에 의해 조건부로 구동됩니다.

FIPS 모드에서 **/dev/random** 및 **/dev/urandom** 의사 임의 번호 생성기는 DRBG(커널 API 결정 임의 비트 생성기)를 통해 구동됩니다. FIPS 모드의 애플리케이션은 언급된 장치를 FIPS 호환 잡음 소스로 사용하여 장치는 FIPS 승인 알고리즘을 사용해야 합니다. 이 목표를 달성하기 위해 **/dev/random** 드라이버에 필요한 후크가 추가되었습니다. 결과적으로 후크가 FIPS 모드에서 활성화되고 **/dev/random** 및 **/dev/urandom** 이 Kernel API DRBG에 연결됩니다.

(BZ#1785660)

libbpf 가 완전히 지원됨

bpf trace 및 **bpf/xdp** 개발과 같은 **bpf** 관련 애플리케이션에 중요한 **libbpf** 패키지가 이제 완전히 지원됩니다.

bpf-next linux 트리 **bpf-next/tools/lib/bpf** 디렉토리 및 지원 헤더 파일의 미러입니다. 패키지의 버전은 ABI(Application Binary Interface) 버전을 반영합니다.

(BZ#1759154)

lshw 유틸리티에서 추가 CPU 정보 제공

이번 개선된 기능을 통해 **lshw**(List Hardware utility)에 더 많은 CPU 정보가 표시됩니다. CPU 버전 필드에는 이제 **<family>.<model>.<stepping>** 버전의 숫자 형식으로 시스템 프로세서의 제품군, 모델 및 스텝핑 세부 정보를 제공합니다.

(BZ#1794049)

kernel-rt 소스 트리가 RHEL 8.3 트리로 업데이트되었습니다.

최신 Red Hat Enterprise Linux 커널 소스 트리를 사용하도록 **kernel-rt** 소스가 업데이트되었습니다. 실시간 패치 세트도 최신 업스트림 버전 v5.6.14-rt7로 업데이트되었습니다. 이 두 업데이트 모두 여러 버그 수정 및 개선 사항을 제공합니다.

(BZ#1818138, BZ#1818142)

tpm2-tools 가 버전 4.1.1로 업데이트

tpm2-tools 패키지가 버전 4.1.1으로 업그레이드되어 많은 명령 추가, 업데이트 및 제거를 제공합니다. 자세한 내용은 [RHEL8.3 솔루션의 업데이트에서 tpm2-tools 패키지를 참조하십시오](#).

(BZ#1789682)

Mellanox ConnectX-6 Dx 네트워크 어댑터가 완전히 지원됩니다.

이번 개선된 기능에는 Mellanox ConnectX-6 Dx 네트워크 어댑터의 PCI ID가 **mlx5_core** 드라이버에 추가됩니다. 이 어댑터를 사용하는 호스트에서 RHEL은 **mlx5_core** 드라이버를 자동으로 로드합니다. 이전에 기술 프리뷰로 사용할 수 있는 이 기능은 이제 RHEL 8.3에서 완전히 지원됩니다.

(BZ#1782831)

mlxsw 드라이버가 버전 5.7로 업데이트

mlxsw 드라이버가 업스트림 버전 5.7로 업그레이드되고 다음과 같은 새 기능이 포함되어 있습니다.

- 버퍼 점유 데이터를 제공하는 공유 버퍼 occupancy 기능입니다.
- 계층 2, 계층 3, 터널 및 액세스 제어 목록 드롭을 모니터링할 수 있는 패킷 드롭 기능.
- 패킷 트랩 구매자 지원.
- LLDP(링크 계층 검색 프로토콜) 에이전트를 사용한 기본 포트 우선 순위 구성 지원.
- ETS(Transmission Selection) 및 TBF(Token 버킷 필터) 대기열 처리 지원.
- 초기에 패킷이 손실되지 않도록 대기열 규제 **nodrop** 모드가 활성화됩니다.
- 트래픽 클래스 SKB 편집 작업 **skbedit** 우선 순위 기능을 사용하면 패킷 메타데이터를 변경하고 **pedit** Traffic Class Offloading(TOS)으로 보완됩니다.

(BZ#1821646)

crash 커널이 kdump에 대한 메모리 예약 확장

이번 개선된 기능을 통해 **crashkernel=auto** 인수는 이제 4GB ~ 64GB 메모리 용량의 머신에 더 많은 메모리를 예약합니다. 이전 버전에서는 메모리 예약이 제한되어 크래시 커널이 커널 공간 및 사용자 공간 메모리가 확장됨에 따라 크래시 덤프를 캡처하지 못했습니다. 그 결과 크래시 커널에 OOM(메모리 부족) 오류가 발생했습니다. 이번 업데이트에서는 설명된 시나리오에서 OOM 오류 발생을 줄이고 그에 따라 **kdump**의 메모리 용량을 확장할 수 있습니다.

(BZ#1746644)

5.1.9. 파일 시스템 및 스토리지

LVM에서 VDO 볼륨을 관리할 수 있음

LVM에서 VDO(가상 데이터 최적화 도구) 세그먼트 유형을 지원합니다. 결과적으로 LVM 유틸리티를 사용하여 VDO 볼륨을 기본 LVM 논리 볼륨으로 만들고 관리할 수 있습니다.

VDO는 인라인 블록 수준 중복 제거, 압축 및 썬 프로비저닝 기능을 제공합니다.

자세한 내용은 [RHEL에서 논리 볼륨 복제 및 압축을 참조하십시오](#).

(BZ#1598199)

SCSI 스택이 고성능 어댑터에서 더 잘 작동합니다.

SCSI 스택의 성능이 향상되었습니다. 결과적으로 차세대 고성능 HBA(호스트 버스 어댑터)가 RHEL에서 더 높은 IOPS(초당 I/O)를 사용할 수 있습니다.

(BZ#1761928)

megaraid_sas 드라이버가 최신 버전으로 업데이트되었습니다

megaraid_sas 드라이버가 버전 07.713.01.00-rc1로 업데이트되었습니다. 이번 업데이트에서는 성능 향상, 지원 대상 어댑터의 안정성 향상, 더욱 풍부한 기능 세트와 관련된 여러 버그 수정 및 개선 사항을 제공합니다.

(BZ#1791041)

Stratis에서 오류가 발생한 풀 이름을 나열합니다.

기존 Stratis 풀에서 이미 사용 중인 블록 장치에 Stratis 풀을 생성하려고 하면 **stratis** 유틸리티에서 기존 풀의 이름을 보고합니다. 이전에는 유틸리티가 풀의 UUID 레이블만 나열했습니다.

(BZ#1734496)

FPIN ELS 프레임 알림 지원

lpfc Fibre Channel(FC) 드라이버는 이제 링크 수준 문제를 식별하고 스위치가 보다 안정적인 경로를 선택할 수 있도록 링크 무결성에 관한 Fabric Performance Impact Notifications(PASSWORDINs)을 지원합니다.

(BZ#1796565)

LVM on-disk 메타데이터를 디버깅하기 위한 새로운 명령

lvm2 패키지에서 사용할 수 있는 **pvck** 유틸리티는 이제 물리 볼륨의 LVM on-disk 메타데이터를 디버그하거나 복구하는 하위 수준의 명령을 제공합니다.

- 메타데이터를 추출하려면 **pvck --dump** 명령을 사용합니다.
- 메타데이터를 복구하려면 **pvck --repair** 명령을 사용합니다.

자세한 내용은 **pvck(8)** 도움말 페이지를 참조하십시오.

(BZ#1541165)

LVM RAID는 장치에서 손상된 데이터로 인해 데이터 손실을 방지하기 위해 DM 무결성 지원

이제 데이터가 손실되지 않도록 LVM RAID 구성에 장치 매핑(DM) 무결성을 추가할 수 있습니다. 무결성 계층은 장치에서 데이터 손상을 감지하고 RAID 계층을 경고하여 LVM RAID에서 손상된 데이터를 수정합니다.

RAID는 장치 오류로 인한 데이터 손실을 방지하지만 LVM RAID 어레이에 무결성을 추가하면 장치의 손상된 데이터로 인해 데이터가 손실되지 않습니다. 새 LVM RAID를 생성할 때 무결성 계층을 추가하거나 이미 존재하는 LVM RAID에 추가할 수 있습니다.

(JIRA:RHELPLAN-39320)

AWS, Azure 및 Aliyun 공용 클라우드에서 지원되는 탄력적 스토리지 (GFS2)

탄력적 스토리지(GFS2)는 이제 공유 블록 장치 지원을 도입하여 AWS(Amazon), Microsoft(Azure) 및 보중(Aliyun)의 세 가지 주요 퍼블릭 클라우드에서 지원됩니다. 그 결과 GFS2는 이제 온프레미스와 퍼블릭 클라우드에서 모두 사용할 수 있는 옵션이 있는 진정한 하이브리드 클라우드 클러스터 파일 시스템이 되었습니다. Microsoft Azure 및 AWS에서 공유 블록 스토리지를 구성하는 방법에 대한 자세한 내용은 [공용](#)

클라우드 플랫폼에 Red Hat Enterprise Linux 8 배포를 참조하십시오. 슬롯 클라우드에서 공유 블록 스토리지 구성 방법에 대한 자세한 내용은 프리뷰 클라우드에서 Red Hat High Availability Cluster용 공유 블록 스토리지 구성을 참조하십시오.

(BZ#1900019)

사용자 공간에서 최신 **nfsdclld** 데몬 지원

이제 userspace는 네임스페이스 인식 클라이언트 추적 방법인 latest **nfsdclld** 데몬을 지원합니다. 이 향상된 기능을 통해 데이터 손상 없이 클라이언트가 컨테이너화된 **knfsd** 데몬에서 클라이언트 열기 또는 잠금 복구를 수행할 수 있습니다.

(BZ#1817756)

nconnect 에서 여러 동시 연결을 지원

이 향상된 기능을 사용하면 **nconnect** 기능을 사용하여 NFS 서버에 대한 여러 동시 연결을 만들어 다른 로드 밸런싱 기능을 사용할 수 있습니다. **nconnect =X NFS 마운트 옵션을 사용하여 nconnect** 기능을 활성화합니다. 여기서 X는 사용할 동시 연결 수입니다. 현재 제한은 16입니다.

(BZ#1683394, BZ#1761352)

클라이언트 정보 추적을 위한 **nfsdclld** 데몬 지원

이번 개선된 기능을 통해 **nfsdclld** 데몬은 이제 안정적인 스토리지에 대한 클라이언트별 정보를 추적하는 기본 방법입니다. 결과적으로 컨테이너에서 실행 중인 NFS v4를 사용하면 서버를 다시 시작한 후 클라이언트가 열기 또는 잠금을 회수할 수 있습니다.

(BZ#1817752)

5.1.10. 고가용성 및 클러스터

Pacemaker 가 버전 2.0.4로 업데이트

Pacemaker 클러스터 리소스 관리자가 여러 버그 수정 사항을 제공하는 업스트림 버전 2.0.4로 업그레이드되었습니다.

(BZ#1828488)

새로운 **priority-fencing-delay** 클러스터 속성

Pacemaker에서 새 **priority-fencing-delay** 클러스터 속성을 지원하므로, split-brain 상황에서 노드가 펜싱되는 노드라고 할 수 있도록 2-노드 클러스터를 구성할 수 있습니다.

priority-fencing-delay 속성은 기간으로 설정할 수 있습니다. 이 속성의 기본값은 0(비활성화됨)입니다. 이 속성이 0이 아닌 값으로 설정되고 meta-attribute **우선 순위**가 하나 이상의 리소스에 대해 구성된 경우 split-brain 상황에서 모든 리소스가 실행되는 모든 리소스의 조합 우선 순위가 가장 높은 노드가 생존할 가능성이 높습니다.

예를 들어 pcs **resource defaults priority=1** 및 pcs 속성 세트 **priority-fencing-delay=15s** 를 설정하고 다른 우선순위가 설정되지 않은 경우 대부분의 리소스를 실행하는 노드는 펜싱을 시작하기 전에 15초 동안 대기하므로 대부분의 리소스를 실행하는 노드가 생존할 가능성이 높습니다. 특정 리소스가 나머지보다 중요한 경우 우선 순위를 높일 수 있습니다.

해당 복제본에 대해 우선 순위가 구성된 경우 promotable 복제의 마스터 역할을 실행하는 노드에는 추가 1 포인트가 부여됩니다.

priority-fencing-delay 로 설정된 지연은 pcmk_delay_ **base** 및 pcmk_delay_ **max** 펜스 장치 속성에서

지연에 추가됩니다. 이 동작을 사용하면 두 노드 모두 우선 순위가 같거나 노드 손실 이외의 이유로 두 노드를 모두 펜싱해야 합니다(예: 리소스 모니터 작업에 대해 **on-fail=fencing** 은 설정됨). 조합으로 사용하는 경우 우선순위-펜싱-delay 속성을 **pcmk_delay_base** 및 **pcmk_delay_max** 에서 최대 지연보다 훨씬 큰 값으로 설정하여 우선순위가 지정된 노드를 선호하는지 확인하는 것이 좋습니다(값이 완전히 안전합니다).

(BZ#1784601)

여러 리소스 및 작업 기본값을 관리하기 위한 새로운 명령

이제 여러 리소스 및 작업 기본값을 생성, 나열, 변경 및 삭제할 수 있습니다. 기본값 세트를 생성할 때 리소스 및 **op** 표현식이 포함된 규칙을 지정할 수 있습니다. 예를 들어 특정 유형의 모든 리소스에 대한 기본 리소스 값을 구성할 수 있습니다. 기존 기본값을 나열하는 명령에는 이제 출력에 여러 개의 기본값 세트가 포함됩니다.

- **pcs resource [op] defaults set create** 명령을 실행하면 새 기본값 세트를 생성합니다. 이 명령을 사용하여 규칙을 지정할 때 **및**, **및** 괄호를 포함한 리소스 및 **op** 표현식만 허용됩니다.
- **pcs resource [op] defaults set delete | remove** 명령은 기본값 세트를 제거합니다.
- **pcs resource [op] defaults set update** 명령은 세트의 기본값을 변경합니다.

(BZ#1817547)

클러스터 리소스 태그 지정 지원

이제 **pcs tag** 명령을 사용하여 **Pacemaker** 클러스터의 클러스터 리소스에 태그를 지정할 수 있습니다. 이 기능을 사용하면 단일 명령으로 지정된 리소스 세트를 관리할 수 있습니다. **pcs tag** 명령을 사용하여 리소스 태그를 제거하거나 수정하고 태그 구성을 표시할 수도 있습니다.

pcs resource enable, **pcs resource disable**, **pcs resource manage**, **pcs resource manage**, **pcs resource unmanage** 명령은 태그 ID를 인수로 수락합니다.

(BZ#1684676)

Pacemaker에서 완전히 중지하지 않고 승격된 리소스를 시연하여 복구 지원

이제 승격 또는 모니터 작업이 해당 리소스에 실패하거나 리소스가 실행 중인 파티션이 쿼럼을 손실하도록 **Pacemaker** 클러스터에서 승격 가능한 리소스를 구성할 수 있지만 완전히 중지되지 않습니다.

이 기능은 승격되지 않은 모드에서 리소스를 계속 사용할 수 있도록 하려는 경우에 유용할 수 있습니다. 예를 들어 데이터베이스 마스터 파티션의 파티션이 쿼럼을 손실하는 경우 데이터베이스 리소스가

Master 역할을 손실하는 것을 선호할 수 있지만 읽기 전용 모드에만 활성 상태로 유지되므로 읽기 전용 모드만 있으면 손실된 쿼럼에도 불구하고 읽기 전용 애플리케이션이 계속 작동할 수 있습니다. 이 기능은 성공적인 **demote**가 복구에 충분하고 전체 재시작보다 훨씬 빠른 경우 유용할 수 있습니다.

이 기능을 지원하려면 다음을 수행합니다.

- 이제 **on-fail** 작업 **meta-attribute**에서 다음 예와 같이 승격 작업에 사용할 때 **demote** 값을 허용합니다.

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

- 이제 **on-fail** 작업 메타 기여자가 다음 예와 같이 간격이 0이 아닌 값과 역할로 설정된 **monitor** 작업과 함께 사용할 때 **demote** 값을 허용합니다.

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

- **no-quorum-policy** 클러스터 속성에서 **demote** 값을 허용합니다. 설정된 경우 클러스터 파티션이 쿼럼을 유실하면 승격된 리소스가 강등되지만 실행 중으로 남아 있으며 다른 모든 리소스가 중지됩니다.

작업에 대한 **demote meta-attribute**를 지정하면 리소스 승격이 결정되는 방식에는 영향을 미치지 않습니다. 영향을 받는 노드에 여전히 승격 점수가 가장 높은 경우 다시 승격되도록 선택합니다.

(BZ#1837747, [BZ#1843079](#))

Pacemaker와의 동기화를 개선하기 위한 새로운 **SBD_SYNC_RESOURCE_STARTUP** SBD 구성 매개 변수

SBD와 **Pacemaker** 간의 동기화를 보다 효과적으로 제어하기 위해 **/etc/sysconfig/sbd** 파일에서 **SBD_SYNC_RESOURCE_STARTUP** 매개 변수를 지원합니다. **RHEL 8.3** 이상의 **Pacemaker** 및 **SBD** 패키지가 설치되고 **SBD**가 **SBD_SYNC_RESOURCE_STARTUP=true**로 구성된 경우 **SBD**는 데몬 상태에 대한 정보를 받기 위해 **Pacemaker** 데몬에 연결합니다.

이 구성에서는 **Pacemaker** 데몬이 **SBD**에서 연결할 때까지 기다립니다. 이 두 데몬은 하위 데몬을 시작하기 전에 그리고 최종 종료 전에 기다립니다. 결과적으로 **SBD**에서 적극적으로 통신할 수 없는 경우 **Pacemaker**에서 리소스를 실행하지 않으며 정상 종료로 **SBD**에 보고될 때까지 **Pacemaker**에서 종료하지 않습니다. 이로 인해 **SBD**에서 **Pacemaker**의 연결을 끊기 전에 리소스가 실행되지 않는 경우 **SBD**에서 정상 종료 중에 발생할 수 있는 예기치 않은 상황이 발생하여 불필요한 재부팅이 트리거됩니다. 정의된 핸드셰이크를 사용하여 정상 종료를 감지하면 유지 관리 모드에서도 작동합니다. 종료 시 리소스를 실행하

지 않으므로 실행 중인 리소스가 남아 있지 않은 상태에서 정상 종료를 감지하는 이전 방법은 유지 관리 모드에서 비활성화해야 합니다.

또한 이 기능을 활성화하면 **SBD**와 **Pacemaker**가 성공적으로 시작될 때 클러스터에서 분리 장애 (**split-brain**) 상황이 발생하지 않지만 **SBD**가 **pacemaker**에 연결할 수 없습니다. 예를 들어 **SELinux** 정책으로 인해 발생할 수 있습니다. 이 경우 **Pacemaker**는 **SBD**가 작동하지 않을 때 작동한다고 가정합니다. 이 새 기능을 활성화하면 **SBD**에 연결할 때까지 **Pacemaker**가 시작을 완료하지 않습니다. 이 새로운 기능의 또 다른 장점은 **SBD**가 활성화된 경우 하트비트를 사용하여 **Pacemaker**에 반복적으로 접속하고 **Pacemaker**가 언제든지 응답하지 않는 경우 노드를 패닉할 수 있다는 것입니다.



참고

`/etc/sysconfig/sbd` 파일을 편집했거나 **PCS**를 통해 **SBD**를 구성한 경우 **RPM** 업데이트를 새 **SBD_SYNC_RESOURCE_STARTUP** 매개 변수로 가져오지 않습니다. 이 경우 이 기능을 구현하려면 `/etc/sysconfig/sbd.rpmnew` 파일에서 수동으로 추가하거나 **sbd(8)** 도움말 페이지의 환경 섹션을 통해 구성에 설명된 절차를 따라야 합니다.

([BZ#1718324](#), [BZ#1743726](#))

5.1.11. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

새 모듈 스트림: **ruby:2.7**

RHEL 8.3에서는 **Ruby 2.7.1**을 새로운 **ruby:2.7** 모듈 스트림에 도입했습니다. 이 버전은 **RHEL 8.1**에서 배포한 **Ruby 2.6**에 비해 다양한 성능 개선, 버그 및 보안 수정, 새로운 기능을 제공합니다.

주요 개선 사항은 다음과 같습니다.

- 새로운 **GC(Garbage Collector)**가 도입되었습니다. 이 **GC**는 조각화된 메모리 공간을 조각 모음할 수 있습니다.
- **Ruby** 아직 **another Compiler-Compiler (✓cc)**는 이제 일대화 **Look-Ahead Left-to-Right - LALR(1)** - 파서 생성기에 대한 명령줄 인터페이스를 제공합니다.
- **REPL(Read-Eval-Print Loop)** 환경에 번들로 제공되는 대화형 **Ruby Shell(irb)**이 이제 여러 줄 편집을 지원합니다.

- 기능적 프로그래밍 언어에서 자주 사용되는 패턴 일치는 실험적인 기능으로 도입되었습니다.
- 기본 **block** 매개 변수로 번호가 매겨진 매개 변수가 실험적 기능으로 도입되었습니다.

다음과 같은 성능 개선이 구현되었습니다.

- 파이버 생성을 가속화하도록 파이버 캐시 전략이 변경되었습니다.
- **CGI.escapeHTML** 방법의 성능이 향상되었습니다.
- **Monitor** 클래스 및 **Monitor Mic** 모듈의 성능이 향상되었습니다.

또한 키워드 인수와 위치 인수의 자동 변환은 더 이상 사용되지 않습니다. **Ruby 3.0**에서는 위치 인수 및 키워드 인수가 구분됩니다. 자세한 내용은 [업스트림 문서를 참조하십시오](#).

실험적 기능에 대한 경고를 표시하지 않으려면 **-W:no-experimental** 명령줄 옵션을 사용합니다. 중단 경고를 비활성화하려면 **-W:no-deprecated** 명령줄 옵션을 사용하거나 **Warning[:deprecated] = false** 를 코드에 추가합니다.

ruby:2.7 모듈 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install ruby:2.7
```

ruby:2.6 스트림에서 업그레이드하려면 [이후 스트림으로 전환](#)을 참조하십시오.

(BZ#1817135)

새 모듈 스트림: **nodejs:14**

새 모듈 스트림 **nodejs:14** 를 사용할 수 있습니다. **RHEL 8.3**에 포함된 **Node.js 14** 는 **RHEL 8.1**에서 배포된 **Node.js 12** 에 비해 여러 가지 새로운 기능 및 버그 및 보안 수정 사항을 제공합니다.

주요 변경 사항은 다음과 같습니다.

- V8 엔진이 버전 **8.3**으로 업그레이드되었습니다.
- 새로운 실험적 **WebAssembly System Interface(WASI)**가 구현되었습니다.
- 새로운 실험적 **Async** 로컬 스토리지 **API**가 도입되었습니다.
- 이제 진단 보고서 기능이 안정적입니다.
- 스트림 **API**가 강화되었습니다.
- 실험적 모듈 경고가 제거되었습니다.

[RHEA-2020:5101](#) 권고가 릴리스되면서 **RHEL 8**에서는 **Node.js 14.15.0** 을 제공합니다. 이 버전은 안정성이 개선된 최신 **LTS(Long Term Support)** 버전입니다.

nodejs:14 모듈 스트림을 설치하려면 다음을 사용합니다.

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

nodejs:12 스트림에서 업그레이드하려면 **Switching** 을 [이후 스트림으로](#) 참조하십시오.

([BZ#1815402](#), [BZ#1891809](#))

Git 기반 버전 2.27

git 패키지가 업스트림 버전 **2.27**로 업그레이드되었습니다. 이전에 사용 가능한 버전 **2.18**에 대한 주요 변경 사항은 다음과 같습니다.

- **git checkout** 명령은 다음 두 가지 명령으로 나뉩니다.

- 분기 관리를 위한 **Git** 스위치
- 디렉터리 트리 내에서 변경 사항을 관리하기 위한 **Git** 복원
- **git rebase** 명령의 동작은 기본적으로 이전 **patch+apply** 워크플로우가 아닌 병합 워크플로를 기반으로 합니다. 이전 동작을 보존하려면 **rebase.backend** 구성 변수를 적용 하도록 설정합니다.
- 이제 **git difftool** 명령을 리포지토리 외부에서도 사용할 수 있습니다.
- 보다 구체적인 사례에서 새로운 구성 변수 **{author,committer} .{name,email}** 이(를) 재정의 하도록 도입되었습니다.
- 사용자가 프록시와의 통신을 위해 **SSL**을 구성할 수 있는 몇 가지 새로운 옵션이 추가되었습니다.
- **git fast-export** 및 **git fast-import** 유틸리티에서 **UTF-8** 이외의 문자 인코딩에서 로그 메시지로 커밋 처리가 개선되었습니다.
- **lfs** 확장 기능이 새 **git-lfs** 패키지로 추가되었습니다. **LFS(GIT Large File Storage)**는 큰 파일을 **Git** 내의 텍스트 포인터로 대체하고 원격 서버에 파일 내용을 저장합니다.

([BZ#1825114](#), [BZ#1783391](#))

Python변경 사항

RHEL 8.3에서는 **python38:3.8** 모듈 스트림에 다음과 같은 변경 사항이 추가되었습니다.

- **Python** 인터프리터가 버전 **3.8.3**으로 업데이트되어 여러 버그 수정을 제공합니다.
- **python38-pip** 패키지가 버전 **19.3.1**로 업데이트되었으며 **pip**는 **manylinux2014**의 설치를 지원합니다.

python3 패키지에서 제공하는 **Python 3.6** 인터프리터의 성능이 크게 향상되었습니다.

ubi8/python-27, **ubi8/python-36** 및 **ubi8/python-38** 컨테이너 이미지는 고객이 제공하는 경우 사용자 정의 패키지 인덱스 또는 **PyPI** 미러에서 **pipenv** 유틸리티 설치를 지원합니다. 이전에는 업스트림 **PyPI** 리포지토리에서만 **pipenv** 를 다운로드할 수 있었으며 업스트림 리포지토리를 사용할 수 없는 경우 설치에 실패했습니다.

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

새 모듈 스트림: **php:7.4**

RHEL 8.3에는 **7.3** 버전에 비해 많은 버그 수정 및 개선 사항을 제공하는 **PHP 7.4** 가 도입되었습니다.

이 릴리스에는 새로운 실험적 확장 기능 인터페이스(**FFI**)를 도입하여 네이티브 함수를 호출하고 네이티브 변수에 액세스하며 **C** 라이브러리에 정의된 데이터 구조를 생성 및 액세스할 수 있습니다. **FFI** 확장 기능은 **php-ffi** 패키지에서 사용할 수 있습니다.

다음의 확장 기능이 제거되었습니다.

- **php-xml** 패키지에서 제거된 **wddx** 확장 기능
- **recode** 확장 기능이 **php-recode** 패키지에서 제거됩니다.

php:7.4 모듈 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install php:7.4
```

php:7.3 스트림에서 업그레이드하려면 [이후 스트림으로 전환](#)을 참조하십시오.

RHEL 8의 **PHP** 사용법에 대한 자세한 내용은 [PHP 스크립팅 언어](#) 사용을 참조하십시오.

([BZ#1797661](#))

새 모듈 스트림: nginx:1.18

버전 1.16에 대한 여러 버그 수정, 보안 수정, 새로운 기능 및 개선 사항을 제공하는 **nginx 1.18** 웹 및 프록시 서버를 사용할 수 있습니다. 주요 변경 사항은 다음과 같습니다.

- HTTP 요청 속도 및 연결 제한에 대한 개선 사항이 구현되었습니다. 예를 들어, **limit_rate** 및 **limit_rate_after** 지시문은 이제 새로운 **\$limit_req_status** 및 **\$limit_conn_status** 변수를 포함하여 변수를 지원합니다. 또한 **limit_conn_dry_run** 및 **limit_req_dry_run** 지시문에 대해 시험 실행 모드가 추가되었습니다.
- 권한 없는 요청을 지연된 처리할 수 있는 새로운 **auth_delay** 지시문이 추가되었습니다.
- 이제 **grpc_pass**, **proxy_upload_rate** 및 **proxy_download_rate** 의 변수를 지원합니다.
- 추가 **PROXY** 프로토콜 변수(예: **\$proxy_protocol_server_addr** 및 **\$proxy_protocol_server_port**)가 추가되었습니다.

nginx:1.18 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install nginx:1.18
```

nginx:1.16 스트림에서 업그레이드하려면 [이후 스트림으로 전환](#)을 참조하십시오.

([BZ#1826632](#))

새 모듈 스트림: perl:5.30

RHEL 8.3에는 이전에 출시된 **Perl 5.26**에 비해 많은 버그 수정 및 개선 사항을 제공하는 **Perl 5.30** 이 도입되었습니다. 또한 새 버전은 특정 언어 기능을 더 이상 사용하지 않거나 제거합니다. 심각한 영향을 미치는 주요 변경 사항은 다음과 같습니다.

- **The Math::BigInt::CalcEmu, arybase, and B::Debug modules have been removed**
- **close-on-exec** 플래그를 사용하여 파일 설명자를 엽니다

- 동일한 기호를 파일로 열 수 있으며 디렉토리 처리로 열 수 없습니다.
- 서브루틴 속성이 서브루틴 서명 앞에 있어야 합니다
- **:locked** 및 **:uniq** 속성이 제거되었습니다.
- 형식이 쉽표가 없는 변수 목록은 더 이상 허용되지 않습니다
- 베이 메탈 **here -document** 연산자는 더 이상 허용되지 않습니다.
- 정규 표현식 패턴에서 이스케이프되지 않은 왼쪽 중괄호 (**{**) 문자의 이전에 사용되지 않는 특정 사용은 더 이상 허용되지 않습니다.
- 더 이상 메서드 가 아닌 함수로 상속될 수 없습니다.
- **sort pragma**에서 더 이상 정렬 알고리즘을 지정할 수 없습니다
- **B::OP::terse()** 서브루틴이 **B::Concise::b_terse()** 서브루틴으로 교체되었습니다.
- **File::Glob::glob()** 함수가 **File::Glob::bsd_glob()** 함수로 교체되었습니다.
- 이제 **dump()** 함수를 **CORE::dump()**로 정규화해야 합니다.
- **yada-yada** 연산자 (...)는 이제 문이므로 식으로 사용할 수 없습니다.
- 0이 아닌 값을 **\$[** 변수에 할당하면 치명적인 오류가 반환됩니다.
- **\$*** 및 **\$#** 변수는 더 이상 허용되지 않습니다.

- **false** 조건 분기에서 **my()** 함수를 사용하여 변수를 선언하는 것은 더 이상 허용되지 않습니다.
- **:utf8** 핸들에서 **sysread()** 및 **syswrite()** 함수를 사용하면 치명적인 오류가 반환됩니다.
- **pack()** 함수는 더 이상 잘못된 형식의 **UTF-8** 형식을 반환하지 않습니다
- **IV_MAX** 보다 큰 값을 갖는 유니코드 코드 포인트는 더 이상 허용되지 않습니다.
- 유니코드 12.1이 지원됨

이전 perl 모듈 스트림에서 업그레이드하려면 [이후 스트림으로 전환](#)을 참조하십시오.

Perl 5.30 은 s2i 지원 ubi8/perl-530 컨테이너 이미지로도 사용할 수 있습니다.

([BZ#1713592](#), [BZ#1732828](#))

새 모듈 스트림: **perl-libwww-perl:6.34**

RHEL 8.3에는 RHEL 8에서 사용 가능한 모든 버전의 **perl-libwww-perl** 패키지를 제공하는 새로운 **perl-libwww-perl:6.34** 모듈 스트림이 도입되었습니다. 5.26 이외의 Perl 스트림에서는 사용할 수 없는 RHEL 8.0 이후부터 사용할 수 없는 모듈식 **perl-libwww-perl** 패키지가 새로운 기본 **perl-libwww-perl:6.34** 스트림에서 더 이상 사용되지 않습니다.

([BZ#1781177](#))

새 모듈 스트림: **perl-IO-Socket-SSL:2.066**

이제 새로운 **perl-IO-Socket-SSL:2.066** 모듈 스트림을 사용할 수 있습니다. 이 모듈은 **perl-IO-Socket-SSL** 및 **perl-Net-SSLeay** 패키지를 제공하며 RHEL 8에서 사용할 수 있는 모든 Perl 스트림과 호환됩니다.

([BZ#1824222](#))

squid:4 모듈 스트림이 버전 **4.11**로 재정의

squid:4 모듈 스트림에서 제공하는 **Squid** 프록시 서버가 **4.4**에서 버전 **4.11**로 업그레이드되었습니다. 이 릴리스는 여러 버그 및 보안 수정 사항과 새로운 구성 옵션과 같은 다양한 개선 사항을 제공합니다.

([BZ#1829467](#))

httpd:2.4 모듈 스트림의 변경 사항

RHEL 8.3에는 **httpd:2.4** 모듈 스트림을 통해 사용할 수 있는 **Apache HTTP Server**에 다음과 같은 주요 변경 사항이 도입되었습니다.

- **mod_http2** 모듈이 **1.15.7**로 다시 기반
- **H2Upgrade** 및 **H2 Push** 지시문의 구성 변경
- **HTTP/2** 페이로드 프레임의 패딩을 제어하는 새로운 **H2Padding** 구성 지시문
- 수많은 버그 픽스.

([BZ#1814236](#))

httpd의 **CustomLog** 지시문에서 **to journald** 로깅 지원

이제 **CustomLog** 지시문에 새 옵션을 사용하여 **Apache HTTP** 서버에서 액세스(전송) 로그를 출력할 수 있습니다.

지원되는 구문은 다음과 같습니다.

```
CustomLog journald:priority format|nickname
```

여기서 **priority**는 [LogLevel 지시문에서](#) 사용되는 대로 디버깅 하기 위한 우선 순위 문자열입니다.

예를 들어 결합된 로그 형식을 사용하여 **to journald** 를 기록하려면 다음을 사용합니다.

```
CustomLog journald:info combined
```

이 옵션을 사용하는 경우 플랫폼 파일에 직접 로깅할 때 서버 성능이 서버 성능이 낮을 수 있습니다.

([BZ#1209162](#))

5.1.12. 컴파일러 및 개발 도구

RHEL에서 .NET 5 사용 가능

.NET 5는 Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8 및 OpenShift Container Platform에서 사용할 수 있습니다. **.NET 5**에는 다음과 같은 새로운 언어 버전이 포함되어 있습니다. **C# 9** 및 **F# 5.0**. 기본 라이브러리 **GC** 및 **JIT**에서 상당한 성능 향상이 이루어졌습니다. **.NET 5**에는 단일 파일 애플리케이션이 있어 **.NET** 애플리케이션을 단일 실행 파일로 배포할 수 있으며 모든 종속성이 포함되어 있습니다. **.NET 5**용 **UBI8** 이미지는 Red Hat 컨테이너 레지스트리에서 사용할 수 있으며 **OpenShift**와 함께 사용할 수 있습니다.

.NET 5를 사용하려면 **dotnet-sdk-5.0** 패키지를 설치합니다.

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

자세한 내용은 [.NET 5 문서를 참조하십시오](#).

([BZ#1944677](#))

새로운 GCC 툴 세트 10

GCC Toolset 10은 최신 버전의 개발 툴을 제공하는 컴파일러 툴셋입니다. **AppStream** 리포지토리의 소프트웨어 컬렉션 형태로 애플리케이션 스트림으로 사용할 수 있습니다.

GCC 컴파일러가 버전 **10.2.1**로 업데이트되어 업스트림 **GCC**에서 사용할 수 있는 많은 버그 수정 및 개선 사항을 제공합니다.

다음 도구와 버전은 **GCC Toolset 10**에서 제공합니다.

툴	버전
GCC	10.2.1
GDB	9.2
valgrind	3.16.0
SystemTap	4.3
Dyninst	10.1.0
binutils	2.35
elfutils	0.180
dwz	0.12
Make	4.2.1
strace	5.7
ltrace	0.7.91
annobin	9.29

GCC Toolset 10을 설치하려면 **root**로 다음 명령을 실행합니다.

```
# yum install gcc-toolset-10
```

GCC Toolset 10에서 도구를 실행하려면 다음을 수행합니다.

```
$ scl enable gcc-toolset-10 tool/
```

셸 세션을 실행하려면 **GCC Toolset 10**의 툴 버전이 이러한 툴의 시스템 버전을 재정의합니다.

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

자세한 내용은 [GCC Toolset 사용](#)을 참조하십시오.

GCC Toolset 10 구성 요소는 다음 두 개의 컨테이너 이미지에서 사용할 수 있습니다.

- **rhel8/gcc-toolset-10-toolchain**에는 **GCC** 컴파일러, **GDB** 디버거 및 **make** 자동화 도구가 포함됩니다.
- **rhel8/gcc-toolset-10-perftools**: **SystemTap** 및 **Valgrind**와 같은 성능 모니터링 툴이 포함되어 있습니다.

컨테이너 이미지를 가져오려면 다음 명령을 **root**로 실행합니다.

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

GCC Toolset 10 컨테이너 이미지만 지원됩니다. 이전 **GCC** 도구 세트 버전의 컨테이너 이미지는 더 이상 사용되지 않습니다.

컨테이너 이미지에 대한 자세한 내용은 [GCC Toolset 컨테이너 이미지 사용](#)을 참조하십시오.

(BZ#1842656)

jboss Toolset을 버전 **1.45.2**로 업데이트

capsule Toolset이 **1.45.2** 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 종속성을 보기 위한 하위 명령 트리 가 이제 종료되어 있습니다.
- 부동 소수점 값에서 정수로 바꿉니다. 이전 버전에서는 잘린 부동 소수점 값이 대상 정수 유형의 범위를 벗어나면 결과적으로 컴파일러가 정의되지 않았습니. 불일치값이 없기 때문에 정의되지 않은 동작도 발생했습니다. 이번 개선된 기능을 통해 제한된 값은 최소 또는 정수의 최대 범위 중 하나입니다. 양의 정수 및 음수의 정수는 기본적으로 최대 및 최소 정수, 즉 **Not-a-Number(NaN)** 값을 **0**으로 표시합니다.
- 이제 식, 패턴, 문 등의 절차 매크로가 확장되고 안정화되었습니다.

사용법에 대한 자세한 지침은 사용 설명서 [를 참조하십시오](#).

(BZ#1820593)

LLVM Toolset을 버전 10.0.1로 업데이트

LLVM Toolset이 버전 10.0.1로 업그레이드되었습니다. 이번 업데이트를 통해 **clang-libs** 패키지에 더 이상 개별 구성 요소 라이브러리가 포함되지 않습니다. 따라서 애플리케이션을 더 이상 연결할 수 없습니다. **clang** 라이브러리와 애플리케이션을 연결하려면 **libclang-cpp.so** 패키지를 사용합니다.

자세한 내용은 [LLVM Toolset 사용](#)을 참조하십시오.

(BZ#1820587)

Go Toolset을 버전 1.14.7로 업데이트

Go Toolset이 버전 1.14.7로 업그레이드되었습니다. 주목할 만한 변경 사항은 다음과 같습니다.

- 이제 Go 모듈 시스템이 완전히 지원됩니다.
- SSLv3(SSL 버전 3.0)은 더 이상 지원되지 않습니다. 주요 Delve 디버거 개선 사항은 다음과 같습니다.
- 원시 메모리를 검사하기 위한 새 명령 **examinemem** (또는 **x**)
- 프로그램의 각 중지 중 식의 값을 인쇄하기 위한 새로운 명령 표시
- 디버그된 프로그램에 대한 Teletypewriter(TTY)를 제공하는 새로운 **--tty** 플래그
- Arm64에 대한 새로운 **coredump** 지원
- goroutine 라벨을 인쇄하는 새로운 기능
- DAP(디버그 어댑터 프로토콜) 서버 릴리스

•

dlv 추적 및 추적 **REPL (read-eval-print-loop)** 명령의 향상된 출력

Go Toolset에 대한 자세한 내용은 [Go Toolset](#) 사용을 참조하십시오.

Delve에 대한 자세한 내용은 업스트림 [Delve](#) 문서를 참조하십시오.

(BZ#1820596)

SystemTap 버전 4.3으로 업데이트

SystemTap 계측 툴이 버전 4.3으로 업데이트되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

•

사용자 공간 프로브는 **readelf -n**에서 16진수 빌드를 대상으로 지정할 수 있습니다. 경로 이름에 대한 이 대안을 사용하면 임의의 이름으로 일치하는 바이너리를 검색할 수 있으므로 단일 스크립트가 다양한 버전을 대상으로 할 수 있습니다. 이 기능은 **elfutils debuginfod** 서버와 함께 잘 작동합니다.

•

스크립트 기능은 프로브 **\$context** 변수를 사용하여 프로브 위치의 변수에 액세스할 수 있으므로 **SystemTap** 스크립트가 일반적인 논리를 사용하여 다양한 프로브에서 작업할 수 있습니다.

•

try-catch 문 및 오류 프로브를 포함하여 **stapbpf** 프로그램이 개선되어 **BPF** 백엔드에서 실행되는 스크립트에서 적절한 오류 허용 오차가 활성화되었습니다.

주요 변경 사항에 대한 자세한 내용은 업데이트하기 전에 [업스트림 릴리스 노트](#)를 참조하십시오.

(BZ#1804319)

Valgrind를 버전 3.16.0으로 업데이트

Valgrind 실행 가능 코드 분석 도구가 버전 3.16.0으로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

•

이제 **Valgrind gdbserver**에 연결된 **gdb**를 통해 또는 프로그램 클라이언트 요청을 통해

Valgrind: `vgdb` 에서 실행되는 동안 여러 명령줄 옵션의 값을 동적으로 변경할 수 있습니다. 동적으로 변경할 수 있는 옵션 목록을 가져오려면 `valgrind --help-dyn-options` 명령을 실행합니다.

- **Cachegrind**(`cg_annotate`) 및 **Callgrind**(`callgrind_annotate`) 툴의 경우 `--auto` 및 `--show-percs` 옵션이 기본값인 `yes` 가 되었습니다.
- **Memcheck** 툴은 최적화된 코드에서 오탐(false positive) 오류를 줄입니다. 특히 **Memcheck** 는 컴파일러가 `A && B` 검사를 `B && A` 로 변환 했을 때 `B`를 정의하지 않을 수 있고 `A` 가 거짓인 경우 케이스를 더 잘 처리합니다. **Memcheck**는 부분적으로 정의된 값에서 정수 증가 확인 및 비고급 검사를 더 효율적으로 처리합니다.
- 실험적 스택 및 글로벌 어레이 검사 도구(`exp-sgcheck`)가 제거되었습니다. 스택 및 글로벌 어레이 오버런을 감지하기 위한 대안은 **GCC**의 **AAN(AddressSanitizer)** 기능을 사용하는 것으로, `-fsanitize=address` 옵션으로 코드를 다시 빌드해야 합니다.

([BZ#1804324](#))

elfutils 를 버전 0.180으로 다시 기반

elfutils 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 0.180으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- **GCC LTO**(링크 시간 최적화)로 빌드된 코드 디버그 정보에 대한 향상된 지원. **eu-readelf** 및 **libdw** 유틸리티는 이제 `.gnu.debuglto_` 섹션을 읽고 처리할 수 있으며 **CU**(컴파일 단위)에 정의된 함수의 파일 이름을 올바르게 확인합니다.
- 이제 **eu-nm** 유틸리티가 약한 객체를 **V** 로, 공통 기호를 **C** 로 명시적으로 식별합니다.
- **The debuginfod** 서버는 이제 `index.deb` 아카이브를 사용할 수 있으며 `-Z EXT[=CMD]` 옵션을 사용하여 다른 패키지 아카이브 형식을 추가할 수 있는 일반 확장명이 있습니다. 예를 들어 `-Z '.tar.zst=zstdcat'` 은 `.tar.zst` 확장자로 끝나는 아카이브를 `zstdcat` 유틸리티를 사용하여 압축 해제해야 함을 나타냅니다.
- **The debuginfo-client** 도구에는 `debuginfo_d_set_user_data`, `debuginfod_get_user_data`, `debuginfod_get_url` 및 `debuginfo_d_add_http_header` 와 같은 몇 가지 새로운 도우미 함수가 있습니다. 또한 `file:// URL`도 지원합니다.

(BZ#1804321)

GDB에서 IBM z15에서 프로세스 레코드 및 재생 지원

이 향상된 기능을 통해 **GDB(GNU Debugger)**가 이제 프로세스 레코드를 지원하고 **IBM z15** 프로세서 (이전의 **arch13**)의 새 명령 대부분을 사용하여 재생합니다. 다음 지침은 현재 지원되지 않습니다. **SORTL**(서열 목록), **DFLTCC**(차별 변환 호출), **KDSA**(계산 디지털 서명 인증).

(BZ#1659535)

papi에서 **satellitel ThunderX2** 성능 모니터링 이벤트가 업데이트되었습니다.

이번 개선된 기능을 통해 **uncore** 이벤트를 포함하여 **ThunderX2**와 관련된 여러 성능 이벤트가 업데이트되었습니다. 그 결과 개발자는 **brl ThunderX2** 시스템에서 시스템 성능을 더 잘 조사할 수 있습니다.

(BZ#1726070)

glibc math 라이브러리가 **IBM Z**에 최적화되었습니다.

이 향상된 기능을 통해 **IBM Z** 시스템의 성능을 향상시키기 위해 **libm** 수학 기능이 최적화되었습니다. 주요 변경 사항은 다음과 같습니다.

- 영향력 있는 부동 소수점 제어 레지스터 세트 및 추출 방지를 위해 향상된 라운딩 모드 처리
- **z196** 정수와 플로트 간의 변환 사용

(BZ#1780204)

추가 **libffi** 특정 임시 디렉터리를 사용할 수 있습니다.

이전에는 강화된 시스템에서 시스템 전체 임시 디렉터리에 **libffi** 라이브러리에 사용하기에 적합한 권한이 없을 수 있었습니다.

이 향상된 기능을 통해 시스템 관리자는 이제 **write** 및 **exec** 마운트 또는 **selinux** 권한이 있는 **libffi** 관련 임시 디렉터리를 가리키도록 **LIBFFI_TMPDIR** 환경 변수를 설정할 수 있습니다.

(BZ#1723951)**strstr() 및 strcasestr() 의 성능 개선**

이번 업데이트를 통해 지원되는 여러 아키텍처에서 **strstr()** 및 **strcasestr()** 함수의 성능이 향상되었습니다. 결과적으로 사용자는 문자열 및 메모리 조작 루틴을 사용하여 모든 애플리케이션의 훨씬 더 나은 성능을 활용할 수 있습니다.

(BZ#1821531)

glibc 에서 잘린 로케일 아카이브 로드를 올바르게 처리합니다.

업그레이드 중 정전 또는 디스크 장애로 인해 시스템 로케일의 아카이브가 이전에 잘린 경우 아카이브를 로드할 때 프로세스가 예기치 않게 종료될 수 있었습니다. 이번 개선된 기능으로 로케일 아카이브 로드 시 일관성 검사가 추가되었습니다. 결과적으로 프로세스는 아카이브 잘림을 감지하고 아카이브가 아닌 로케일 또는 기본 **POSIX** 로케일로 대체할 수 있습니다.

(BZ#1784525)**GDB에서 Debuginfo d지원**

이 향상된 기능을 통해 이제 **elfutils debuginfod** 클라이언트 라이브러리를 사용하여 **GDB(GNU Debugger)**에서 중앙 집중식 서버에서 디버그 정보 패키지를 다운로드할 수 있습니다.

(BZ#1838777)**PCP 기반 버전 5.1.1-3**

pcp 패키지가 버전 **5.1.1-3**으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 모든 **PCP** 서비스에 대해 업데이트된 서비스 단위 및 향상된 **systemd** 통합 및 신뢰성. 아카이브 로그 순환이 향상되고 시의적절한 압축이 향상되었습니다. **pmproxy** 프로토콜의 아카이브 검색 버그 수정.
- **pmrep** 및 내보내기 도구에서 메트릭 레이블을 보고하는 기능과 함께 **pcp-atop**, **pcp-dstat**, **pmrep** 및 관련 모니터 툴이 향상되었습니다.
-

향상된 **bpfftrace**, **OpenMetrics**, **MMV**, **Linux** 커널 에이전트 및 기타 컬렉션 에이전트. **Open vSwitch** 및 **RabbitMQ** 서버의 새 지표 수집기.

- 독립 실행형 **pm mgr** 데몬을 대체하는 새로운 호스트 검색 **pm find systemd** 서비스.

([BZ#1792971](#))

Grafana 가 6.7.3 버전으로 업데이트

grafana 패키지가 6.7.3 버전으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 일반 **OAuth** 역할 매핑 지원
- 새 로그 패널
- 테이블 패널에서 여러 줄 텍스트 표시
- 새로운 통화 및 에너지 단위

([BZ#1807323](#))

Grafana-pcp 버전 2.0.2로 업데이트

grafana-pcp 패키지가 버전 2.0.2로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 표시에 표시할 다차원 **eBPF** 맵을 지원합니다.
- 쿼리 편집기에서 자동 완성 캐시를 제거하여 **PCP** 지표를 동적으로 표시할 수 있습니다.

([BZ#1807099](#))

새 **rhel8/pcp** 컨테이너 이미지

이제 **Red Hat Container Registry**에서 **rhel8/pcp** 컨테이너 이미지를 사용할 수 있습니다. 이미지에 사전 설치된 **pcp-zeroconf** 패키지와 **OpenMetrics PMDA**가 포함된 **PCP(Performance Co- Pilot)** 툴킷이 포함되어 있습니다.

(BZ#1497296)

새로운 **rhel8/grafana** 컨테이너 이미지

이제 **Red Hat Container Registry**에서 **rhel8/grafana** 컨테이너 이미지를 사용할 수 있습니다. **Grafana**는 지표 대시보드가 있는 오픈소스 유틸리티이며 **Graphite, Elasticsearch , OpenTSDB, Prometheus, InfluxDB** 및 **PCP** 모니터링 툴용 그래프 편집기입니다.

(BZ#1823834)

5.1.13. IdM (Identity Management)

IdM 백업 유틸리티에서 필요한 복제본 역할을 확인합니다.

이제 **ipa-backup** 유틸리티에서 **IdM** 클러스터에서 사용되는 모든 서비스(예: **CA**(인증 기관), **DNS(Domain Name System)** 및 **KRA(Key Recovery Agent)**)가 백업을 실행 중인 복제본에 설치되어 있는지 확인합니다. 복제본에 이러한 서비스가 모두 설치되어 있지 않으면 **ipa-backup** 유틸리티가 경고와 함께 종료됩니다. 해당 호스트에서 수행한 백업은 전체 클러스터 복원에 충분하지 않기 때문입니다.

예를 들어 **IdM** 배포에서 통합 **CA**(인증 기관)를 사용하는 경우 비**CA** 복제본에서 실행되는 백업은 **CA** 데이터를 캡처하지 않습니다. **Red Hat**은 **ipa-backup** 을 수행하는 복제본에 클러스터에 사용된 모든 **IdM** 서비스가 설치되어 있는지 확인하는 것이 좋습니다.

자세한 내용은 [IdM 백업으로 데이터 손실 준비를 참조하십시오](#).

(BZ#1810154)

새 암호 만료 알림 도구

ipa-client-epn 패키지에서 제공하는 암호 알림(**EPN**) 만료는 암호가 곧 만료되는 **IdM(Identity Management)** 사용자 목록을 빌드하는 데 사용할 수 있는 독립 실행형 도구입니다.

IdM 관리자는 **EPN**을 사용하여 다음을 수행할 수 있습니다.

- 영향을 받는 사용자 목록을 **JSON** 형식으로 표시(런타임 시 계산)
- 지정된 날짜 또는 날짜 범위에 대해 전송할 이메일 수를 계산
- 암호 만료 이메일 알림 전송

Red Hat은 포함된 **ipa-epn.timer systemd** 타이머를 사용하여 **IdM** 클라이언트 또는 복제본에서 매일 **EPN**을 시작할 것을 권장합니다.

(BZ#913799)

JSS에서 **FIPS** 호환 **SSLContext** 제공

이전에는 **Tomcat**에서 **JCA(Java Cryptography Architecture)** **SSLContext** 클래스의 **SSLEngine** 지시문을 사용했습니다. 기본 **SunJSSE** 구현은 **FIPS(Federal Information Processing Standard)**와 호환되지 않으므로 **PKI**는 이제 **JSS**를 통해 **FIPS** 호환 구현을 제공합니다.

(BZ#1821851)

공개 키 인프라의 전반적인 상태를 확인할 수 있습니다

이번 업데이트를 통해 **PKI(공개 키 인프라)** 상태 점검 툴에서 **PKI** 하위 시스템의 상태를 **RHEL 8.1**에서 도입한 **IdM(Identity Management)** **Healthcheck** 툴에 보고합니다. **IdM Healthcheck**를 실행하면 **PKI** 하위 시스템의 상태 보고서를 수집하고 반환하는 **PKI Healthcheck**가 호출됩니다.

pki-healthcheck 툴은 배포된 **RHEL IdM** 서버 또는 복제본에서 사용할 수 있습니다. **pki-healthcheck** 에서 제공하는 모든 검사도 **ipa-healthcheck** 툴에 통합됩니다. **ipa-healthcheck** 는 **idm:DL1** 모듈 스트림과 별도로 설치할 수 있습니다.

pki-healthcheck 는 독립 실행형 **RHCS(Red Hat Certificate System)** 인프라에서도 작동할 수 있습니다.

(BZ#1770322)

RSA PSS 지원

이 향상된 기능을 통해 PKI는 이제 RSA PSS(Probabilistic Signature Scheme) 서명 알고리즘을 지원합니다.

이 기능을 활성화하려면 지정된 하위 시스템에 대한 `pkispawn` 스크립트 파일에서 다음 행을 설정하십시오. `pki_use_pss_rsa_signing_algorithm=True`

결과적으로 이 하위 시스템의 기존의 모든 기본 서명 알고리즘(`PS .cfg` 구성 파일에서 지정됨)은 해당 PSS 버전을 사용합니다. 예를 들어 `SHA256withRSA` 는 `SHA256withRSA/PSS`가 됩니다.

(BZ#1824948)

Directory Server는 서비스가 시작될 때 개인 키 및 인증서를 개인 네임 스페이스로 내보냅니다.

Directory Server는 복제 계약과 같이 나가는 연결에 OpenLDAP 라이브러리를 사용합니다. 이러한 라이브러리는 NSS(네트워크 보안 서비스) 데이터베이스에 직접 액세스할 수 없으므로 Directory Server는 TLS 암호화가 지원되는 인스턴스에서 NSS 데이터베이스에서 개인 키 및 인증서를 추출하여 OpenLDAP 라이브러리에서 암호화된 연결을 설정할 수 있습니다. 이전 버전에서는 Directory Server에서 `cn=config` 항목의 `nsslapd-certdir` 매개 변수에 설정된 디렉터리로 개인 키 및 인증서를 추출했습니다(기본값: `/etc/dirsrv/slapd-<instance_name>/`). 결과적으로 Directory Server는 `Server-Cert-Key.pem` 및 `Server-Cert.pem` 을 이 디렉터리에 저장했습니다. 이 향상된 기능을 통해 Directory Server는 `/tmp/` 디렉터리에 `systemd` 가 마운트하는 개인 네임스페이스로 개인 키와 인증서를 추출합니다. 그 결과 보안이 향상되었습니다.

(BZ#1638875)

디스크 모니터링 임계값에 도달하면 Directory Server에서 인스턴스를 읽기 전용 모드로 전환할 수 있습니다.

이번 업데이트에서는 `nsslapd-disk-monitoring-readonly-on-threshold` 매개 변수를 `cn=config` 항목에 추가합니다. 이 설정을 활성화하면 디스크 모니터링이 활성화되고 사용 가능한 디스크 공간이 `nsslapd-disk-monitoring-threshold` 에서 구성한 값보다 낮은 경우 Directory Server는 모든 데이터베이스를 읽기 전용으로 전환합니다. `nsslapd-disk-monitoring-readonly-on-threshold` 를 `on` 으로 설정하여 Directory Server가 인스턴스를 종료할 때까지 데이터베이스를 수정할 수 없습니다. 이렇게 하면 데이터 손상을 방지할 수 있습니다.

(BZ#1728943)

Samba 가 버전 4.12.3으로 업데이트

`samba` 패키지가 업스트림 버전 4.12.3으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선

사항을 제공합니다.

- 기본 제공 암호화 기능은 **GnuTLS** 함수로 교체되었습니다. 이렇게 하면 서버 메시지 블록 버전 **3(SMB3)** 성능이 향상되고 복사 속도가 크게 향상됩니다.
- 이제 최소 런타임 지원이 **Python 3.5**입니다.
- 이전 쓰기 캐시 개념이 메모리 제한 시스템의 성능을 줄일 수 있기 때문에 쓰기 캐시 크기 매개 변수가 제거되었습니다.
- **DES** 암호화 유형의 **Kerberos** 티켓을 사용한 연결 인증 지원이 제거되었습니다.
- **vfs_netatalk VFS**(가상 파일 시스템) 모듈이 제거되었습니다.
- **ldap ssl ad** 매개 변수는 더 이상 사용되지 않는 것으로 표시되며 향후 **Samba** 버전에서 제거됩니다. **LDAP** 트래픽을 다른 방법으로 암호화하고 자세한 내용은 [samba: "ldap ssl ad" smb.conf 옵션](#) 솔루션 제거를 참조하십시오.
- 기본적으로 **RHEL 8.3**의 **Samba**는 더 이상 사용되지 않는 **RC4** 암호화 제품군을 지원하지 않습니다. **Kerberos** 인증에 계속 **RC4**가 필요한 도메인 구성원으로 **Samba**를 실행하는 경우 **update-crypto-policies --set DEFAULT:AD-SUPPORT** 명령을 사용하여 **RC4** 암호화 유형을 지원합니다.

smbd, nmbd 또는 **winbind** 서비스가 시작될 때 **Samba**는 **tdb** 데이터베이스 파일을 자동으로 업데이트합니다. **Samba**를 시작하기 전에 데이터베이스 파일을 백업합니다. **Red Hat**은 **tdb** 데이터베이스 파일 다운그레이드를 지원하지 않습니다.

주요 변경 사항에 대한 자세한 내용은 업데이트하기 전에 [업스트림 릴리스 노트](#)를 참조하십시오.

([BZ#1817557](#))

Cockpit-session-recording을 버전 4로 다시 기반

cockpit-session-recording 모듈은 버전 4로 다시 기반되었습니다. 이 버전은 이전 버전에서 다음과 같은 주요 변경 사항을 제공합니다.

- **metainfo** 파일에서 업데이트된 상위 ID입니다.
- 업데이트된 패키지 매니페스트.
- CentOS7에서 올바른 경로를 확인하기 위해 **rpmmacro** 수정.
- 바이트 배열 인코딩 저널 데이터 처리.
- 더 이상 사용되지 않는 **React** 라이프사이클 함수에서 코드를 이동했습니다.

([BZ#1826516](#))

krb5 를 버전 1.18.2로 업데이트

krb5 패키지가 업스트림 버전 **1.18.2**로 업그레이드되었습니다. 주요 수정 사항 및 개선 사항은 다음과 같습니다.

- 단일 및 **Triple-DES** 암호화 유형이 제거되었습니다.
- 초안 9 PKINIT는 지원되는 **Active Directory** 버전에는 필요하지 않으므로 제거되었습니다.
- **NegoEx** 메커니즘 플러그인이 이제 지원됩니다.
- 호스트 이름 **Canonicalization** 대체가 지원됩니다(**dns_canonicalize_hostname** = 대체).

([BZ#1802334](#))

IdM에서 새로운 Ansible 관리 모듈 지원

이번 업데이트에서는 **Ansible** 플레이북을 사용하여 공통 **IdM(Identity Management)** 작업을 자동화하기 위한 몇 가지 **ansible-freeipa** 모듈이 도입되었습니다.

- **config** 모듈을 사용하면 **IdM** 내에서 글로벌 구성 매개 변수를 설정할 수 있습니다.
- **dnsconfig** 모듈을 사용하면 글로벌 **DNS** 구성을 수정할 수 있습니다.
- **dnsforwardzone** 모듈을 사용하면 **IdM**에서 **DNS** 전달자를 추가하고 제거할 수 있습니다.
- **dnsrecord** 를 사용하면 **DNS** 레코드를 관리할 수 있습니다. 업스트림 **ipa_dnsrecord** 와 달리, 한 실행에서 여러 레코드 관리를 허용하고 더 많은 레코드 유형을 지원합니다.
- **dnszone** 모듈을 사용하면 **DNS** 서버에서 영역을 구성할 수 있습니다.
- **service** 모듈을 사용하면 서비스가 있는지 여부와 서비스가 있는지 확인할 수 있습니다.
- **vault** 모듈을 사용하면 자격 증명 모음 및 자격 증명 모음의 멤버가 있는지 확인할 수 있습니다.

ipagroup 및 **ipa hostgroup** 모듈은 사용자 및 호스트 그룹 멤버십 관리자를 각각 포함하도록 확장되었습니다. 그룹 멤버십 관리자는 그룹에 구성원을 추가하거나 그룹에서 멤버를 제거할 수 있는 사용자 또는 그룹입니다. 자세한 내용은 해당 **/usr/share/doc/ansible-freeipa/README-*** 파일의 **Variables** 섹션을 참조하십시오.

(JIRA:RHELPLAN-49954)

IdM에서 인증서 관리를 위한 새로운 **Ansible** 시스템 역할 지원

IdM(Identity Management)은 인증서 관리 작업을 자동화하는 새로운 **Ansible** 시스템 역할을 지원합니다. 새 역할에는 다음과 같은 이점이 포함됩니다.

- 역할은 인증서 발급 및 갱신을 자동화하는 데 도움이 됩니다.
- **ipa** 인증 기관에서 인증서를 발급하도록 역할을 구성할 수 있습니다. 이러한 방식으로 기존 **IdM** 인프라를 사용하여 인증서 신뢰 체인을 관리할 수 있습니다.

- 역할을 사용하면 인증서를 실행 전후에 실행할 명령을 지정할 수 있습니다(예: 서비스 중지 및 시작).

(JIRA:RHELPLAN-50002)

Identity Management에서 FIPS 지원

이 향상된 기능을 통해 이제 **IdM(Identity Management)**의 인증 메커니즘과 함께 **FIPS(Federal Information Processing Standard)**에서 승인한 암호화 유형을 사용할 수 있습니다. **IdM**과 **Active Directory** 간의 교차 **Pod** 신뢰는 **FIPS**와 호환되지 않습니다.

FIPS가 필요하지만 **AD** 신뢰가 필요하지 않은 고객은 이제 **FIPS** 모드에 **IdM**을 설치할 수 있습니다.

(JIRA:RHELPLAN-43531)

idm :DL1 에서 **OpenDNSSEC** 버전이 **2.1**로 업데이트되었습니다.

idm:DL1 모듈 스트림의 **OpenDNSSEC** 구성 요소는 현재 장기 업스트림 지원 버전인 **2.1** 버전 시리즈로 업그레이드되었습니다. **OpenDNSSEC**는 인터넷 보안을 한층 강화하기 위해 **DNSSEC(Domain Name System Security Extensions)**를 채택하는 오픈 소스 프로젝트입니다. **OpenDNSSEC 2.1**은 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 자세한 내용은 업스트림 릴리스 노트를 참조하십시오. <https://www.opendnssec.org/archive/releases/>

(JIRA:RHELPLAN-48838)

IdM에서 더 이상 사용되지 않는 **RC4** 암호화 제품군과 새로운 시스템 전체 암호화 하위 정책 지원

이번 업데이트에서는 **IdM(Identity Management)**의 **RC4(Rivest Cipher 4)** 암호화 제품군을 활성화하는 새로운 **AD-SUPPORT** 암호화 하위 정책이 도입되었습니다.

AD(Advanced Encryption Standard)를 사용하도록 **AD(Advanced Encryption Standard)**를 사용하도록 구성되지 않은 경우 **AD(IdM-Active Directory)**의 컨텍스트에서 관리자가 새 **AD-SUPPORT** 하위 정책을 활성화할 수 있습니다. 보다 구체적으로 다음 조건 중 하나가 적용되는 경우 새 하위 정책을 활성화하는 것이 좋습니다.

- **AD**의 사용자 또는 서비스 계정에는 **RC4** 암호화 키가 있으며 **AES** 암호화 키가 없습니다.

•

개별 **Active Directory** 도메인 간 신뢰 링크에는 **RC4** 암호화 키가 있으며 **AES** 암호화 키가 없습니다.

DEFAULT 암호화 정책 외에도 **AD-SUPPORT** 하위 정책을 활성화하려면 다음을 입력합니다.

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

또는 **AD** 포레스트에서 **AD** 도메인 간 신뢰성을 업그레이드하여 강력한 **AES** 암호화 유형을 지원하려면 다음 **Microsoft** 문서를 참조하십시오. [AD DS: 보안: 신뢰할 수 있는 도메인의 리소스에 액세스할 때 Kerberos "지원되지 않은 etype" 오류.](#)

(BZ#1851139)

새로운 **Microsoft LDAP** 채널 바인딩 및 **LDAP** 서명 요구 사항에 맞게 조정

최근 **Microsoft** 업데이트를 통해 **AD(Active Directory)**는 **LDAP** 채널 바인딩 및 **LDAP** 서명에 기본 **Windows** 설정을 사용하지 않는 클라이언트에 플래그를 지정합니다. 결과적으로 **AD**와의 직접 또는 간접 통합에 **SSSD(System Security Services Daemon)**를 사용하는 **RHEL** 시스템은 **GSSAPI(Generic Security Services Application Program Interface)**를 사용하는 성공적인 **SASL(Simple Authentication and Security Layer)** 작업 시 **AD**에서 오류 이벤트 ID를 트리거할 수 있습니다.

이러한 알림을 방지하기 위해 **GSSAPI** 대신 **GSS-SPNEGO(Simple and Protected GSSAPI Negotiation Mechanism)** **SASL** 메커니즘을 사용하도록 클라이언트 애플리케이션을 구성합니다. **SSSD**를 구성하려면 **ldap_sasl_mech** 옵션을 **GSS-SPNEGO**로 설정합니다.

또한 채널 바인딩이 **AD**측에 적용되는 경우 다음과 같은 방식으로 **SSL/TLS**와 **SASL**을 사용하는 시스템을 구성합니다.

1.

RHEL 8.3 이상과 함께 제공되는 **Cyrus-sasl,openldap** 및 **krb5-libs** 패키지의 최신 버전을 설치합니다.

2.

/etc/openldap/ldap.conf 파일에서 **SASL_CBINDING** 옵션을 **tls-endpoint**로 설정하여 올바른 채널 바인딩 유형을 지정합니다.

자세한 내용은 **Microsoft** 보안 권고 [ADV190023 | LDAP 채널 바인딩 및 RHEL 및 AD 통합에 LDAP 서명](#)을 참조하십시오.

([BZ#1873567](#))

SSSD, **adcli** 및 **realmd**는 더 이상 사용되지 않는 **RC4** 암호화 제품군과 새로운 시스템 전체 암호화 하위 정책을 지원합니다.

이번 업데이트에서는 다음 유틸리티에 **Rivest Cipher 4 (RC4)** 암호화 제품군을 활성화하는 새로운 **AD-SUPPORT** 암호화 하위 정책이 도입되었습니다.

- **SSSD**(시스템 보안 서비스 데몬)
- **adcli**
- **realmd**

다음 시나리오에서 **AD(Active Directory)**가 **AES(Advanced Encryption Standard)**를 사용하도록 구성되지 않은 경우 관리자는 새 **AD-SUPPORT** 하위 정책을 활성화할 수 있습니다.

- **SSSD**는 **AD**에 직접 연결된 **RHEL** 시스템에서 사용됩니다.
- **adcli**는 **AD** 도메인에 가입하거나 호스트 속성을 업데이트하는 데 사용됩니다(예: 호스트 키).
- **realmd**는 **AD** 도메인에 연결하는 데 사용됩니다.

다음 조건 중 하나가 적용되는 경우 새 하위 정책을 활성화하는 것이 좋습니다.

- **AD**의 사용자 또는 서비스 계정에는 **RC4** 암호화 키가 있으며 **AES** 암호화 키가 없습니다.
- 개별 **Active Directory** 도메인 간 신뢰 링크에는 **RC4** 암호화 키가 있으며 **AES** 암호화 키가 없습니다.

DEFAULT 암호화 정책 외에도 AD-SUPPORT 하위 정책을 활성화하려면 다음을 입력합니다.

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

(BZ#1866695)

Authselect 에는 새로운 최소 프로파일 있습니다.

authselect 유틸리티에는 새로운 최소 프로파일 있습니다. 이 프로파일을 사용하여 다른 인증 공급자를 사용하는 대신 시스템 파일에서 직접 로컬 사용자와 그룹만 제공할 수 있습니다. 따라서 SSSD, winbind 및 fprintd 패키지를 안전하게 제거하고 최소 설치가 필요한 시스템에서 이 프로파일을 사용하여 디스크와 메모리 공간을 절약할 수 있습니다.

(BZ#1654018)

암호를 회전할 때 SSSD에서 Samba의 secrets.tdb 파일을 업데이트합니다.

sssd.conf 파일의 새로운 ad_update_samba_machine_account_password 옵션을 RHEL에서 사용할 수 있습니다. Samba를 사용하는 동안 시스템의 도메인 암호를 순환할 때 SSSD를 사용하여 Samba secrets.tdb 파일을 자동으로 업데이트할 수 있습니다.

그러나 SELinux가 강제 모드인 경우 SSSD는 secrets.tdb 파일을 업데이트하지 못합니다. 따라서 Samba는 새 암호에 액세스할 수 없습니다. 이 문제를 해결하려면 SELinux를 허용 모드로 설정합니다.

(BZ#1793727)

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/sss/sss.conf 파일의 ad_gpo_access_control 옵션 값을 허용 으로 변경합니다.

(JIRA:RHELPLAN-51289)

Directory Server에서 pwdReset 작업 속성을 지원

이번 개선된 기능에는 **pwdReset** 작업 속성을 **Directory Server**에 대한 지원이 추가되었습니다. 관리자가 사용자 암호를 변경하면 **Directory Server**는 사용자 항목의 **pwdReset** 을 **true** 로 설정합니다. 결과적으로 애플리케이션은 이 속성을 사용하여 관리자가 암호를 재설정했는지 여부를 확인할 수 있습니다.

pwdReset 은 작동 속성이므로 사용자가 편집할 수 없습니다.

([BZ#1775285](#))

Directory Server는 이제 **RESULT** 항목에 작업 및 작업 시간을 기록합니다.

이번 업데이트를 통해 **Directory Server**는 이제 `/var/log/dirsrv/slapd-<instance_name>/access` 파일의 **RESULT**'entries에 두 개의 추가 시간 값을 기록합니다.

- **wtime** 값은 작업 큐에서 작업자 스레드로 작업을 이동하는 데 걸리는 시간을 나타냅니다.
- **optime** 값은 작업자 스레드가 작업을 시작한 후 실제 작업을 완료하는 데 걸리는 시간을 표시합니다.

새 값은 **Directory Server**에서 부하 및 프로세스 작업을 처리하는 방법에 대한 추가 정보를 제공합니다.

자세한 내용은 **Red Hat Directory Server Configuration, Command 및 File Reference**의 [액세스 로 그](#) 참조 섹션을 참조하십시오.

([BZ#1850275](#))

5.1.14. 데스크탑

단일 애플리케이션 세션 사용 가능

이제 키오스크 모드라고도 하는 단일 애플리케이션 세션에서 **GNOME**을 시작할 수 있습니다. 이 세션에서 **GNOME**은 구성된 애플리케이션의 전체 화면 창만 표시합니다.

단일 애플리케이션 세션을 활성화하려면 다음을 수행합니다.

1. **gnome-session-kiosk-session** 패키지를 설치합니다.

```
# yum install gnome-session-kiosk-session
```

2. 단일 애플리케이션 세션을 열 사용자의 **\$HOME/.local/bin/redhat-kiosk** 파일을 생성하고 편집합니다.

파일에서 시작할 애플리케이션의 실행 가능 이름을 입력합니다.

예를 들어 텍스트 편집기 애플리케이션을 시작하려면 다음을 수행합니다.

```
#!/bin/sh  
  
gedit &
```

3. 파일을 실행 가능으로 설정합니다.

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

4. **GNOME** 로그인 화면의 **cogc** 버튼 메뉴에서 키오스크 세션을 선택하고 단일 애플리케이션 사용자로 로그인합니다.

(BZ#1739556)

tigervnc 버전이 1.10.1로 업데이트되었습니다

tigervnc 제품군은 버전 1.10.1로 업데이트되었습니다. 업데이트에는 수정 사항 및 개선 사항이 포함되어 있습니다. 가장 중요한 것은 다음과 같습니다.

- **tigervnc**는 이제 **systemd** 서비스 관리자를 사용하는 가상 네트워크 컴퓨팅(VNC) 서버지만 지원합니다.

- 클립 보드는 네이티브 뷰어 **WinVNC** 및 **Xvnc/libvnc.so**에서 전체 유니코드를 지원합니다.
- 이제 네이티브 클라이언트는 서버 인증서를 확인할 때 시스템 신뢰 저장소를 유지합니다.
- **Java** 웹 서버가 제거되었습니다.
- 이제 로컬 연결만 허용하도록 **x0vncserver** 를 구성할 수 있습니다.
- 디스플레이의 일부만 공유되는 경우 **x0vncserver** 에서 수정 사항을 받았습니다.
- 이제 **WinVNC** 에서 폴링이 기본값입니다.
- **VMware**의 **VNC** 서버와의 호환성이 개선되었습니다.
- **macOS**의 일부 입력 방법과의 호환성이 향상되었습니다.
- 기법의 자동 "복합(repair)"이 개선되었습니다.

([BZ#1806992](#))

5.1.15. 그래픽 인프라

새로운 그래픽 카드 지원

이제 다음과 같은 그래픽 카드가 완전히 지원됩니다.

- **AMD Navi 14** 제품군에는 다음 모델이 포함됩니다.
 - **Radeon RX 5300**

- **Radeon RX 5300 XT**
- **Radeon RX 5500**
- **Radeon RX 5500 XT**
- 다음 모델을 포함하는 **AMD Renoir APU** 제품군:
 - **Ryzen 3 4300U**
 - **Ryzen 5 4500U, 4600U, 4600H**
 - **Ryzen 7 4700U, 4800U, 4800H**
- 다음 모델을 포함하는 **AMD Dali APU** 제품군:
 - **Athlon Silver 3050U**
 - **Athlon Gold 3150U**
 - **Ryzen 3 3250U**

또한 다음 그래픽 드라이버가 업데이트되었습니다.

- **Matrox mgag200** 드라이버

(JIRA:RHELPLAN-55009)

Nvidia Volta 및 **booting**을 통한 하드웨어 가속

노비 토 그래픽 드라이버는 현재 **Nvidia Volta** 및 **GPU** 제품군과 함께 하드웨어 가속을 지원합니다. 결과적으로 **3D** 그래픽을 사용하는 데스크탑과 애플리케이션이 **GPU**에서 효율적으로 렌더링됩니다. 또한 **CPU**를 다른 작업에 사용할 수 없어 전체 시스템 응답성이 향상됩니다.

(JIRA:RHELPLAN-57564)

XWayland에서 디스플레이 해제 감소

XWayland 디스플레이 백엔드는 이제 **XPresent** 확장을 활성화합니다. **XPresent**를 사용하면 애플리케이션에서 창 내용을 효율적으로 업데이트할 수 있어 디스플레이 해제가 줄어듭니다.

이 기능을 사용하면 **3D** 편집기와 같은 전체 화면 **OpenGL** 애플리케이션의 사용자 인터페이스 렌더링이 크게 향상됩니다.

(JIRA:RHELPLAN-57567)

Intel Tiger Lake GPU 지원

이번 업데이트에서는 **Intel Tiger Lake GPU** 제품군에 대한 지원이 추가되었습니다. 여기에는 다음 **CPU** 모델을 사용하여 찾은 **Intel[®] Graphics** 및 **Intel Xe GPU**가 포함됩니다 .
<https://ark.intel.com/content/www/us/en/ark/products/codename/88759/tiger-lake.html>.

Tiger Lake GPU 지원을 활성화하기 위해 **i915.alpha_support=1** 또는 **i915.force_probe=* 커널 옵션**을 더 이상 설정할 필요가 없습니다.

이 향상된 기능은 [RHSA-2021:0558](#) 비동기 권고의 일부로 릴리스되었습니다.

(BZ#1882620)

5.1.16. 웹 콘솔

웹 콘솔 세션 내에서 권한 설정

이번 업데이트를 통해 웹 콘솔은 사용자 세션 내부에서 관리 액세스와 제한된 액세스를 전환할 수 있는 옵션을 제공합니다. 웹 콘솔 세션에서 관리 액세스 또는 제한된 액세스 표시기를 클릭하여 모드 간에 전환할 수 있습니다.

(JIRA:RHELPLAN-42395)

로그 검색 개선 사항

이번 업데이트를 통해 웹 콘솔에는 사용자가 로그 중에서 검색할 수 있는 몇 가지 새로운 방법을 지원하는 검색 상자가 도입되었습니다. 검색 상자는 로그 메시지에서 검색하거나 서비스를 지정하거나 특정 로그 필드가 있는 항목을 검색하는 정규 표현식을 지원합니다.

(BZ#1710731)개요 페이지에 더 자세한 **Insights** 보고서 표시

이번 업데이트를 통해 **Red Hat Insights**에 연결된 경우 웹 콘솔의 개요 페이지의 상태 카드는 적중 수와 우선 순위에 대한 자세한 정보를 보여줍니다.

(JIRA:RHELPLAN-42396)**5.1.17. Red Hat Enterprise Linux 시스템 역할****RHEL 시스템 역할에 터미널 로그 역할 추가**

이 향상된 기능을 통해 **rhel-system-roles** 패키지와 함께 **RHEL** 시스템 역할에 새 **터미널 로그 (TLOG)** 역할이 추가되었습니다. 이제 사용자는 **tlog** 역할을 사용하여 **Ansible**을 사용하여 세션 기록을 설정하고 구성할 수 있습니다.

현재 **tlog** 역할은 다음 작업을 지원합니다.

- **systemd** 저널에 기록 데이터를 기록하도록 **tlog** 구성
- **SSSD**를 통해 명시적 사용자 및 그룹에 대한 세션 기록 활성화

(BZ#1822158)**Ansible에서 RHEL 로깅 시스템 역할을 사용할 수 있습니다**

로깅 시스템 역할을 사용하면 로컬 및 원격 호스트에 다양한 로깅 구성을 일관되게 배포할 수 있습니다

다. 여러 클라이언트 시스템에서 로그를 수집하도록 **RHEL** 호스트를 서버로 구성할 수 있습니다.

([BZ#1677739](#))

rhel-system-roles-sap 완전 지원

이전에 기술 프리뷰로 사용 가능한 **rhel-system-roles-sap** 패키지가 이제 완전히 지원됩니다. **SAP** 워크로드를 실행하기 위해 **RHEL** 시스템의 구성을 자동화하는 데 사용할 수 있는 **SAP용 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 다음과 같은 새로운 역할은 완전히 지원됩니다.

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

자세한 내용은 [SAP용 Red Hat Enterprise Linux 시스템 역할](#)을 참조하십시오.

([BZ#1660832](#))

이제 **Metrics RHEL System Role**을 **Ansible**에 사용할 수 있습니다.

메트릭 **RHEL** 시스템 역할을 사용하면 로컬 및 원격 호스트에 대해 를 구성할 수 있습니다.

- **pcp** 애플리케이션을 통한 성능 분석 서비스
- **grafana** 서버를 사용하여 이 데이터의 시각화
- 이러한 서비스를 수동으로 구성하지 않고도 **redis** 데이터 소스를 사용하여 이 데이터를 쿼리

합니다.

([BZ#1890499](#))

rhel-system-roles-sap 업그레이드

rhel-system-roles-sap 패키지가 여러 버그 수정 및 개선 사항을 제공하는 업스트림 버전 **2.0.0**으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 호스트 이름 설정 및 확인 개선
- **uuid** 상태 감지 및 처리 개선
- **--check (-c)** 옵션에 대한 지원 추가
- **nofile** 한도를 32800에서 65536으로 늘립니다.
- **nfs-utils** 파일을 **sap_preconfigure_packages***에 추가합니다.
- **firewalld** 를 비활성화합니다. 이 변경으로 **firewalld** 가 설치될 때만 비활성화됩니다.
- **RHEL 8.0** 및 **RHEL 8.1**에 필요한 최소 버전의 설정을 추가합니다.
- **tmpfiles.d/sap.conf** 파일 처리 개선
- 단일 단계 실행 지원 또는 **SAP** 노트 확인 지원
- 필요한 **compat-sap-c++** 패키지를 추가합니다.
- 최소 패키지 설치 처리 개선

- **RHEL 시스템 역할을 적용한 후 재부팅이 필요한지 감지**
- 모든 **SELinux** 상태 설정 지원. 기본 상태는 "비활성화됨"입니다.
- 동일한 **IP** 주소가 있는 행이 두 개 이상 있는 경우 더 이상 실패하지 않습니다
- **sap_ip**가 포함된 행이 두 개 이상 있는 경우 **/etc/hosts** 를 더 이상 수정하지 않습니다
- **RHEL 7.7**에서 **HANA** 지원
- **PPc 64le** 플랫폼의 **SAP HANA**에 필요한 **IBM** 서비스 및 생산성 도구용 리포지토리 추가 지원

([BZ#1844190](#))

스토리지 **RHEL** 시스템 역할이 파일 시스템 관리를 지원

이번 개선된 기능을 통해 관리자는 스토리지 **RHEL** 시스템 역할을 사용하여 다음을 수행할 수 있습니다.

- **ext4** 파일의 크기 조정
- **LVM** 파일의 크기 조정
- 기본 매개 변수를 사용하는 블록 장치에 스왑 파티션을 만들거나 스왑 파티션을 수정합니다.

([BZ#1959289](#))

5.1.18. 가상화

호환되지 않는 **TSC** 설정을 사용하여 가상 머신을 호스트로 마이그레이션하는 속도가 빨라졌습니다.

이전에는 호환되지 않는 **TSC(Time Stamp Counter)** 설정이 있는 호스트로 가상 머신을 마이그레이션하는 데 실패했습니다. 이번 업데이트를 통해 마이그레이션 프로세스를 시작하기 전에 이러한 마이그레이션을 시도하면 오류가 발생합니다.

(JIRA:RHELPLAN-45950)

2세대 AMD EPYC 프로세서의 가상화 지원

이번 업데이트에서는 **RHEL 8**의 가상화에 **EPYC**라고도 하는 2세대 **AMD EPYC** 프로세서가 지원됩니다. 결과적으로 **RHEL 8**에서 호스팅되는 가상 머신은 이제 **EPYC-Rome CPU** 모델을 사용할 수 있으며 프로세서에서 제공하는 새로운 기능을 사용할 수 있습니다.

(JIRA:RHELPLAN-45959)

새 명령: **virsh iothreadset**

이번 업데이트에서는 **IOThread** 풀링을 구성하는 데 사용할 수 있는 **virsh iothreadset** 명령이 도입되었습니다. 따라서 **IOThread**에 더 많은 **CPU** 소비를 희생하면서 **I/O** 집약적인 워크로드에 대한 대기 시간이 짧은 가상 머신을 설정할 수 있습니다. 특정 옵션은 **virsh** 도움말 페이지를 참조하십시오.

(JIRA:RHELPLAN-45958)

10세대 Intel Core 프로세서에서 KVM에서 **UMIP** 지원

이번 업데이트를 통해 이제 **KVM**에서 10세대 **Intel Core** 프로세서(**Ice Lake Server**라고도 함)에서 실행되는 호스트에 대해 **UMIP(User-mode instructions)** 기능을 지원합니다. 현재 권한 수준(**CPL**)이 0보다 크면 **UMIP** 기능은 **sgdt,sidt,sldt,smsw, str** 와 같은 특정 지침이 실행되면 일반 보호 예외를 발행합니다. 결과적으로 **UMIP**는 무단 애플리케이션이 권한 에스컬레이션 공격을 시작하는 데 사용할 수 있는 특정 시스템 전체 설정에 액세스하지 못하도록 하여 시스템 보안을 보장합니다.

(JIRA:RHELPLAN-45957)

libvirt 라이브러리에서 **Memory Bandwidth Allocation** 지원

libvirt 는 이제 **MBA**(메모리 대역폭 할당)를 지원합니다. **MBA**를 사용하면 <cputune> 섹션의 <memorytune> 요소를 사용하여 **vCPU** 스레드에서 호스트 메모리 대역폭 부분을 할당할 수 있습니다.

MBA는 **Intel Xeon v4** 프로세서에서 **Broadwell** 서버라고도 하는 기존 **Cache QoS Enforcement(CQE)** 기능을 확장한 것입니다. **CPU** 선호도와 관련된 작업의 경우 **MBA**에서 사용하는 메

커니즘은 **CQE**와 동일합니다.

(JIRA:RHELPLAN-45956)

RHEL 6 가상 머신에서 **Q35** 머신 유형을 지원

RHEL 6을 게스트 **OS**로 사용하는 **RHEL 8**에서 호스팅되는 **VM**(가상 머신)은 이제 최신 **PCI Express** 기반 머신 유형인 **Q35**를 사용할 수 있습니다. 이를 통해 가상 장치의 기능 및 성능이 다양하게 개선되고 광범위한 최신 장치가 **RHEL 6 VM**과 호환될 수 있습니다.

(JIRA:RHELPLAN-45952)

이제 기록된 모든 **QEMU** 이벤트에 타임스탬프가 있습니다. 결과적으로 **/var/log/libvirt/qemu/** 디렉터리에 저장된 로그를 사용하여 가상 머신의 문제를 보다 쉽게 해결할 수 있습니다.

QEMU 로그에 **spice-server** 이벤트의 타임스탬프가 포함됩니다.

이번 업데이트에서는 '**spice-server**' 이벤트 로그에 타임스탬프가 추가되었습니다. 따라서 모든 기록된 **QEMU** 이벤트에 타임스탬프가 있습니다. 결과적으로 **/var/log/libvirt/qemu/** 디렉터리에 저장된 로그를 사용하여 가상 머신의 문제를 보다 쉽게 해결할 수 있습니다.

(JIRA:RHELPLAN-45945)

bochs-display 장치가 지원됨

RHEL 8.3 이상에서는 **Bochs** 디스플레이 장치를 도입하는데, 이는 현재 사용된 **stdvga** 장치보다 더 안전합니다. **bochs-display** 와 호환되는 모든 **VM**(가상 머신)은 기본적으로 사용됩니다. 여기에는 주로 **UEFI** 인터페이스를 사용하는 **VM**이 포함됩니다.

(JIRA:RHELPLAN-45939)

가상 머신에 최적화된 **MDS** 보호

이번 업데이트를 통해 **RHEL 8** 호스트는 해당 **VM**(가상 머신)이 **MDS**(**Microarchitectural Data Sampling**)에 취약했는지 여부를 알 수 있습니다. 취약하지 않은 **VM**은 **MDS**에 대한 측정값을 사용하지 않으므로 성능이 향상됩니다.

(JIRA:RHELPLAN-45937)**RBD에서 QCOW2 디스크 이미지 생성 지원**

이번 업데이트를 통해 **RADOS** 블록 장치(**RBD**) 스토리지에서 **QCOW2** 디스크 이미지를 생성할 수 있습니다. 결과적으로 가상 시스템은 **QCOW2** 이미지로 스토리지 백엔드에 **RBD** 서버를 사용할 수 있습니다.

그러나 현재 **RBD** 스토리지의 **QCOW2** 디스크 이미지의 쓰기 성능이 예상보다 낮습니다.

(JIRA:RHELPLAN-45936)**지원되는 최대 VFIO 장치 최대 64개로 증가**

이번 업데이트를 통해 **VFIO**를 사용하는 최대 **64**개의 **PCI** 장치를 **RHEL 8** 호스트의 단일 가상 머신에 연결할 수 있습니다. **RHEL 8.2**에서는 **32**개 이상입니다.

(JIRA:RHELPLAN-45930)**QEMU/KVM에서 discard 및 write-zeroes 명령이 지원됩니다.**

이번 업데이트를 통해 **virtio-blk**의 삭제 및 쓰기-0es 명령이 **QEMU/KVM**에서 지원됩니다. 결과적으로 가상 시스템은 **virtio-blk** 장치를 사용하여 사용되지 않는 섹터 **SSD**를 폐기하거나 비어 있을 때 **0**으로 섹터를 채울 수 있습니다. 이 옵션을 사용하여 **SSD** 성능을 향상하거나 드라이브가 안전하게 지워지도록 할 수 있습니다.

(JIRA:RHELPLAN-45926)**RHEL 8에서 IBM POWER 9 XIVE 지원**

이번 업데이트에서는 **IBM POWER9**에서 **RHEL 8**의 외부 인터럽트 가상화 엔진(**XIVE**) 기능을 지원합니다. 결과적으로 **IBM POWER 9** 시스템의 **RHEL 8** 하이퍼바이저에서 실행되는 **VM**(가상 머신)은 **XIVE**를 사용할 수 있으므로 **I/O** 집약적인 **VM**의 성능이 향상됩니다.

(JIRA:RHELPLAN-45922)**가상 머신 제어 그룹 v2 지원**

이번 업데이트를 통해 **libvirt** 제품군은 제어 그룹 **v2**를 지원합니다. 따라서 **RHEL 8**에서 호스팅되는 가상 머신은 제어 그룹 **v2**의 리소스 제어 기능을 활용할 수 있습니다.

(JIRA:RHELPLAN-45920)

반가상화 **IPI**가 **Windows** 가상 머신에서 지원

이번 업데이트를 통해 **hv_ipi** 플래그가 **Windows VM**(가상 머신)에 지원되는 하이퍼바이저 구현에 추가되었습니다. 이를 통해 프로세서 간 인터럽트(**IPI**)를 **hypercall**을 통해 보낼 수 있습니다. 결과적으로 **Windows OS**를 실행하는 **VM**에서 **IPI**를 더 빠르게 수행할 수 있습니다.

(JIRA:RHELPLAN-45918)

디스크 캐시가 활성화된 가상 머신을 마이그레이션할 수 있습니다.

이번 업데이트에서는 디스크 캐시 실시간 마이그레이션과 호환되는 **RHEL 8 KVM** 하이퍼바이저가 업데이트되었습니다. 결과적으로 디스크 캐시가 활성화된 가상 머신을 실시간 마이그레이션할 수 있습니다.

(JIRA:RHELPLAN-45916)

권한 없는 세션의 가상 시스템에서 **MacVTap** 인터페이스를 사용할 수 있습니다

이제 **VM**(가상 머신)에서 이전에 권한 있는 프로세스에 의해 생성된 **macvtap** 인터페이스를 사용할 수 있습니다. 특히 **libvirtd**의 권한이 없는 사용자 세션에서 시작된 **VM**은 **macvtap** 인터페이스를 사용할 수 있습니다.

이를 위해 먼저 권한 있는 환경에서 **macvtap** 인터페이스를 만들고 권한이 없는 세션에서 **libvirtd**를 실행할 사용자가 소유하도록 설정합니다. 이 작업은 웹 콘솔과 같은 관리 애플리케이션을 사용하거나 **root**와 같은 명령줄 유틸리티를 사용하여 수행할 수 있습니다. 예를 들면 다음과 같습니다.

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

그런 다음 새로 생성된 **macvtap** 인터페이스를 참조하도록 **VM <interface>** 구성의 **<target>** 하위 요소를 수정합니다.

```
<interface type='ethernet'>
  <model type='virtio'/>
  <mac address='52:54:00:11:11:11'/>
```

```
<target dev='mymacvtap0' managed='no' />
</interface>
```

이 구성을 사용하면 **libvirt**가 사용자 **myuser**로 실행되면 VM이 시작될 때 기존 **macvtap** 인터페이스를 사용합니다.

(JIRA:RHELPLAN-45915)

가상 머신은 이제 10세대 **Intel Core** 프로세서의 기능을 사용할 수 있음

이제 가상 머신(VM)에 **Icelake-Server** 및 **Icelake-Client CPU** 모델 이름을 사용할 수 있습니다. 10세대 **Intel Core** 프로세서가 있는 호스트에서는 **Icelake-Server** 또는 **Icelake-Client**를 VM의 XML 구성에서 CPU 유형으로 사용하면 이러한 CPU의 새로운 기능이 VM에 노출됩니다.

(JIRA:RHELPLAN-45911)

QEMU에서 LUKS 암호화 지원

이번 업데이트를 통해 **LUKS**(Linux Unified Key Setup) 암호화를 사용하여 가상 디스크를 생성할 수 있습니다. 가상 머신의(VM) XML 구성에 **<encryption>** 필드를 포함하여 스토리지 볼륨을 생성할 때 디스크를 암호화할 수 있습니다. XML 구성 파일의 디스크 도메인 정의에 **<encryption>** 필드를 포함하여 **LUKS** 암호화된 가상 디스크를 VM에 완전히 투명하게 만들 수도 있습니다.

(JIRA:RHELPLAN-45910)

nbdkit로그 개선

nbdkit 서비스 로깅이 덜 자세한 정보 표시로 수정되었습니다. 결과적으로 **nbdkit**은 잠재적으로 중요한 메시지만 로그하고 **virt-v2v** 변환 중에 생성된 로그는 짧고 구문 분석하기 쉽습니다.

(JIRA:RHELPLAN-45909)

가상 머신 SELinux 보안 레이블 및 권한의 일관성 개선

이번 업데이트를 통해 **libvirt** 서비스는 파일과 관련된 **SELinux** 보안 레이블 및 권한을 기록하고 파일을 수정한 후 레이블을 복원할 수 있습니다. 예를 들어, **libguestfs** 유틸리티를 사용하여 특정 사용자가 소유한 가상 머신(VM) 디스크 이미지를 수정해도 더 이상 이미지 소유자가 **root**로 변경되지 않습니다.

이 기능은 **NFS**와 같은 확장된 파일 속성을 지원하지 않는 파일 시스템에서는 작동하지 않습니다.

(JIRA:RHELPLAN-45908)

QEMU에서 **XTS** 암호화 라이브러리에 **gcrypt** 라이브러리를 사용

이번 업데이트를 통해 **QEMU** 에뮬레이터가 **gcrypt** 라이브러리에서 제공하는 **XTS** 암호화 모드 구현을 사용하도록 변경되었습니다. 이렇게 하면 호스트 스토리지에서 **QEMU**의 기본 **luks** 암호화 드라이버를 사용하는 가상 시스템의 I/O 성능이 향상됩니다.

(JIRA:RHELPLAN-45904)

Windows Virtio 드라이버는 이제 **Windows Updates**를 사용하여 업데이트할 수 있습니다.

이번 업데이트를 통해 **QEMU**가 시작될 때 기본적으로 새로운 표준 **SMBIOS** 문자열이 시작됩니다. **SMBIOS** 필드에 제공된 매개 변수를 사용하면 가상 시스템(VM)에서 실행되는 가상 하드웨어의 ID를 생성할 수 있습니다. 결과적으로 **Windows** 업데이트는 가상 하드웨어와 **RHEL** 하이퍼바이저 머신 유형을 식별하고 **Windows 10+**, **Windows Server 2016** 및 **Windows Server 2019+**를 실행하는 VM에서 **Virtio** 드라이버를 업데이트할 수 있습니다.

(JIRA:RHELPLAN-45901)

새 명령: **virsh guestinfo**

virsh guestinfo 명령이 **RHEL 8.3**에 도입되었습니다. 이렇게 하면 가상 머신(VM)에 대한 다음 유형의 정보를 보고할 수 있습니다.

- 게스트 OS 및 파일 시스템 정보
- 활성 사용자
- 사용된 시간대

virsh guestinfo 를 실행하기 전에 **qemu-guest-agent** 패키지가 설치되어 있는지 확인합니다. 또한 **guest_agent** 채널은 다음과 같이 VM의 XML 구성에서 활성화되어야 합니다.

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

(JIRA:RHELPLAN-45900)

KVM에서 BFLOAT16 입력에 대한 VNNI 지원

이번 업데이트에서 VNNI(Vector Neural Network instructions)가 BFLOAT16 입력(X 512_BF16 명령이라고도 함)을 지원하는 VNNI(Vector Neural Network instructions)는 이제 KVM에서 3세대 Intel Xeon 확장형 프로세서에서 실행되는 호스트에 대해 지원되고 있습니다. 결과적으로 게스트 소프트웨어는 가상 CPU 구성에서 이를 활성화하여 가상 머신 내에서 암호 해독_BF16 지침을 사용할 수 있습니다.

(JIRA:RHELPLAN-45899)

새 명령: virsh pool-capabilities

RHEL 8.3에는 virsh pool-capabilities 명령 옵션이 도입되었습니다. 이 명령은 호스트의 각 풀 내에 있는 스토리지 풀 외에도 스토리지 풀을 만드는 데 사용할 수 있는 정보를 표시합니다. 여기에는 다음이 포함됩니다.

- 스토리지 풀 유형
- 스토리지 풀 소스 형식
- 대상 스토리지 볼륨 형식 유형

(JIRA:RHELPLAN-45884)

Intel Xeon 플래티넘 9200 시리즈 프로세서가 탑재된 가상 시스템에서 CPUID.1F 지원

이번 업데이트를 통해 CPUID.1F(Extended Topology Enumeration playbooks) 기능(CPUID.1F)을 사용하여 여러 가상 CPU 토폴로지가 종료된 RHEL 8에서 호스팅되는 가상 머신을 구성할 수 있습니다. 이 기능은 이전에 Cascade Lake라고 알려진 Intel Xeon 플래티넘 9200 시리즈 프로세서에서 지원됩니다. 결과적으로 Intel Xeon 플래티넘 9200 시리즈 프로세서를 사용하는 호스트에서 호스트의 물리적 CPU 토폴로지를 미리링하는 vCPU 토폴로지를 생성할 수 있습니다.

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

가상 머신은 이제 3세대 Intel Xeon 확장형 프로세서의 기능을 사용할 수 있음

이제 VM(가상 머신)에 CPU 모델 이름을 사용할 수 있습니다. VM의 XML 구성에 CPU 유형을 CPU 유형으로 사용하면 호스트가 이 CPU를 사용하는 경우 VM에 노출된 3세대 Intel Xeon 확장 프로세서의 새로운 기능이 생성됩니다.

(JIRA:RHELPLAN-37570)

Intel Optane 영구 메모리가 KVM에서 지원

이번 업데이트를 통해 RHEL 8에서 호스팅되는 가상 머신은 이전에 Intel Optane Ridge라고 하는 Intel Optane 영구 메모리 기술을 활용할 수 있습니다. Intel Optane 영구 메모리 스토리지 장치는 데이터 센터급 영구 메모리 기술을 제공하므로 트랜잭션 처리량이 크게 증가할 수 있습니다.

(JIRA:RHELPLAN-14068)

가상 머신에서 Intel Processor Trace 사용 가능

이번 업데이트를 통해 RHEL 8에서 호스팅되는 VM(가상 머신)은 Intel 프로세서 추적(PT) 기능을 사용할 수 있습니다. 호스트에서 Intel UEFI를 지원하는 CPU를 사용하는 경우 특수 Intel 소프트웨어를 사용하여 VM CPU의 성능에 대한 다양한 지표를 수집할 수 있습니다. 이를 위해서는 VM의 XML 구성에서 intel-pt 기능을 활성화해야 합니다.

(JIRA:RHELPLAN-7788)

이제 DASD 장치를 IBM Z의 가상 머신에 할당할 수 있음

DASD(직접 액세스 스토리지 장치)는 다양한 특정 스토리지 기능을 제공합니다. vfio-ccw 기능을 사용하여 DASD를 IBM Z 호스트의 VM(가상 머신)에 중재된 장치로 할당할 수 있습니다. 예를 들어 VM이 z/OS 데이터 세트에 액세스하거나 할당된 DASD를 z/OS 시스템과 공유할 수 있습니다.

(JIRA:RHELPLAN-40234)

IBM Z에 지원되는 IBM Secure Execution

IBM Z 하드웨어를 사용하여 RHEL 8 호스트를 실행하는 경우 VM(가상 시스템)에 대한 IBM Secure Execution을 구성하여 VM(가상 시스템)의 보안을 개선할 수 있습니다. IBM Secure Execution(보호된

가상화이라고도 함)을 사용하면 호스트 시스템이 VM의 상태 및 메모리 콘텐츠에 액세스할 수 없습니다.

따라서 호스트가 손상되어도 게스트 운영 체제를 공격하기 위한 벡터로 사용할 수 없습니다. 또한 **Secure Execution**을 사용하여 신뢰할 수 없는 호스트가 VM에서 중요한 정보를 얻지 못하도록 할 수 있습니다.

(JIRA:RHELPLAN-14754)

5.1.19. 클라우드 환경의 RHEL

cloud-utils-growpart 를 1로 변경

cloud-utils-growpart 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 1로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- **GPT 디스크가 2TB** 지난 성장을 방지하는 버그가 수정되었습니다.
- 시작 섹터와 크기가 같으면 **growpart** 작업이 더 이상 실패하지 않습니다.
- 일부 경우 이전에 **sgdisk** 유틸리티를 사용하여 파티션 크기 조정에 실패했습니다. 이 문제는 이제 해결되었습니다.

(BZ#1846246)

5.1.20. 컨테이너

Skopeo 컨테이너 이미지를 사용할 수 있습니다

registry.redhat.io/rhel8/skopeo 컨테이너 이미지는 **skopeo** 패키지의 컨테이너화된 구현입니다. **skopeo** 툴은 컨테이너 이미지 및 이미지 리포지토리에서 다양한 작업을 수행하는 명령줄 유틸리티입니다. 이 컨테이너 이미지를 사용하면 레지스트리의 컨테이너 이미지를 검사하여 레지스트리에서 컨테이너 이미지를 제거하고 인증되지 않은 컨테이너 레지스트리의 컨테이너 이미지를 다른 컨테이너 레지스트리로 복사할 수 있습니다. **registry.redhat.io/rhel8/skopeo** 컨테이너 이미지를 가져오려면 활성 **Red Hat Enterprise Linux** 서브스크립션이 필요합니다.

(BZ#1627900)

Buildah 컨테이너 이미지를 사용할 수 있습니다

registry.redhat.io/rhel8/buildah 컨테이너 이미지는 **buildah** 패키지의 컨테이너화된 구현입니다. **buildah** 툴을 사용하면 **OCI** 컨테이너 이미지를 쉽게 빌드할 수 있습니다. 이 컨테이너 이미지를 사용하면 시스템에 **buildah** 패키지를 설치할 필요 없이 컨테이너 이미지를 빌드할 수 있습니다. 사용 사례는 루트가 아닌 사용자로 이 이미지를 **rootless** 모드에서 실행하는 것을 다루지 않습니다. **registry.redhat.io/rhel8/buildah** 컨테이너 이미지를 가져오려면 활성 **Red Hat Enterprise Linux** 서비스 크립션이 필요합니다.

([BZ#1627898](#))

Podman v2.0 RESTful API 사용 가능

새 **REST** 기반 **Podman 2.0 API**는 **varlink** 라이브러리를 기반으로 이전 원격 **API**를 대체합니다. 새 **API**는 **rootful** 환경과 **rootless** 환경에서 모두 작동하며 **Docker** 호환성 계층을 제공합니다.

([JIRA:RHELPLAN-37517](#))

Podman을 설치할 때 **container-selinux**가 필요하지 않습니다.

이번 개선된 기능을 통해 이제 컨테이너 빌드 중에 **container-selinux** 패키지 설치가 선택 사항으로 표시됩니다. 따라서 **Podman**은 다른 패키지에 대한 종속성이 줄어듭니다.

([BZ#1806044](#))

5.2. 외부 커널 매개변수로 중요한 변경

이 장에서는 시스템 관리자에게 **Red Hat Enterprise Linux 8.3**과 함께 제공되는 커널의 중요한 변경 사항을 요약해서 설명합니다. 이러한 변경에는 추가 또는 업데이트된 **proc** 항목, **sysctl** 및 **sysfs** 기본값, 부팅 매개 변수, 커널 구성 옵션 또는 눈에 띄게 동작 변경이 포함될 수 있습니다.

새 커널 매개변수

acpi_no_watchdog = [HW,ACPI,WDT]

이 매개 변수를 사용하면 고급 구성 및 전원 인터페이스(**ACPI**) 기반 위치독 인터페이스(**WDAT**)를 무시하고 기본 드라이버가 위치독 장치를 대신 제어하도록 합니다.

dfltcc = [HW,S390]

이 매개 변수는 **IBM Z** 아키텍처에 대한 **zlib** 하드웨어 지원을 구성합니다.

형식: { on | off | def_only | inf_only | always }

옵션은 다음과 같습니다.

- 에서 (기본값) - 레벨 1에서의 압축 및 압축 해제를 위한 **IBM Z zlib** 하드웨어 지원
- **off** - **IBM Z zlib** 하드웨어 지원 없음
- **deflate** 알고리즘에 대한 **IBM Z zlib** 하드웨어 지원(레벨 1에 대한 압축)
- **inf_only** - **IBM Z zlib** 하드웨어가 비플릿 알고리즘에 대한 지원 (압축 해제)
- **Always** - 와 유사하지만 선택한 압축 수준을 무시하고 항상 하드웨어 지원을 사용합니
다(디렉터리에 사용됨)

irqchip.gicv3_pseudo_nmi = [ARM64]

이 매개 변수는 커널에서 마스크 불가능 인터럽트(NMI)를 지원합니다.

이 매개 변수를 사용하려면 **CONFIG_ARM64_PS EUDO_NMI** 구성 항목을 사용하여 커널을 빌드해야 합니다.

panic_on_taint =

add_taint ()에서 **panic()** 을 조건부로 호출하는 비트마스크

형식: <hex>[,nouser_taint]

이 세트에서 **add_taint()** 시스템 호출을 호출할 때 커널이 패닉을 발생시키는 **TAINT** 플래그 세트를 나타내는 16진수 비트마스크입니다. 선택 사항인 **nouser_taint** 스위치는 **panic_on_taint**의 비트마스크와 일치하는 플래그 세트와 일치하는 **/proc/sys/kernel/tainted** 파일에 기록하여 사용자 공간 강화 충돌을 방지합니다.

자세한 내용은 [업스트림 문서를 참조하십시오](#).

prot_virt = [S390]

형식: <bool>

이 매개 변수를 사용하면 하드웨어 지원이 있는 경우 하이퍼바이저와 격리된 보호된 가상 시스템을 호스팅할 수 있습니다.

rcutree.use_softirq = [KNL]

이 매개 변수를 사용하면 **Tree-RCU softirq** 처리를 제거할 수 있습니다.

이 매개 변수를 **0**으로 설정하면 모든 **RCU_SOFTIRQ** 처리를 CPU당 **rcuc kthreads**로 이동합니다. **rcutree.use_softirq** 를 **0**이 아닌 값(기본값)으로 설정하면 **RCU_SOFTIRQ** 가 기본적으로 사용됩니다. **rcuc kthreads**를 사용하려면 **rcutree.use_softirq=0** 을 지정합니다.

split_lock_detect = [X86]

이 매개 변수는 분할 잠금 탐지를 활성화합니다. 활성화되고 하드웨어 지원이 있는 경우 캐시 라인 경계에서 데이터에 액세스하는 원자성 지침으로 인해 정렬 확인 예외가 발생합니다.

옵션은 다음과 같습니다.

- **off** - 활성화되지 않음
- **경고** - 커널이 **Alignment Check Exception(#AC)**을 트리거하는 애플리케이션에 대한 속도 제한 경고를 발송합니다. 이 모드는 분할 잠금 탐지를 지원하는 **CPU**의 기본값입니다.
- **치명적** - 커널은 **#AC** 예외를 트리거하는 애플리케이션에 버스 오류(**SIGBUS**) 신호를 보냅니다.

사용자 모드에서 실행하지 않는 동안 **#AC** 예외가 충돌하면 커널은 경고 또는 치명적인 모드에서 **oops** 오류를 실행합니다.

srbds = [X86,INTEL]

이 매개 변수는 **SRBDS(Special Register Buffer Data Sampling)** 완화를 제어합니다.

특정 CPU는 MDS(Microarchitectural Data Sampling)에 취약하여 임의 번호 생성기로부터 비트를 누출할 수 있습니다.

기본적으로 마이크로코드는 이 문제를 완화합니다. 그러나 마이크로 코드 수정으로 RDRAND 및 RDSEED 명령이 훨씬 느려질 수 있습니다. 이로 인해 urandom 커널 임의 소스 장치에서 처리량이 줄어듭니다.

마이크로 코드 완화를 비활성화하려면 다음 옵션을 설정합니다.

- **off** - 완화를 비활성화하고 RDRAND 및 RDSEED에 대한 성능 영향을 제거

svm = [PPC]

형식: { on | off | y | n | 1 | 0 }

이 매개변수는 pSeries 시스템에서 보호된 실행 기능 사용을 제어합니다.

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

이 매개변수는 PV 최적화를 비활성화하여 게스트가 PV 드라이버 없이 일반 게스트로 실행되도록 합니다.

현재 지원되는 XEN HVM, KVM, HYPER_V 및 VMWARE 게스트.

업데이트된 커널 매개변수

hugepagesz = [HW]

이 매개변수는 대규모 페이지 크기를 지정합니다. 지정된 크기의 대규모 페이지를 미리 할당하려면 hugepages 매개변수와 함께 이 매개변수를 사용합니다.

다음과 같이 hugepagesz 및 hugepages 매개변수를 쌍으로 지정합니다.

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

hugepagesz 매개변수는 특정 대규모 페이지 크기에 대해 명령줄에서 한 번만 지정할 수 있습니다. 유효한 대규모 페이지 크기는 아키텍처에 따라 다릅니다.

hugepages = [HW]

이 매개 변수는 사전 할당할 대규모 페이지 수를 지정합니다. 이 매개 변수는 일반적으로 유효한 **hugepagesz** 또는 **default_hugepagesz** 매개 변수를 따릅니다.

그러나 **hugepages** 가 첫 번째 또는 유일한 **HugeTLB** 명령줄 매개 변수인 경우 할당할 기본 크기의 대규모 페이지 수를 암시적으로 지정합니다. 기본 크기의 대규모 페이지 수를 암시적으로 지정하는 경우 기본 크기에 대한 **hugepagesz + hugepages** 매개변수 쌍으로 덮어쓸 수 없습니다.

예를 들어 **2M**의 기본 대규모 페이지 크기가 있는 아키텍처에서 다음을 수행합니다.

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

위의 예에서 설정하면 **256 2M** 대규모 페이지가 할당되고 **hugepages=512** 매개 변수가 무시된 경고 메시지가 표시됩니다. **hugepages** 앞에 잘못된 **hugepages z** 가 있으면 **hugepages** 가 무시됩니다.

default_hugepagesz = [HW]

이 매개 변수는 기본 대규모 페이지 크기를 지정합니다. 명령행에서 **default_hugepagesz** 를 한 번만 지정할 수 있습니다. 선택적으로 **default_hugepagesz** 를 **hugepages** 매개 변수로 따라 기본 크기의 특정 대규모 페이지 수를 사전 할당할 수 있습니다. 또한 사전 할당할 기본 대규모 페이지 수를 암시적으로 지정할 수 있습니다.

예를 들어 **2M**의 기본 대규모 페이지 크기가 있는 아키텍처에서 다음을 수행합니다.

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

위의 예제의 설정은 모두 **256 2M** 대규모 페이지를 할당합니다. 유효한 기본 대규모 페이지 크기는 아키텍처에 따라 다릅니다.

efi = [EFI]

Format: { "old_map", "nochunk", "noruntime", "debug", "nosoftreserve" }

옵션은 다음과 같습니다.

- **old_map [X86-64]** - 기존의 **ioremap** 기반 **EFI** 런타임 서비스 매핑으로 전환합니다. 32 비트는 기본적으로 이 파일을 계속 사용합니다.

- **nochunk** - 일부 펌웨어 구현에서 문제를 일으킬 수 있으므로 **EFI** 부트 스텝의 "체크"에서 파일을 읽지 않도록 설정할 수 있습니다.
- **noruntime** - **EFI** 런타임 서비스 지원 비활성화
- **debug** - 기타 디버그 출력 활성화
- **nosoftreserve** - **EFI_MEMORY_SP** (특정 용도) 속성으로 인해 커널이 메모리 매핑 드라이버의 메모리 범위를 클레임하는 경우가 있습니다. 이 예약을 비활성화하고 기본 유형(예: **EFI_CONVENTIONAL_MEMORY** / "System RAM")으로 메모리를 처리하려면 **efi=nosoftreserve** 를 지정합니다.

intel_iommu = [DMAR]

Intel IOMMU 드라이버 **DMAR**(Direct Memory Access Remapping).

추가 옵션은 다음과 같습니다.

- **nobounce** (기본값 끄기) - **HFS** 장치와 같은 신뢰할 수 없는 장치에 대해 바운스 버퍼 비활성화. 이렇게 하면 신뢰할 수 없는 장치를 신뢰할 수 있는 장치로 처리합니다. 따라서 이 설정은 **DMA**(직접 메모리 액세스) 공격의 보안 위험을 초래할 수 있습니다.

mem = nn[KMG] [KNL, BoOT]

이 매개 변수는 특정 메모리 양을 강제로 사용합니다.

사용할 메모리 양은 다음과 같습니다.

1. 테스트용.
2. 커널이 전체 시스템 메모리를 볼 수 없는 경우.
3. 하이퍼바이저에서 **mem** 경계를 제외한 후 **KVM** 게스트에 할당된 메모리입니다.

[X86] 최대 주소 제한으로 작업합니다. 물리적 주소 공간 충돌을 방지하려면 **memmap**

매개변수와 함께 를 사용합니다. **memmap** 이 없으면 **PCI(Peripheral Component Interconnect)** 장치를 사용하지 않는 **RAM**에 속하는 주소에 배치할 수 있었습니다.

위의 경우 3번의 경우 하이퍼바이저의 시스템 메모리가 충분하지 않은 경우 부팅 후 메모리를 핫으로 추가해야 하므로 이 설정은 부팅 시에만 적용됩니다.

pci = [PCI]

다양한 **PCI(Peripheral Component Interconnect)** 하위 시스템 옵션.

여기에서 일부 옵션은 특정 장치 또는 장치 집합(<pci_dev>)에서 작동합니다. 다음 형식 중 하나로 지정됩니다.

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

첫 번째 형식은 새 하드웨어가 삽입되거나 마더보드 펌웨어가 변경되거나 다른 커널 매개 변수로 인한 변경으로 인해 변경될 수 있는 **PCI** 버스/장치/기능 주소를 지정합니다. 도메인이 지정되지 않은 경우 0이 됩니다. 또는 기본 주소 이후에 여러 장치/기능 주소를 통해 장치의 경로를 지정할 수 있습니다(문제의 번호 변경에 대해 더 강력함). 두 번째 형식은 구성 공간의 **ID**를 사용하여 시스템의 여러 장치와 일치할 수 있는 장치를 선택합니다.

옵션은 다음과 같습니다.

- **hpmniosize** - 핫플러그 브리지의 메모리 매핑 I/O(MMIO) 창에 예약된 고정된 버스 공간입니다. 기본 크기는 **2MB**입니다.
- **hpmmioprefsize** - 핫플러그 브리지의 **MMIO_PREF** 창을 위해 예약된 고정된 버스 공간 기본 크기는 **2MB**입니다.

pcie_ports = [PCIE]

PCle(Wear Component Interconnect Express) 포트 서비스 처리.

옵션은 다음과 같습니다.

- **네이티브** - 플랫폼이 OS에서 사용할 수 있는 권한을 제공하지 않아도 기본 **PCle** 서비스(**PME**, **AER**, **DPC**, **PCle** 핫플러그) 사용. 플랫폼에서 이러한 서비스를 사용하려는 경우에도

이러한 설정이 충돌할 수 있습니다.

- **DPC -native - DPC**에만 기본 **PCIe** 서비스를 사용합니다. 펌웨어가 **AER** 또는 **DPC**를 사용하는 경우 이러한 설정이 충돌할 수 있습니다.
- **Compat - 기본 PCIe 서비스(PME, AER, DPC, PCIe 핫플러그)**를 비활성화합니다.

rcu_nocbs = [KNL]

인수는 **CPU** 목록입니다. 문자열 "**all**"을 사용하여 시스템의 모든 **CPU**를 지정할 수 있습니다.

usbcore.authorized_default = [USB]

기본 **USB** 장치 권한 부여.

옵션은 다음과 같습니다.

- **-1 (기본값) - 무선 USB를 제외하고 인증됨**
- **0 - 인증되지 않음**
- **1 - 인증됨**
- **2 - 장치가 내부 포트에 연결된 경우 인증**

usbcore.old_scheme_first = [USB]

이 매개 변수를 사용하면 이전 장치 초기화 스키마로 시작할 수 있습니다. 이 설정은 낮음 및 전체 속도 장치에만 적용됩니다(기본값 **0** = 꺼짐).

usbcore.quirks = [USB]

기본 제공 **USB** 코어 **quirk** 목록을 보강하는 **quirk** 항목 목록입니다. 목록 항목은 쉼표로 구분됩니다. 각 항목에는 **VendorID:ProductID:Flags**(예: **quirks=0781:5580:bk,0a5c:5834:gij**) 형식이 있습니다. **ID**는 4자리 16진수이고 플래그는 문자 집합입니다. 각 문자는 내장된 **quirk**를 변경하고, 명확하고 설정된 경우 이를 지웁니다.

추가된 플래그:

- - o - **USB_QUIRK_HUB_SLOW_RESET**, 포트를 재설정 한 후 허브가 추가 지연이 필요합니다

새로운 **/proc/sys/fs** 매개변수

protected_fifos

이 매개 변수는 **Openwall** 소프트웨어의 제한 사항을 기반으로 하며, 프로그램이 일반 파일을 만들려는 공격자가 제어하는 **FIFO**에 의도하지 않은 쓰기를 방지할 수 있도록 함으로써 보호를 제공합니다.

옵션은 다음과 같습니다.

- - 0 - **FIFO**에게 쓰기는 제한되지 않습니다.
- - 1 - 디렉터리 소유자가 소유하지 않는 한 세계 쓰기 가능한 고정 디렉터리에서 소유하지 않는 **FIFO**에 **O_CREAT** 플래그를 열도록 허용하지 않습니다.
- - 2 - 쓰기 가능한 **Sticky** 디렉토리에 적용됩니다.

protected_regular

이 매개 변수는 **protected_fifos** 매개변수와 비슷하지만, 프로그램을 생성하려는 공격자가 제어하는 정규 파일에 쓰기를 방지할 수 있습니다.

옵션은 다음과 같습니다.

- - 0 - 일반 파일에 쓰는 것은 제한되지 않습니다.
- - 1 - 디렉터리 소유자가 소유하지 않는 한 **world writable sticky directory**에 소유하지 않는 일반 파일에서 **O_CREAT** 플래그를 열도록 허용하지 않습니다.
- - 2 - 쓰기 가능한 **Sticky** 디렉토리에 적용됩니다.

5.3. 장치 드라이버

5.3.1. 새 드라이버

네트워크 드라이버

- **KvaserCAN/DVD 장치용 JDK 드라이버 (kvaser_usb.ko.xz)**
- **Theob natural Systems UCAN 장치 드라이버 (ucan.ko.xz)**
- **Pensando 이더넷 NIC 드라이버 (ionic.ko.xz)**

그래픽 드라이버 및 기타 드라이버

- **일반 원격 프로세서 프레임워크(remoteproc.ko.xz)**
- **패키지 Intel® CPU에 대한 레벨 C 상태 Idle 주입(intel_powerclamp.ko.xz)**
- **X86 PKG TEMP Thermal Driver (x86_pkg_temp_thermal.ko.xz)**
- **INT3402 열 드라이버 (int3402_thermal.ko.xz)**
- **ACPI INT3403 제거 드라이버 (int3403_thermal.ko.xz)**
- **Intel® acpi jboss rel misc dev 드라이버 (acpi_thermal_rel.ko.xz)**
- **INT3400 Thermal 드라이버 (int3400_thermal.ko.xz)**
- **Intel® INT340x 일반적인 온도 영역 처리기 (int340x_thermal_zone.ko.xz)**
- **프로세서 Thermal Reporting Device Driver (processor_thermal_device.ko.xz)**

- **Intel® PCH Thermal 드라이버 (intel_pch_thermal.ko.xz)**
- **gem ttm helpers (drm_ttm_helper.ko.xz)**
- **cec 드라이버의 장치 노드 등록 (cec.ko.xz)**
- **Fairchild F302 Type-Cœ Driver (fusb302.ko.xz)**
- **VHOST IOTLB (vhost_iotlb.ko.xz)**
- **virtio를 위한 vDPA 기반 vhost 백엔드(vhost_vdpa.ko.xz)**
- **VMware 가상 PTP 클록 드라이버 (ptp_vmw.ko.xz)**
- **Intel® LPSS PCI 드라이버 (intel-lpss-pci.ko.xz)**
- **Intel® LPSS 코어 드라이버 (intel-lpss.ko.xz)**
- **Intel® LPSS ACPI 드라이버 (intel-lpss-acpi.ko.xz)**
- **Mellanox 워치독 드라이버 (HTMLx_wdt.ko.xz)**
- **Mellanox FAN 드라이버 (kubexreg-fan.ko.xz)**
- **Mellanox regmap I/O 액세스 드라이버 (kubexreg-io.ko.xz)**
- **Intel® 속도 선택 인터페이스 pci 사서함 드라이버 (isst_if_mbox_pci.ko.xz)**

- **Intel® 속도 선택 인터페이스 사서함 드라이버 (isst_if_mbox_msr.ko.xz)**
- **Intel® 속도 선택 인터페이스 mmio 드라이버 (isst_if_mmio.ko.xz)**
- **Mellanox regmap 드라이버 (leds-mlxreg.ko.xz)**
- **vDPA 장치 시뮬레이터 (vdpa_sim.ko.xz)**
- **Intel® Tiger Lake PCH pinctrl/GPIO 드라이버 (pinctrl-tigerlake.ko.xz)**
- **PXA2x SSP SPI 컨트롤러 (spi-pxa2xx-platform.ko.xz)**
- **PXA 드라이버용 CE4100/LPSS PCI-SPI 본딩 코드 (spi-pxa2xx-pci.ko.xz)**
- **Hyper-V PCI 인터페이스 (pci-hyperv-intf.ko.xz)**
- **virtio 장치용 vDPA 버스 드라이버 (virtio_vdpa.ko.xz)**

5.3.2. 업데이트된 드라이버

네트워크 드라이버 업데이트

- **VMware vmxnet3 가상 NIC 드라이버 (vmxnet3.ko.xz)가 버전 1.5.0.0-k로 업데이트되었습니다.**
- **Realtek RTL8152/RTL8153 기반 USB 이더넷 어댑터 (r8152.ko.xz)가 버전 1.09.10으로 업데이트되었습니다.**
- **Broadcom BCM573xx 네트워크 드라이버 (bnxt_en.ko.xz)가 1.10.1 버전으로 업데이트되었습니다.**
- **NFS(Netronome Flow Processor) 드라이버 (nfp.ko.xz)가 4.18.0-240.el8.x86_64로 업데이트**

트되었습니다.

- **Intel® Ethernet Switch Host Interface Driver(fm10k.ko.xz)**가 0.27.1-k 버전으로 업데이트되었습니다.
- **Intel® Ethernet Connection E800 Series Linux Driver(ice.ko.xz)**가 버전 **redhat.2-k**로 업데이트되었습니다.

스토리지 드라이버 업데이트

- **Emulex LightPulse Fibre Channel SCSI 드라이버(lpfc.ko.xz)**가 버전 **0:12.8.0.1**로 업데이트되었습니다.
- **Qlogic FCoE Driver(bnx2fc.ko.xz)**가 버전 **2.12.13**으로 업데이트되었습니다.
- **LSI MPT Fusion SAS 3.0 장치 드라이버(mpt3sas.ko.xz)**가 **34.100.00.00** 버전으로 업데이트되었습니다.
- **HP Smart Array Controller 버전(hpsa.ko.xz)**용 드라이버가 버전 **3.4.20-170-RH5**로 업데이트되었습니다.
- **Qlogic 파이버 채널 HBA 드라이버(qla2xxx.ko.xz)**가 버전 **10.01.00.25.08.3-k**로 업데이트되었습니다.
- **BroadcomRAID SAS Driver(megaraid_sas.ko.xz)**가 버전 **07.714.04.00-rh1**로 업데이트되었습니다.

그래픽 및 기타 드라이버 업데이트

- **VMware SVGA 장치(vmwgfx.ko.xz)**용 독립형 **drm** 드라이버가 버전 **2.17.0.0**으로 업데이트되었습니다.
- **Chelsio Terminator 카드용 crypto Co-processor. (chcr.ko.xz)**가 버전 **1.0.0.0-ko**로 업데이트되었습니다.

5.4. 버그 수정

이 부분에서는 사용자에게 중요한 영향을 미치는 **Red Hat Enterprise Linux 8.3**에서 수정된 버그에 대해 설명합니다.

5.4.1. 설치 프로그램 및 이미지 생성

RHEL 8 초기 설정이 **SSH**를 통해 올바르게 작동합니다.

이전에는 **SSH**를 사용하여 시스템에 로그인할 때 **RHEL 8** 초기 설정 인터페이스가 표시되지 않았습다. 그 결과 **SSH**를 통해 관리되는 **RHEL 8** 시스템에서 초기 설정을 수행할 수 없었습니다. 이 문제는 해결되었으며 이제 **SSH**를 통해 수행될 때 **RHEL 8** 초기 설정이 올바르게 작동합니다.

([BZ#1676439](#))

reboot --kexec 명령을 사용할 때 설치에 실패했습니다

이전에는 **reboot --kexec** 명령이 포함된 **Kickstart** 파일을 사용할 때 **RHEL 8** 설치에 실패했습니다.

이번 업데이트를 통해 **reboot --kexec** 를 사용한 설치가 이제 예상대로 작동합니다.

([BZ#1672405](#))

미국/뉴욕 시간대를 올바르게 설정할 수 있음

이전에는 대화형 **Anaconda** 설치 프로세스에서 사용자가 **kickstart** 파일을 사용할 때 *미국/뉴욕* 시간대를 설정할 수 없었습니다. 이번 업데이트를 통해 사용자가 킥스타트 파일에 시간대가 지정되지 않은 경우 이제 대화형 설치 프로그램에서 *미국/뉴욕* 을 기본 시간대로 설정할 수 있습니다.

([BZ#1665428](#))

SELinux 컨텍스트가 올바르게 설정되었습니다

이전 버전에서는 **SELinux**가 강제 모드일 때 일부 폴더와 파일의 잘못된 **SELinux** 컨텍스트로 인해 설치 후 이러한 파일에 액세스하려고 할 때 예기치 않은 **AVC** 거부 발생했습니다.

이번 업데이트를 통해 **Anaconda**는 올바른 **SELinux** 컨텍스트를 설정합니다. 결과적으로 파일 시스템의 레이블을 수동으로 다시 지정하지 않고 폴더와 파일에 액세스할 수 있습니다.

(BZ#1775975)

자동 파티셔닝이 유효한 / 부트 파티션을 만듭니다

이전에는 자동 파티션을 사용하거나 미리 구성된 파티션이 포함된 **kickstart** 파일을 사용하여 시스템에 **RHEL**을 설치할 때 설치 프로그램에서 잘못된 **/boot** 파티션을 포함할 수 있는 파티션 스키마를 생성했습니다. 결과적으로 파티션 구성 확인에 실패하여 자동 설치 프로세스가 조기에 종료되었습니다. 이번 업데이트를 통해 **Anaconda**는 유효한 **/boot** 파티션을 포함하는 파티션 스키마를 만듭니다. 결과적으로 자동 설치가 예상대로 완료됩니다.

(BZ#1630299)

바이너리 **DVD ISO** 이미지를 사용한 **GUI** 설치가 **CDN** 등록 없이 성공적으로 완료

이전에는 바이너리 **DVD ISO** 이미지 파일을 사용하여 **GUI** 설치를 수행할 때 설치 프로그램의 경쟁 조건으로 인해 **Connect to Red Hat** 기능을 사용하여 시스템을 등록할 때까지 설치가 진행되지 않았습니다.

이번 업데이트를 통해 이제 **Connect to Red Hat** 기능을 사용하여 시스템을 등록하지 않고 설치를 진행할 수 있습니다.

(BZ#1823578)

Kickstart에서 생성되어 **ignoredisk --only-use** 명령에서 사용하는 **iSCSI** 또는 **FCoE** 장치는 더 이상 설치 프로세스를 중지하지 않습니다

이전에는 **ignoredisk --only-use** 명령에서 **Kickstart**에서 생성된 **iSCSI** 또는 **FCoE** 장치를 사용할 때 **ignoredisk** 명령에 지정된 Disk "**disk/by-id/scsi-360a9800042566643352b476d674a774a**"와 유사한 오류로 설치 프로그램이 실패했습니다. 이로 인해 설치 프로세스가 중지되었습니다.

이번 업데이트를 통해 문제가 해결되었습니다. 설치 프로그램이 계속 작동합니다.

(BZ#1644662)

CDN을 사용한 시스템 등록에 실패했습니다. 오류 메시지 **Name** 또는 **service not known**

CDN(Content Delivery Network)을 사용하여 시스템을 등록하려고 하면 등록 프로세스에서 **Name or service not known** 오류 메시지로 실패했습니다.

이 문제는 비어 있는 **Custom** 서버 **URL** 및 **Custom Base URL** 값이 시스템 등록의 기본값을 덮어쓰기 때문에 발생했습니다.

이번 업데이트를 통해 이제 빈 값이 기본값을 덮어쓰지 않고 시스템 등록이 성공적으로 완료됩니다.

(BZ#1862116)

5.4.2. 소프트웨어 관리

DNF-automatic 이 올바른 **GPG** 서명을 사용하여 패키지만 업데이트

이전에는 업데이트를 수행하기 전에 **dnf-automatic** 구성 파일에서 다운로드한 패키지의 **GPG** 서명을 확인하지 않았습니다. 결과적으로 리포지토리 구성에 **GPG** 서명 확인(**gpgcheck=1**)이 필요한 경우에도 **dnf-automatic** 에서 가져오지 않은 키로 서명되지 않은 업데이트 또는 업데이트를 설치할 수 있습니다. 이번 업데이트를 통해 문제가 수정되었으며 **dnf-automatic** 은 업데이트를 수행하기 전에 다운로드한 패키지의 **GPG** 서명을 확인합니다. 따라서 **GPG** 서명 확인이 필요한 리포지토리에서 올바른 **GPG** 서명이 있는 업데이트만 설치됩니다.

(BZ#1793298)

후행 쉼표로 인해 추가 유형 옵션에서 항목이 제거되지 않습니다

이전 버전에서는 추가 유형 옵션(예: **exclude**, **exclude pkgs**, **includepkgs**)에 후행 쉼표(목록 끝에 빈 항목)를 추가하면 옵션의 모든 항목이 제거되었습니다. 또한 쉼표 2개(빈 항목)를 추가하면 쉼표 뒤에 만 쉼표가 사용되었습니다.

이번 업데이트를 통해 선행 쉼표 이외의 빈 항목(리스트 시작 시 빈 항목)이 무시됩니다. 그 결과 선행 쉼표만 이제 **append type** 옵션에서 기존 항목을 제거하므로 사용자는 이 항목을 사용하여 이러한 항목을 덮어쓸 수 있습니다.

(BZ#1788154)

5.4.3. 셸 및 명령행 툴

ReaR 디스크 레이아웃에는 더 이상 **Rancher 2** 장치 **iSCSI** 장치 및 파일 시스템 항목이 포함되지 않습니다.

이번 업데이트에서는 **ReaR**에 의해 생성된 디스크 레이아웃에서 **Rancher 2** 장기 iSCSI 장치 및 파일 시스템에 대한 항목을 제거합니다.

([BZ#1843809](#))

IBM POWER, little endian에서 **4GB** 이상의 파일을 사용하여 복구 이미지 생성 가능

이전에는 **ReaR** 유틸리티에서 **IBM POWER**에서 **little endian** 아키텍처인 **4GB**보다 큰 파일이 포함된 복구 이미지를 생성할 수 없었습니다. 이번 업데이트를 통해 문제가 해결되었으며 이제 **IBM POWER**에서 **little endian**인 **4GB**보다 큰 파일로 복구 이미지를 생성할 수 있습니다.

([BZ#1729502](#))

5.4.4. 보안

SELinux는 **corosync**에서 사용하는 **/dev/shm/** 파일에서 **newfstatat()**를 호출하는 **systemd-journal-gatewayd**를 더 이상 차단하지 않습니다.

이전 버전에서는 **SELinux** 정책에 **systemd-journal-gatewayd** 데몬이 **corosync** 서비스에서 생성한 파일에 액세스할 수 있도록 하는 규칙이 포함되지 않았습니다. 그 결과 **SELinux**는 **systemd-journal-gatewayd**를 거부하여 **corosync**에서 만든 공유 메모리 파일에서 **newfstatat()** 함수를 호출합니다. 이번 업데이트를 통해 **SELinux**는 더 이상 **corosync**에서 만든 공유 메모리 파일에서 **newfstatat()**를 호출하도록 **systemd-journal-gatewayd**를 사용하지 않습니다.

([BZ#1746398](#))

Libreswan은 모든 설정에서 **seccomp=enabled**와 함께 작동합니다

이번 업데이트 이전에는 **Libreswan SECCOMP** 지원의 허용된 **syscall** 세트가 **RHEL** 라이브러리의 새로운 사용과 일치하지 않았습니다. 그 결과 **ipsec.conf** 파일에서 **SECCOMP**를 활성화하면 **syscall** 필터링이 **pluto** 데몬이 제대로 작동하는 데 필요한 **syscall**도 거부했습니다. 데몬이 종료되고 **ipsec** 서비스가 다시 시작되었습니다. 이번 업데이트를 통해 새로 필요한 모든 **syscall**이 허용되었으며 **Libreswan**은 이제 **seccomp=enabled** 옵션에서 올바르게 작동합니다.

([BZ#1544463](#))

SELinux는 더 이상 시스템을 중단하거나 전원을 끄기 위해 **auditd**를 차단하지 않습니다

이전에는 **SELinux** 정책에 감사 데몬이 **power_unit_file_t systemd** 장치를 시작할 수 있는 규칙이 없었습니다. 결과적으로 **auditd**는 로깅 디스크 파티션에 남은 공간이 없는 경우와 같은 경우 이를 수행하도

록 구성된 경우에도 시스템을 중지하거나 끌 수 없었습니다.

이번 업데이트에서는 **selinux-policy** 패키지에서 누락된 규칙이 추가되고 **auditd** 는 강제 모드에서 SELinux에서만 시스템을 올바르게 중지하고 전원을 끌 수 있습니다.

(BZ#1826788)

IPTABLES_SAVE_ON_STOP 가 올바르게 작동합니다

이전에는 IP 테이블 내용이 저장된 파일이 잘못된 SELinux 컨텍스트를 수신했기 때문에 **iptables** 서비스의 **IPTABLES_SAVE_ON_STOP** 기능이 작동하지 않았습니다. 이로 인해 **iptables** 스크립트가 권한을 변경하지 못했으며 결과적으로 스크립트에서 변경 사항을 저장하지 못했습니다. 이번 업데이트에서는 **iptables.save** 및 **ip6tables.save** 파일에 대한 적절한 컨텍스트를 정의하고 파일 이름 전환 규칙을 생성합니다. 그 결과 **iptables** 서비스의 **IPTABLES_SAVE_ON_STOP** 기능이 올바르게 작동합니다.

(BZ#1776873)

NSCD 데이터베이스에서 다양한 모드를 사용할 수 있음

the nsswitch_domain 속성의 도메인은 **NSCD**(Name Service Cache Daemon) 서비스에 액세스할 수 있습니다. 각 **NSCD** 데이터베이스는 **nscd.conf** 파일에서 구성되며, **shared** 속성은 데이터베이스에서 공유 메모리 또는 소켓 모드를 사용하는지 여부를 결정합니다. 이전에는 모든 **NSCD** 데이터베이스에서 **nscd_use_shm** 부울 값에 따라 동일한 액세스 모드를 사용해야 했습니다. 이제 **Unix** 스트림 소켓을 사용하는 것이 항상 허용되므로 **NSCD** 데이터베이스가 서로 다른 모드를 사용할 수 있습니다.

(BZ#1772852)

oscap-ssh 유틸리티는 **--sudo**를 사용하여 원격 시스템을 스캔할 때 올바르게 작동합니다.

oscap-ssh 툴을 **--sudo** 옵션과 함께 사용하여 원격 시스템을 **SCAP**(Security Content Automation Protocol) 스캔을 수행할 때 원격 시스템의 **oscap** 툴은 스캔 결과 파일을 저장하고 파일을 **root** 사용자로 임시 디렉터리에 보고합니다. 이전에는 원격 시스템의 **umask** 설정이 변경되면 **oscap-ssh** 가 해당 파일에 대한 액세스 권한이 없을 수 있었습니다. 이번 업데이트에서는 문제가 해결되어 **oscap** 이 파일을 대상 사용자로 저장하고 **oscap-ssh** 는 일반적으로 파일에 액세스합니다.

(BZ#1803116)

OpenSCAP에서 원격 파일 시스템을 올바르게 처리

이전에는 마운트 사양이 두 슬래시로 시작되지 않은 경우 **OpenSCAP**에서 원격 파일 시스템을 안정적

으로 탐지하지 않았습니다. 결과적으로 **OpenSCAP**은 일부 네트워크 기반 파일 시스템을 로컬로 처리했습니다. 이번 업데이트를 통해 **OpenSCAP**는 마운트 사양 대신 **file-system** 유형을 사용하여 파일 시스템을 식별합니다. 결과적으로 **OpenSCAP**에서 원격 파일 시스템을 올바르게 처리합니다.

(BZ#1870087)

OpenSCAP이 더 이상 **YAML** 다중 줄 문자열에서 빈 줄을 제거하지 않음

이전에는 **OpenSCAP**에서 생성된 **Ansible** 해결 방법 내 **YAML** 다중 줄 문자열에서 비어 있는 줄을 데이터 스트림에서 제거했습니다. 이로 인해 **Ansible** 해결에 영향을 미치고 **openscap** 유틸리티가 해당 **OVAL(Open Vulnerability and Assessment Language)** 확인에 실패하여 잘못된 긍정적인 결과가 생성되었습니다. 이제 문제가 해결되어 **openscap**이 더 이상 **YAML** 다중 줄 문자열에서 빈 행을 제거하지 않습니다.

(BZ#1795563)

OpenSCAP에서 메모리가 부족하지 않고 많은 수의 파일이 있는 시스템을 스캔할 수 있음

이전에는 **RAM**이 적고 많은 수의 파일이 있는 시스템을 스캔할 때 **OpenSCAP** 스캐너로 인해 시스템에 메모리가 부족한 경우가 있었습니다. 이번 업데이트를 통해 **OpenSCAP** 스캐너 메모리 관리가 개선되었습니다. 결과적으로 스캐너는 많은 수의 파일을 스캔할 때 **RAM**이 부족한 시스템에서 더 이상 메모리가 부족하지 않습니다(예: **GUI** 및 **Workstation**을 사용한 패키지 그룹 서버).

(BZ#1824152)

config.enabled 이제 설명이 올바르게 제어됩니다.

이전 버전에서는 **rsyslog**가 문을 구성하는 동안 **config.enabled** 지시문을 잘못 평가했습니다. 그 결과 **include ()**를 제외한 각 문에 대해 알 수 없는 오류가 표시되었습니다. 이번 업데이트를 통해 모든 문에 대해 구성이 동일하게 처리됩니다. 결과적으로 **config.enabled**는 오류를 표시하지 않고 문을 올바르게 비활성화하거나 활성화합니다.

(BZ#1659383)

fapolicyd가 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 때문에 애플리케이션을 신뢰할 수 없는 것으로 처리하여 다른 파일을 열고 실행할 수 없었습니다. 그 결과 업데이트를 적용한 후 시스템을 부팅할 수 없는 경우가 있었습니다.

RHBA-2020:5242 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#1897090)

이제 **e8** 프로필을 사용하여 **GUI**를 사용하여 **RHEL 8** 시스템을 해결할 수 있습니다.

OpenSCAP Anaconda 애드온을 사용하여 서버에서 시스템을 강화하여 **GUI** 패키지 그룹을 사용하여 **RPM** 그룹과 무결성 확인에서 규칙을 선택하는 프로필이 있는 **GUI** 패키지 그룹을 사용하면 더 이상 시스템에 극적인 **RAM**이 필요하지 않습니다. 이 문제의 원인은 **OpenSCAP** 스캐너였습니다. 자세한 내용은 **OpenSCAP**로 많은 수의 파일 스캔을 참조하십시오. 이로 인해 시스템에 메모리가 부족합니다. 그 결과, **RHEL 8 Essential Eight(e8)** 프로필을 사용하여 시스템 강화가 이제 **GUI**에서 **Server with GUI**에서도 작동합니다.

(BZ#1816199)

5.4.5. 네트워킹

nft_compat 모듈로 **iptables** 확장 모듈을 자동 로드해도 더 이상 중단되지 않음

이전에는 네트워크 네임스페이스(**netns**)에 대한 작업이 병렬로 수행되는 동안 **nft_compat** 모듈이 확장 모듈을 로드할 때 초기화 중에 **pernet** 하위 시스템을 등록하면 해당 확장에서 잠금 충돌이 발생할 수 있었습니다. 그 결과 커널이라고 하는 **modprobe** 명령이 중단됩니다. 또한 **iptables** 명령을 실행하는 **libvirt**와 같은 다른 서비스로 인해 발생할 수 있습니다. 이 문제는 해결되었습니다. 결과적으로 **nft_compat** 모듈로 **iptables** 확장 모듈을 로드해도 더 이상 중단되지 않습니다.

(BZ#1757933)

서비스가 중지되면 **firewalld** 서비스에서 **ipsets**를 제거합니다.

이전에는 **firewalld** 서비스를 중지해도 **ipsets**가 제거되지 않았습니다. 이번 업데이트에서는 문제가 해결되었습니다. 결과적으로 **firewalld**가 중지된 후 **ipsets**는 더 이상 시스템에 남아 있지 않습니다.

(BZ#1790948)

firewalld는 종료 후 더 이상 **ipset** 항목을 유지하지 않습니다

이전에는 **firewalld**를 종료해도 **ipset** 항목이 제거되지 않았습니다. 그 결과 **firewalld** 서비스를 중지한 후에도 **ipset** 항목이 커널에서 활성 상태로 유지되었습니다. 이번 수정으로 **firewalld**를 종료하면

ipset 항목이 예상대로 제거됩니다.

([BZ#1682913](#))

firewalld 가 다시 로드한 후 **ipset** 항목을 복원합니다

이전에는 **firewalld** 를 다시 로드한 후 런타임 **ipset** 항목이 유지되지 않았습니다. 결과적으로 사용자는 누락된 항목을 수동으로 다시 추가해야 했습니다. 이번 업데이트를 통해 다시 로드한 후 **ipset** 항목을 복원하도록 **firewalld** 가 수정되었습니다.

([BZ#1809225](#))

nftables 및 **firewalld** 서비스가 함께 사용할 수 없습니다.

이전에는 **nftables** 와 **firewalld** 서비스를 동시에 활성화할 수 있었습니다. 그 결과 **nftables** 가 **firewalld** 규칙 세트를 재정의했습니다. 이번 업데이트를 통해 이제 **nftables** 및 **firewalld** 서비스가 상호 배타되어 동시에 활성화할 수 없습니다.

([BZ#1817205](#))

5.4.6. 커널

huge_page_setup_helper.py 스크립트가 올바르게 작동합니다.

Python 3용 **huge_page_setup_helper.py** 스크립트를 업데이트한 패치가 실수로 제거되었습니다. 그 결과 **huge_page_setup_helper.py** 를 실행하면 다음과 같은 오류 메시지가 표시됩니다.

```
SyntaxError: Missing parentheses in call to 'print'
```

이번 업데이트를 통해 **libhugetlbfs.spec** 파일을 업데이트하여 문제가 해결되었습니다. 결과적으로 **huge_page_setup_helper.py** 는 설명된 시나리오에 오류가 표시되지 않습니다.

([BZ#1823398](#))

대량의 영구 메모리 부팅이 시간 초과 없이 더 빠르고 빠른 시스템

메모리가 많은 시스템은 원래 소스 코드가 노드당 하나의 초기화 스레드만 허용했기 때문에 부팅하는 데 시간이 오래 걸렸습니다. 예를 들어 4-노드 시스템의 경우 4개의 메모리 초기화 스레드가 있었습니다. 결과적으로 **/etc/fstab** 파일에 나열된 영구 메모리 파일 시스템이 있는 경우 시스템을 사용할 수 있을 때까지

지 대기하는 동안 시스템이 시간 초과될 수 있었습니다. 이번 업데이트를 통해 소스 코드에서 단일 노드 내에서 여러 메모리 초기화 스레드를 허용할 수 있기 때문에 문제가 해결되었습니다. 결과적으로 시스템이 더 빠르게 부팅되고 설명된 시나리오에 시간 초과가 표시되지 않습니다.

(BZ#1666538)

Bcc 스크립트가 BPF 모듈을 성공적으로 컴파일합니다.

BPF(Berkeley Packet Filter) 모듈을 생성하기 위한 스크립트 코드 컴파일 중에 bcc 툴킷은 데이터 유형 정의에 커널 헤더를 사용했습니다. 일부 커널 헤더에는 **KBUILD_MODNAME** 매크로를 정의해야 했습니다. 결과적으로 **KBUILD_MODNAME** 을 추가하지 않은 bcc 스크립트는 다양한 CPU 아키텍처에서 BPF 모듈을 컴파일하지 못할 가능성이 있었습니다. 다음 bcc 스크립트에 영향을 받았습니다.

- bindsnoop
- sofdsnoop
- solisten
- tcpaccept
- TCPConnect
- tcpconnlst
- tcpdrop
- tcpretrans
- tcpsubnet
- tcptop

•

tcptracer

이번 업데이트를 통해 **bcc**의 기본 **cflags** 매개 변수에 **KBUILD_MODNAME**을 추가하여 문제가 해결되었습니다. 따라서 이 문제는 설명된 시나리오에 더 이상 나타나지 않습니다. 또한 고객 스크립트에서 **KBUILD_MODNAME**을 자체적으로 정의할 필요가 없습니다.

(BZ#1837906)

bcc-tools 및 **bpfftrace**는 IBM Z에서 제대로 작동합니다.

이전에는 기능 백포트에서 **ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE** 커널 옵션을 도입했습니다. 그러나 IBM Z 아키텍처용 **bcc-tools** 패키지 및 **bpfftrace** 추적 언어 패키지는 이 옵션을 올바르게 지원하지 않았습니다. 그 결과 잘못된 인수 예외로 **bpf()** 시스템 호출에 실패했습니다. **bpfftrace**는 **BPF** 프로그램을 로드하려고 할 때 오류 로드 프로그램 오류로 실패했습니다. 이번 업데이트를 통해 이제 **ARCH_HAS_NON_OVERLAPPING_ADDRESS_SPACE** 옵션이 제거되었습니다. 따라서 설명된 시나리오에 더 이상 문제가 나타나지 않습니다.

(BZ#1847837, BZ#1853964)

엔트로피 부족으로 인해 부팅 프로세스가 더 이상 실패하지 않습니다

이전에는 엔트로피 부족으로 인해 부팅 프로세스가 실패했습니다. 이제 더 나은 메커니즘을 사용하여 커널이 하드웨어별 인터럽트에 의존하지 않는 부팅 프로세스 초기에 엔트로피를 수집할 수 있습니다. 이번 업데이트에서는 초기 부팅 시 임의 생성 보안을 위해 충분한 엔트로피의 가용성을 보장하여 문제를 해결합니다. 결과적으로 수정으로 키스타트 시간 초과 또는 느린 부팅이 방지되고 부팅 프로세스가 예상대로 작동합니다.

(BZ#1778762)

kexec를 사용하여 반복 재부팅이 예상대로 작동합니다

이전에는 **Amazon EC2 Nitro** 플랫폼에서 커널 재부팅 중에 커널 실행 경로를 **shutdown()** 호출하는 동안 **remove** 모듈(**rmmod**)이 호출되지 않았습니다. 결과적으로 **kexec** 시스템 호출을 사용하여 반복된 커널이 재부팅되어 오류가 발생했습니다. 이번 업데이트를 통해 안전한 커널 실행을 허용하는 **PCI shutdown()** 핸들러를 추가하여 문제가 해결되었습니다. 결과적으로 **Amazon EC2 Nitro** 플랫폼에서 **kexec**를 사용하여 반복적으로 재부팅할 수 있습니다.

(BZ#1758323)

덤프 대상으로 **vPMEM** 메모리를 사용하여 반복적으로 재부팅할 수 있습니다. 이제 예상대로 작동합니다.

이전 버전에서는 **vPMEM(Virtual Persistent Memory)** 네임스페이스를 **kdump** 또는 **fadump**의 덤프 대상으로 사용하여 **papr_scm** 모듈에서 **vPMEM**에서 지원하는 메모리를 매핑하고 다시 매핑하고 메모리를 선형 맵에 다시 추가했습니다.

그 결과 이 동작으로 인해 **POWER Hypervisor**에 **HCalls(HCalls)**가 트리거되었습니다. 결과적으로 캡처 커널 부팅 속도가 느려지고 덤프 파일을 저장하는 데 시간이 오래 걸립니다. 이번 업데이트에서는 문제가 해결되어 설명된 시나리오에서 부팅 프로세스가 예상대로 작동합니다.

(BZ#1792125)

ICE 드라이버 **NIC** 포트를 모드 5 본딩 마스터 인터페이스에 추가하려고 하면 더 이상 실패하지 않습니다

이전 버전에서는 모드 5(밸런싱)본딩 마스터 인터페이스에 **ICE** 드라이버 **NIC** 포트를 추가하면 **Master 'bond0', Slave 'ens1f0'** 오류가 발생했습니다. 오류: **enslave failed**. 결과적으로 **NIC** 포트를 본딩 마스터 인터페이스에 추가하는 간헐적인 오류가 발생했습니다. 이번 업데이트에서는 문제가 해결되어 인터페이스가 더 이상 실패하지 않습니다.

(BZ#1791664)

cxgb4 드라이버가 더 이상 **kdump** 커널에서 충돌하지 않습니다

이전에는 **vmcore** 파일에 정보를 저장하는 동안 **kdump** 커널이 충돌했습니다. 결과적으로 **cxgb4** 드라이버는 **kdump** 커널이 나중에 분석을 위해 코어를 저장하는 것을 방지했습니다. 이 문제를 해결하려면 핵심 파일을 저장할 수 있도록 **kdump** 커널 명령줄에 **novmcoredd** 매개변수를 추가합니다.

[RHSA-2020:1769](#) 권고가 릴리스되면서 **kdump** 커널은 이 상황을 올바르게 처리하고 더 이상 충돌하지 않습니다.

(BZ#1708456)

5.4.7. 고가용성 및 클러스터

Filesystem 에이전트와 함께 **GFS2** 파일 시스템을 사용하면 **fast_stop** 옵션이 기본적으로 **no**로 설정됩니다.

이전에는 **Filesystem** 에이전트와 함께 **GFS2** 파일 시스템을 사용할 때 **fast_stop** 옵션이 기본적으로 **yes**로 설정되었습니다. 이 값으로 인해 **GFS2** 파일 시스템을 마운트 해제하는 데 걸리는 시간으로 인해 불필요한 펜스 이벤트가 발생할 수 있습니다. 이번 업데이트를 통해 이 옵션은 기본적으로 **no**로 설정됩니다. 다른 모든 파일 시스템의 경우 기본값은 **yes**입니다.

(BZ#1814896)

fence_compute 및 **fence_evacuate** 에이전트가 안전하지 않은 옵션을 더 표준적으로 해석합니다.

이전에는 **fence_compute** 및 **fence_evacuate** 에이전트가 기본적으로 **--insecure** 가 지정된 것처럼 작동했습니다. 이번 업데이트를 통해 컴퓨팅 또는 비우기 서비스에 유효한 인증서를 사용하지 않는 고객은 **CLI**에서 수동으로 실행할 때 **insecure=true** 를 설정하고 **--insecure** 옵션을 사용해야 합니다. 이는 다른 모든 에이전트의 동작과 일치합니다.

(BZ#1830776)

5.4.8. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

libdb에 의한 최적화된 **CPU** 사용

libdb 데이터베이스에 대한 이전 업데이트로 인해 복잡한 스레드에서 과도한 **CPU** 사용량이 발생했습니다. 이번 업데이트를 통해 **CPU** 사용량이 최적화되었습니다.

(BZ#1670768)

do_you_mean Ruby gem에는 더 이상 상용 라이선스가 없는 파일이 포함되어 있지 않습니다.

이전에는 **ruby:2.5** 모듈 스트림에서 사용할 수 있는 **do_you_mean** gem에 상용화되지 않은 라이선스가 있는 파일이 포함되어 있었습니다. 이번 업데이트에서는 영향을 받는 파일이 제거됩니다.

(BZ#1846113)

Nginx 는 이제 **PKCS#11** URI를 통해 하드웨어 보안 토큰에서 서버 인증서를 로드할 수 있습니다.

nginx 웹 서버의 **ssl_certificate** 지시문은 **PKCS#11** 모듈에서 직접 하드웨어 보안 토큰에서 **TLS** 서버 인증서 로드를 지원합니다. 이전에는 **PKCS#11** URI를 통해 하드웨어 보안 토큰에서 서버 인증서를 로드할 수 없었습니다.

(BZ#1668717)

5.4.9. 컴파일러 및 개발 도구

DT_FILTER를 사용하고 생성자가 있는 공유 라이브러리를 로드하는 동안 **glibc** 동적 로더가 더 이상 실패하지 않습니다.

이 업데이트 이전에는 필터와 생성자가 있는 공유 라이브러리를 로드하는 동안 필터로 공유 개체의 동적 로더 구현에 결함이 발생하여 동적 로더가 실패했습니다. 이번 릴리스에서는 이러한 공유 라이브러리를 올바르게 처리하도록 **DT_FILTER(DT_FILTER)**의 동적 로더 구현이 수정되었습니다. 그 결과 동적 로더가 이제 언급된 시나리오에서 예상대로 작동합니다.

(BZ#1812756)

glibc에서 **getmntent()** 목록에서 의사 마운트를 제거할 수 있음

커널에는 사용자 공간에 노출된 테이블에 **automount pseudo-entries**가 포함됩니다. 결과적으로 **getmntent()** API를 사용하는 프로그램은 목록의 일반 마운트와 이러한 의사 마운트를 모두 확인합니다. 의사 마운트는 실제 마운트에 일치하지 않으며 유효한 정보를 포함하지 않습니다.

이번 업데이트를 통해 **mount** 항목에 **automount(8)** 설정에 **ignore** 마운트 옵션이 있는 경우 **glibc** 라이브러리는 이제 **getmntent()** 목록에서 이러한 의사 마운트를 제거합니다. 이전 동작이 예상되는 프로그램은 다른 API를 사용해야 합니다.

(BZ#1743445)

IBM Z에서 **movv1qi** 패턴이 더 이상 자동 검사 코드에서 잘못 컴파일되지 않습니다.

이번 업데이트 이전에는 **movv1qi** 패턴에 대해 잘못된 로드 지침이 생성되었습니다. 그 결과 자동 벡터가 적용된 경우 **IBM Z** 시스템에서 잘못된 컴파일이 발생할 수 있었습니다. 이번 업데이트에서는 **movv1qi** 패턴이 수정되어 결과적으로 코드 컴파일이 수정되어 이제 올바르게 실행됩니다.

(BZ#1784758)

PAPI_event_name_to_code()가 여러 스레드에서 올바르게 작동합니다

이번 업데이트 이전에는 **PAPI** 내부 코드가 스레드 조정을 올바르게 처리하지 않았습니다. 그 결과 여러 스레드가 **PAPI_event_name_to_code()** 작업을 사용하는 경우 경쟁 조건이 발생하고 작업이 실패했습니다. 이번 업데이트에서는 **PAPI** 내부 코드의 여러 스레드 처리가 향상되었습니다. 결과적으로 **PAPI_event_name_to_code()** 작업을 사용하는 다중 스레드 코드가 올바르게 작동합니다.

(BZ#1807346)

IBM Power Systems에서 **glibc** 수학 기능에 대한 성능 개선

이전에는 **glibc** 수학 기능이 **IBM Power Systems**에서 불필요한 부동 소수점 상태 업데이트 및 시스템 호출을 수행했기 때문에 성능에 부정적인 영향을 미쳤습니다. 이번 업데이트에서는 불필요한 부동 소수점 상태 업데이트를 제거하고 다음과 같은 구현을 개선합니다. **ceil()**, **ceilf()**, **fe_getmode()**, **fe_setmode()**, **fe_setenv()**, **fe_getexcept()**, **feenableexcept()**, **fedisableexcept()**, **fe_getround()** 및 **fesetround()**. 그 결과 **IBM Power Systems**에서 수학 라이브러리의 성능이 향상되었습니다.

(BZ#1783303)

메모리 보호 키가 **IBM Power**에서 지원

IBM Power Systems에서 메모리 보호 주요 인터페이스 **pkey_set** 및 **pkey_get** 은 이전에는 스텝 기능이므로 항상 실패했습니다. 이번 업데이트에서는 인터페이스를 구현하고 결과적으로 **GNU C** 라이브러리(**glibc**)에서 **IBM Power Systems**의 메모리 보호 키를 지원합니다.

메모리 보호 키에는 현재 해시 기반 **MMU**(메모리 관리 단위)가 필요하므로 **disable_radix** 커널 매개 변수를 사용하여 특정 시스템을 부팅해야 할 수 있습니다.

(BZ#1642150)

papi-testsuite 및 **papi-devel** 이 필수 **papi-libs** 패키지를 설치합니다.

이전에는 **papi-testsuite** 및 **papi-devel RPM** 패키지가 일치하는 **papi-libs** 패키지에 종속성을 선언하지 않았습니다. 결과적으로 테스트를 실행할 수 없어 개발자에게 애플리케이션에 사용할 수 있는 필수 버전의 **papi** 공유 라이브러리가 없었습니다.

이번 업데이트를 통해 사용자가 **papi-testsuite** 또는 **papi-devel** 패키지를 설치할 때 **papi-libs** 패키지도 설치됩니다. 결과적으로 **papi-testsuite** 에 테스트를 실행할 수 있는 올바른 라이브러리가 있으며 **papi-devel** 을 사용하는 개발자가 실행 파일을 **papi** 공유 라이브러리의 적절한 버전과 연결합니다.

(BZ#1664056)

여러 아키텍처에 **lldb** 패키지를 설치해도 더 이상 파일 충돌이 발생하지 않습니다.

이전에는 **lldb** 패키지가 아키텍처와 독립된 위치에 아키텍처 종속 파일을 설치했습니다. 결과적으로 32비트 및 64비트 버전의 패키지를 모두 설치하면 파일 충돌이 발생했습니다. 이번 업데이트에서는 올바른 아키텍처 종속 위치에 파일을 패키징합니다. 그 결과 설명된 시나리오에 **lldb** 설치가 성공적으로 완료됩니다.

(BZ#1841073)

getaddrinfo 에서 메모리 할당 실패를 올바르게 처리합니다.

이전 버전에서는 메모리 할당 실패 후 **GNU C** 라이브러리 **glibc** 의 **getaddrinfo** 함수에서 내부 확인자 컨텍스트를 릴리스하지 않았습니다. 그 결과 **getaddrinfo** 에서 호출 스레드의 나머지 수명 동안 **/etc/resolv.conf** 파일을 다시 로드할 수 없어 메모리 누수가 발생할 수 있었습니다.

이번 업데이트에서는 확인자 컨텍스트에 대한 추가 릴리스 작업을 사용하여 오류 처리 경로를 수정합니다. 결과적으로 **getaddrinfo** 는 간헐적인 메모리 할당 실패 후에도 새 구성 값으로 **/etc/resolv.conf** 를 다시 로드합니다.

(BZ#1810146)

Glibc 는 **IFUNC** 확인자 순서로 인한 특정 오류를 방지합니다.

이전 버전에서는 **GNU C Library glibc** 의 **librt** 및 **libpthread** 라이브러리 구현에 **clock_gettime**, **clock_getcpuclockid**, **clock_nanosleep**, **clock_settime**, **vfork** 등의 함수에 대한 간접 함수(**IFUNC**) 확인자가 포함되어 있었습니다. 경우에 따라 **IFUNC** 확인자가 **librt** 및 **libpthread** 라이브러리를 재배치하기 전에 실행될 수 있었습니다. 그 결과 초기 프로그램을 시작하는 동안 **glibc** 동적 로더에서 애플리케이션이 실패했습니다.

이번 릴리스에서는 이러한 기능의 구현이 **glibc** 의 **libc** 구성 요소로 이동되어 설명된 문제가 발생하지 않습니다.

(BZ#1748197)

pthread_create 중에 어설션 실패가 더 이상 발생하지 않습니다

이전에는 **glibc** 동적 로더가 내부 스레드 로컬 스토리지(**TLS**) 모듈 ID 카운터의 변경 사항을 롤백하지 않았습니다. 결과적으로 **dlopen** 함수가 특정 방식으로 실패한 후 **pthread_create** 함수의 어설션 오류가 발생할 수 있었습니다. 이번 수정으로 **glibc** 동적 로더는 특정 오류가 더 이상 발생하지 않으면 나중에 **TLS** 모듈 ID 카운터를 업데이트합니다. 결과적으로 어설션 오류가 더 이상 발생하지 않습니다.

(BZ#1774115)

glibc 에서 **nss_db**를 사용하여 32비트 애플리케이션에 대한 올바른 종속성을 설치합니다.

이전에는 **nss_db.x86_64** 패키지에서 **nss_db.i686** 패키지에 대한 종속성을 선언하지 않았습니다. 따

라서 자동 설치되는 32비트 환경의 **glibc.i686**을 설치했지만 시스템에 **nss_db.i686**을 설치하지 않았습니다. 결과적으로 **nss_db**를 사용하는 32비트 애플리케이션은 정확한 사용자 데이터베이스 조회를 수행하지 못하고 동일한 설정의 64비트 애플리케이션이 올바르게 작동합니다.

이번 업데이트를 통해 **glibc** 패키지가 시스템에 **glibc.i686** 및 **nss_db**를 모두 설치할 때 **nss_db.i686** 패키지 설치를 트리거하는 약한 종속성이 추가되었습니다. 결과적으로 시스템 관리자가 **nss_db.i686** 패키지를 명시적으로 설치하지 않은 경우에도 **nss_db**를 사용하는 32비트 애플리케이션이 올바르게 작동합니다.

([BZ#1807824](#))

Odia 언어로 업데이트된 **glibc** 로케일 정보

이전에 오리사로 알려진 인도의 이름은 오디하(**Odisha**)로 바뀌었으며 공식 언어의 이름이 오리야에서 오디아어로 바뀌었습니다. 이번 업데이트를 통해 **glibc** 로케일 정보는 언어의 새 이름을 반영합니다.

([BZ#1757354](#))

LLVM 하위 패키지가 아카이브 종속 위치에 아카이브 종속 파일을 설치합니다

이전에는 **LLVM** 하위 패키지가 아카이브 독립된 위치에 아카이브 종속 파일을 설치했습니다. 이로 인해 32 및 64비트 버전의 **LLVM**을 설치할 때 충돌이 발생했습니다. 이번 업데이트를 통해 이제 패키지 파일이 아카이브 종속 위치에 올바르게 설치되어 버전 충돌이 발생하지 않습니다.

([BZ#1820319](#))

암호 및 그룹 조회가 더 이상 **glibc**에서 실패하지 않습니다

이전에는 **glibc** 라이브러리의 **nss_compat** 모듈에서 암호 및 그룹 항목을 처리하는 동안 잘못된 오류 코드로 **errno** 상태를 덮어씁니다. 이로 인해 애플리케이션에서 버퍼의 크기를 예상대로 조정하지 않아 암호 및 그룹 조회가 실패했습니다. 이번 업데이트에서는 문제가 해결되어 이제 조회가 예상대로 완료됩니다.

([BZ#1836867](#))

5.4.10. IdM (Identity Management)

SSSD는 기본적으로 와일드카드 문자로 모든 규칙을 더 이상 다운로드하지 않습니다

이전에는 `ldap_sudo_include_regexp` 옵션이 기본적으로 `true` 로 잘못 설정되었습니다. 결과적으로 **SSSD**가 **SSSD** 규칙 업데이트 후 또는 **SSSD**에서 `sudoHost` 속성에 와일드카드 문자(*)가 포함된 모든 규칙을 다운로드했습니다. 이번 업데이트에서는 버그가 수정되어 `ldap_sudo_include_regexp` 옵션이 기본적으로 `false` 로 올바르게 설정됩니다. 따라서 설명된 문제가 더 이상 발생하지 않습니다.

(BZ#1827615)

krb5 는 이제 허용된 암호화 유형만 요청합니다.

이전 버전에서는 `default_tgs_enctypes` 또는 `default_tkt_enctypes` 속성이 설정되지 않은 경우 `/etc/krb5.conf` 파일의 `allowed` 암호화 유형에 지정된 암호화 유형이 기본 암호화 유형에 적용되지 않았습니다. 결과적으로 **Kerberos** 클라이언트는 **RC4**와 같이 더 이상 사용되지 않는 암호화 제품군을 요청할 수 있었기 때문에 다른 프로세스가 실패할 수 있었습니다. 이번 업데이트를 통해 `allowed_enctypes` 변수에 지정된 암호화 유형이 기본 암호화 유형에도 적용되고 허용된 암호화 유형만 요청됩니다.

RHEL 8에서 더 이상 사용되지 않는 **RC4** 암호화 제품군은 **AD** 포리스트의 사용자, 서비스 및 신뢰에 대한 기본 암호화 유형입니다.

- **AD** 포리스트의 **AD** 도메인 간 강력한 **AES** 암호화 유형을 지원하려면 **AD DS**를 참조하십시오. 보안: 신뢰할 수 있는 도메인의 리소스에 액세스할 때 **Kerberos** "지원되지 않은 etype" 오류 **Microsoft**.
- **AD**와의 이전 버전과의 호환성을 위해 **IdM** 서버에서 더 이상 사용되지 않는 **RC4** 암호화 유형을 지원하려면 `update-crypto-policies --set DEFAULT:AD-SUPPORT` 명령을 사용합니다.

(BZ#1791062)

KDC가 **LDAP** 백엔드의 암호 수명 정책을 올바르게 적용

이전에는 **Kerberos LDAP** 백엔드가 암호 정책을 잘못 적용했기 때문에 **비IPA Kerberos** 배포 센터 (**KDC**)가 최대 암호 수명이 보장되지 않았습니다. 이번 업데이트를 통해 **Kerberos LDAP** 백엔드가 수정되었으며 암호 라이프사이클이 예상대로 작동합니다.

(BZ#1784655)

SSSD를 사용하여 **AD** 클라이언트에 전송된 암호 만료 알림

이전에는 **Kerberos** 자격 증명을 취득하기 위한 **SSSD** 인터페이스가 최근 변경되어 **SSSD**를 사용하는 **Active Directory** 클라이언트(**IdM**)가 암호 만료 알림이 전송되지 않았습니다.

Kerberos 인터페이스가 업데이트되어 이제 만료 알림이 올바르게 전송됩니다.

([BZ#1820311](#))

간접 **COS** 정의를 사용할 때 디렉터리 서버가 더 이상 메모리를 유출하지 않습니다

이전에는 **COS**(서비스로서의 클래스) 정의를 처리한 후 **Directory Server**에서 간접 **COS** 정의를 사용하는 각 검색 작업에 대해 메모리가 누수되었습니다. 이번 업데이트를 통해 **Directory Server**를 처리한 후 데이터베이스 항목과 관련된 모든 내부 **COS** 구조를 사용할 수 있습니다. 결과적으로 간접 **COS** 정의를 사용할 때 서버에서 더 이상 메모리가 유출되지 않습니다.

([BZ#1816862](#))

AD 사용자의 **ID** 덮어쓰기를 추가하는 것이 **IdM** 웹 **UI**에서 작동합니다.

이전 버전에서는 **IdM** 웹 **UI**를 사용할 때 관리 역할에 대한 액세스 권한을 부여하는 데 실패하기 위해 **Default Trust View**의 **IdM**(Identity Management) 그룹에 **AD**(Active Directory) 사용자가 **ID** 덮어쓰기를 추가했습니다. 이번 업데이트에서는 버그가 수정되었습니다. 결과적으로 이 시나리오에서 웹 **UI**와 **IdM CLI**(명령줄 인터페이스)를 모두 사용할 수 있습니다.

([BZ#1651577](#))

freeraduna는 패키지 설치 중에 더 이상 인증서를 생성하지 않습니다.

이전에는 **FreeRADIUS**에서 패키지를 설치하는 동안 인증서를 생성했기 때문에 다음과 같은 문제가 발생했습니다.

- **Kickstart**를 사용하여 **FreeRADIUS**가 설치된 경우 시스템에 엔트로피가 충분하지 않은 경우 인증서가 생성되어 설치에 실패하거나 보안 인증서가 줄어듭니다.
- 패키지 설치가 대상 시스템이 아닌 빌더 시스템에서 수행되므로 패키지 설치는 컨테이너와 같은 이미지의 일부로 빌드하기 어려웠습니다. 이미지에서 생성된 모든 인스턴스에는 동일한 인증서 정보가 있습니다.
- 인증서를 제거하고 수동으로 다시 생성해야 하므로 최종 사용자가 해당 환경에서 간단한 **VM**을 생성하기가 어려웠습니다.

이번 업데이트를 통해 **FreeRADIUS** 설치가 더 이상 자체 서명된 기본 **CA** 인증서 또는 하위 **CA** 인증서를 생성하지 않습니다. **FreeRADIUS**가 **systemd** 를 통해 시작될 때 :

- 필요한 인증서가 모두 없으면 기본 인증서 집합이 생성됩니다.
- 하나 이상의 예상 인증서가 있는 경우 새 인증서를 생성하지 않습니다.

([BZ#1672285](#))

freeraduna에서 **FIPS** 호환 **Diffie-Hellman** 매개변수 생성

openssl 이 **dhparam** 을 통해 **Diffie-Hellman (dh)** 매개 변수를 생성할 수 없는 새로운 **FIPS** 요구 사항으로 인해 **dh** 매개변수 생성은 **FreeRADIUS** 부트스트랩 스크립트 및 파일에서 제거되었습니다. **rfc3526-group-18-8192.dhparam** 은 모든 시스템의 **FreeRADIUS** 패키지에 포함되어 **FreeRADIUS**가 **FIPS** 모드에서 시작되도록 합니다.

필요한 경우 **/etc/raddb/certs/bootstrap** 및 **/etc/raddb/certs/Makefile** 을 사용자 지정하여 **DH** 매개변수 생성을 복원할 수 있습니다.

([BZ#1859527](#))

이제 상태 점검이 업데이트되어 **ipa-healthcheck-core** 및 **ipa-healthcheck** 가 모두 올바르게 업데이트됩니다.

이전에는 **yum update healthcheck** 를 입력해도 **ipa-healthcheck** 패키지가 업데이트되지 않았지만 **ipa-healthcheck-core** 패키지로 교체되었습니다. 결과적으로 업데이트 후 **ipa-healthcheck** 명령이 작동하지 않았습니다.

이번 업데이트에서는 버그가 수정되어 **ipa-healthcheck** 패키지와 **ipa-healthcheck-core** 패키지 모두 올바르게 업데이트됩니다. 그 결과 업데이트 후 **Healthcheck** 도구가 올바르게 작동합니다.

([BZ#1852244](#))

5.4.11. 그래픽 인프라

하이브리드 **Nvidia GPU**가 있는 랩톱이 이제 일시 중지에서 재개됩니다.

이전에는 **no office** 그래픽 드라이버가 절전 모드의 특정 노트북에서 하이브리드 **Nvidia GPU**를 작동할 수 없는 경우가 있었습니다. 이로 인해 노트북이 일시 중단되지 않았습니다.

이번 업데이트를 통해 런타임 전원 관리(**runpm**) 시스템의 여러 문제가 수정되었습니다. 결과적으로 하이브리드 그래픽이 있는 노트북이 이제 일시 중지에서 재개될 수 있습니다.

(JIRA:RHELPLAN-57572)

5.4.12. 가상화

기본 **CPU** 모델을 사용하여 가상 머신 마이그레이션이 보다 안정적으로 작동합니다.

이전 버전에서는 **VM**(가상 머신)이 특정 **CPU** 모델 없이 생성되면 **QEMU**에서 **libvirt** 서비스에 표시되지 않는 기본 모델을 사용했습니다. 결과적으로 **VM**을 **VM**의 기본 **CPU** 모델을 지원하지 않는 호스트로 마이그레이션하여 마이그레이션 후 게스트 **OS**에서 충돌 및 잘못된 동작이 발생하는 경우가 있었습니다.

이번 업데이트를 통해 **libvirt**는 **VM**의 **XML** 구성에서 **qemu64** 모델을 기본값으로 명시적으로 사용합니다. 결과적으로 사용자가 기본 **CPU** 모델을 사용하여 **VM**을 해당 모델을 지원하지 않는 호스트로 마이그레이션하려고 하면 **libvirt**에서 오류 메시지를 올바르게 생성합니다.

그러나 **Red Hat**은 **VM**에 특정 **CPU** 모델을 사용할 것을 강력히 권장합니다.

(JIRA:RHELPLAN-45906)

5.4.13. 컨테이너

Podman을 사용한 **FIPS** 지원에 대한 참고 사항

FIPS(Federal Information Processing Standard)를 사용하려면 인증된 모듈을 사용해야 합니다. 이전에는 **Podman**이 시작 시 적절한 플래그를 활성화하여 컨테이너에 인증된 모듈을 올바르게 설치했습니다. 그러나 이 릴리스에서 **Podman**은 **FIPS** 시스템 전체의 **crypto-policy** 형태로 시스템에서 일반적으로 제공하는 추가 애플리케이션 도우미를 올바르게 설정하지 않습니다. 인증된 모듈에는 시스템 전체의 **crypto-policy**를 설정할 필요가 없지만 호환 방식으로 **crypto** 모듈을 사용하는 애플리케이션의 능력을 향상합니다. 이 문제를 해결하려면 다른 애플리케이션 코드가 실행되기 전에 **update-crypto-policies --set FIPS** 명령을 실행하도록 컨테이너를 변경합니다. 이 수정에서는 **update-crypto-policies --set FIPS** 명령이 더 이상 필요하지 않습니다.

(BZ#1804193)

5.5. 기술 프리뷰

다음 부분에서는 **Red Hat Enterprise Linux 8.3**에서 사용할 수 있는 모든 기술 프리뷰 목록을 제공합니다.

기술 프리뷰 기능에 대한 **Red Hat** 지원 범위 내용은 [기술 프리뷰 기능 지원 범위](#)를 참조하십시오.

5.5.1. 네트워킹

xt_u32 Netfilter 모듈 활성화

이제 **kernel-modules-extra rpm**에서 **xt_u32 Netfilter** 모듈을 사용할 수 있습니다. 이 모듈은 다른 프로토콜 기반 패킷 필터에 액세스할 수 없는 데이터를 기반으로 패킷 전달을 지원하므로 **nftables**로 수동 마이그레이션을 쉽게 수행할 수 있습니다. 그러나 **xt_u32 Netfilter** 모듈은 **Red Hat**에서 지원하지 않습니다.

(BZ#1834769)

NMState 를 기술 프리뷰로 사용 가능

NMState는 호스트에 대한 네트워크 **API**입니다. 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. **XDP**와 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. **KTLS**는 **AES-GCM** 암호화를 위한 커널에서 대칭 암호화 또는 암호 해독 알고리즘을 사용하여 **TLS** 레코드를 처리합니다. 또한 **KTLS**는 이 기능을 지원하는 **NIC(네트워크 인터페이스 컨트롤러)**로 **TLS** 레코드 암호화를 오프로드하는 인터페이스를 제공합니다.

(BZ#1570255)

기술 프리뷰로 사용 가능한 **XDP** 기능

Red Hat은 다음 **XDP(eXpress Data Path)** 기능을 지원되지 않는 기술 프리뷰로 사용합니다.

- **AMD** 및 **Intel 64비트**가 아닌 아키텍처에 **XDP** 프로그램 로드. **AMD** 및 **Intel 64비트** 이외의 아키텍처에는 **libxdp** 라이브러리를 사용할 수 없습니다.
- **XDP_TX** 및 **XDP_REDIRECT** 반환 코드.
- **XDP** 하드웨어 오프로딩. 이 기능을 사용하기 전에 **nfp** 드라이버를 사용하는 **Netronome** 네트워크 카드에서 **XDP** 프로그램 언로드를 참조하십시오.

(BZ#1889737)

act_mpls 모듈에서 기술 프리뷰로 사용 가능

act_mpls 모듈은 **kernel-modules-extra rpm**에서 기술 프리뷰로 사용할 수 있습니다. 이 모듈을 사용하면 **Traffic Control(TC)** 필터(예: **TC** 필터를 사용하여 푸시 및 팝업 **MPLS** 레이블 스택 항목) 필터를 사용하는 **MPLS(Multiprotocol Label Switching)** 작업을 적용할 수 있습니다. 이 모듈은 또한 **Label(레이블)**, **Traffic Class(트래픽 클래스)**, **Bottom of Stack(스택의 하단)** 및 **Time To Live(라이브 간 시간)** 필드를 독립적으로 설정할 수 있습니다.

(BZ#1839311)

다중 경로 TCP를 기술 프리뷰로 사용 가능

TCP에 대한 확장인 다중 경로 TCP(MPTCP)를 이제 기술 프리뷰로 사용할 수 있습니다. MPTCP는 네트워크 내의 리소스 사용량을 개선하고 네트워크 오류에 대한 복원력을 향상시킵니다. 예를 들어 RHEL 서버에서 Multipath TCP를 사용하면 MPTCP v1이 활성화된 스마트폰이 서버에서 실행 중인 애플리케이션에 연결하고 서버와의 연결을 중단하지 않고 Wi-Fi와 모바일 네트워크 간에 전환할 수 있습니다.

서버에서 실행되는 애플리케이션은 기본적으로 MPTCP를 지원하지거나 관리자가 eBPF 프로그램을 커널에 로드하여 IPPROTO_TCP를 IPPROTO_MPTCP 로 동적으로 변경해야 합니다.

자세한 내용은 [Multipath TCP 시작하기](#)를 참조하십시오.

(JIRA:RHELPLAN-41549)

systemd-resolved 서비스를 기술 프리뷰로 사용 가능

systemd 확인 서비스는 로컬 애플리케이션에 대한 이름 확인을 제공합니다. 이 서비스는 캐싱을 구현하고 DNS 스텝 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)

5.5.2. 커널

kexec 빠른 재부팅 기능은 기술 프리뷰로 사용할 수 있습니다.

kexec 빠른 재부팅 기능은 기술 프리뷰로 계속 사용할 수 있습니다. kexec 빠른 재부팅 으로 커널이 BIOS(Basic Input/Output System)를 통과하지 않고 두 번째 커널로 직접 부팅할 수 있어 부팅 프로세스가 훨씬 빨라집니다. 이 기능을 사용하려면 다음을 수행합니다.

1.

kexec 커널을 수동으로 로드합니다.

2.

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 컴파일 작업을 사용하여 기본 머신 코드로 변환됩니다. **bpf()** **syscall**은 **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 활용하는 고급 추적 언어인 **bpftool**.
- **AF_XDP**: 패킷 처리 성능 우선 순위를 지정하는 애플리케이션의 사용자 공간에 **eXpress Data Path(XDP)** 경로를 연결하는 소켓입니다.

([BZ#1559616](#))

RHEL 8의 기술 프리뷰로 사용 가능한 **igc** 드라이버

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

(BZ#1495358)

soft-RoCE를 기술 프리뷰로 이용 가능

RoCE(Remote Direct Memory Access) over Converged Ethernet (RoCE)는 이더넷을 통해 **RDMA**를 구현하는 네트워크 프로토콜입니다. 소프트 로빈은 **RoCE v1** 및 **RoCE v2**의 두 프로토콜 버전을 지원하는 **RoCE**의 소프트웨어 구현입니다. **soft-RoCE** 드라이버인 **rdma_rxe**는 **RHEL 8**에서 지원되지 않는 기술 프리뷰로 사용할 수 있습니다.

(BZ#1605216)

5.5.3. 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/TCP 대상 기술 프리뷰는 테스트 목적으로만 포함되며 현재는 완전 지원을 위해 계획되어 있지 않습니다.

(BZ#1696451)

ext4 및 **XFS**에서 기술 프리뷰로 파일 시스템 **DAX** 사용 가능

Red Hat Enterprise Linux 8에서 **DAX** 파일 시스템은 기술 프리뷰로 사용할 수 있습니다. **DAX**는 애플리케이션이 영구 메모리를 주소 공간으로 직접 매핑할 수 있는 수단을 제공합니다. **DAX**를 사용하려면 시스템에 몇 가지 형태의 영구 메모리를 사용할 수 있어야 합니다. 일반적으로 하나 이상의 비**Volat**ile 듀얼 인라인 메모리 모듈(**NVDIMM**) 형식이며 **DAX**를 지원하는 파일 시스템은 **NVDIMM**에서 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-ROM**과 같은 파일 시스템 이미지를 공유할 수 있습니다.

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 **OverlayFS**에 완전 지원을 사용할 수 있습니다.

- **Overlayfs**는 컨테이너 엔진 그래프 드라이버로만 사용됩니다. 이 용도는 영구저장장치가 아닌 컨테이너 **COW** 콘텐츠에만 지원됩니다. 비**OverlayFS** 볼륨에 영구 스토리지를 배치해야 합니다. 기본 컨테이너 엔진 구성만 사용할 수 있습니다. 1 레벨의 오버레이, 한 개의 하위 디렉토리, 하위 수준 및 상위 수준은 모두 동일한 파일 시스템에 있습니다.

- 현재 **XFS**만 더 낮은 계층 파일 시스템으로 사용하도록 지원됩니다.

또한 **OverlayFS**를 사용하는 경우 다음 규칙과 제한 사항이 적용됩니다.

- **OverlayFS** 커널 **ABI** 및 사용자 공간 동작은 안정적이지 않으며 향후 업데이트가 변경될 수 있습니다.
- **Overlayfs**는 **POSIX** 표준의 제한된 집합을 제공합니다. **OverlayFS**를 사용하여 배포하기 전에 애플리케이션을 철저히 테스트합니다. 다음 사례는 **POSIX**와 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 8**에서 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.

- 기존 **XFS** 파일 시스템이 오버레이로 사용할 수 있는지 여부를 확인하려면 다음 명령을 사용하여 **ftype=1** 옵션이 활성화되어 있는지 확인합니다.

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

- **SELinux** 보안 레이블은 **OverlayFS**를 사용하여 지원되는 모든 컨테이너 엔진에서 기본적으로 활성화됩니다.
- 이번 릴리스에서는 **OverlayFS**와 관련된 여러 가지 알려진 문제가 있습니다. 자세한 내용은 **Linux** 커널 설명서의 *비표준 동작*을 참조하십시오 .
<https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt>.

OverlayFS에 대한 자세한 내용은 **Linux** 커널 설명서
<https://www.kernel.org/doc/Documentation/filesystems/overlayfs.txt> 를 참조하십시오.

(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 썬 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](#).

RHEL 8.3은 **Stratis**를 버전 **2.1.0**으로 업데이트합니다. 자세한 내용은 [Stratis 2.1.0 릴리스 정보를 참조하십시오](#).

(JIRA:RHELPLAN-1212)

IdM에서 **IdM** 도메인 멤버에서 기술 프리뷰로 **Samba** 서버 설정 지원

이번 업데이트를 통해 **IdM(Identity Management)** 도메인 멤버에 **Samba** 서버를 설정할 수 있습니다. 동일한 패키지에서 제공하는 새로운 **ipa-client-samba** 유틸리티는 **Samba**별 **Kerberos** 서비스 주체를 **IdM**에 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 **Samba**를 설정할 수 있습니다.

IdM Trust 컨트롤러가 글로벌 카탈로그 서비스를 지원하지 않기 때문에 **AD-Enrolled Windows** 호스트는 **Windows**에서 **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)

5.5.4. 고가용성 및 클러스터

pcs cluster setup 명령의 로컬 모드 버전 기술 프리뷰로 사용 가능

기본적으로 **pcs cluster setup** 명령은 모든 구성 파일을 클러스터 노드에 자동으로 동기화합니다.

Red Hat Enterprise Linux 8.3에서 **pcs cluster setup** 명령은 **--corosync-conf** 옵션을 기술 프리뷰로 제공합니다. 이 옵션을 지정하면 명령이 로컬 모드로 전환됩니다. 이 모드에서 **pcs** 는 **corosync.conf** 파일을 생성하여 다른 노드와 통신하지 않고 로컬 노드의 지정된 파일에만 저장합니다. 이렇게 하면 스크립트에 **corosync.conf** 파일을 생성하고 스크립트를 통해 해당 파일을 처리할 수 있습니다.

(BZ#1839637)

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 Hat**은 **Red Hat Openstack**을 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, 네트워크 업링크에 도달하는 데 문제가 있는 경우 노드에서 서비스를 인계받는 것이 적절하지 않을 수 있으며, 이러한 경우 라우터에 대한 **ping**이 탐지될 수 있는 클라이언트에서 서비스에 연결할 수 없습니다.

(BZ#1775847)

5.5.5. 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)을 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 명령 방식에 따라 구성되지 않은 DNS 영역의 가용성에 영향을 줄 수 있습니다.

(BZ#1664718)

5.5.6. 데스크탑

64비트 ARM 아키텍처용 GNOME을 기술 프리뷰로 사용 가능

이제 64비트 ARM 아키텍처에서 기술 프리뷰로 GNOME 데스크탑 환경을 사용할 수 있습니다. 이를 통해 관리자는 VNC 세션을 사용하여 원격으로 GUI(그래픽 사용자 인터페이스)에서 서버를 구성하고 관리할 수 있습니다.

결과적으로 64비트 ARM 아키텍처에서 새 관리 애플리케이션을 사용할 수 있습니다. 예를 들면 다음과 같습니다. 디스크 사용 분석기 (baobab), 방화벽 구성 (firewall-config), Red Hat 서브스크립션 관리자 (subscription-manager) 또는 Firefox 웹 브라우저. 관리자는 Firefox 를 사용하여 로컬 Cockpit 데몬에 원격으로 연결할 수 있습니다.

(JIRA:RHELPLAN-27394, BZ#1667225, BZ#1667516, BZ#1724302)

IBM Z의 GNOME 데스크탑은 기술 프리뷰로 사용 가능

Firefox 웹 브라우저를 포함한 GNOME 데스크탑은 이제 IBM Z 아키텍처에서 기술 프리뷰로 사용할 수 있습니다. 이제 VNC를 사용하여 IBM Z 서버를 구성하고 관리하기 위해 GNOME을 실행하는 원격 그래픽 세션에 연결할 수 있습니다.

(JIRA:RHELPLAN-27737)

5.5.7. 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)

Intel Tiger Lake 그래픽을 기술 프리뷰로 사용 가능

Intel Tiger Lake UP3 및 UP4 Xe 그래픽이 이제 기술 프리뷰로 제공됩니다.

Intel Tiger Lake 그래픽으로 하드웨어 가속을 활성화하려면 커널 명령줄에 다음 옵션을 추가합니다.

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

이 옵션에서 *pci-id*를 다음 중 하나로 바꿉니다.

- Intel GPU의 PCI ID
- 모든 알파 품질의 하드웨어를 사용하여 i915 드라이버를 활성화하는 * 문자

(BZ#1783396)

5.5.8. 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 Linux에서 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 문서](#)를 참조하십시오.

([BZ#1812552](#))

5.5.9. 가상화

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-V**에서 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 **SEV**는 VM 메모리를 암호화하여 호스트가 VM의 데이터에 액세스할 수 없도록 합니다. 이제 호스트가 악성 코드에 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 **SEV**를 사용하여 최대 **509**개의 실행 중인 VM을 지원합니다.

또한 부팅할 수 있도록 **SEV**가 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 + 256MiB**보다 크거나 같습니다. 예를 들어 게스트에 **2GiB RAM**이 할당되면 **N**은 **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 **GPU**로 할당할 수 있습니다. 결과적으로 이러한 VM은 단일 물리적 **Intel GPU**의 성능을 공유합니다.

선택한 **Intel GPU**만 vGPU 기능과 호환됩니다. 또한 VM에 물리적 **GPU**를 할당하면 호스트가 **GPU**를 사용할 수 없으며 호스트의 그래픽 디스플레이 출력이 작동하지 않을 수 있습니다.

(BZ#1528684)

중첩된 가상 머신 생성

중첩된 KVM 가상화는 **RHEL 8**을 사용하여 **AMD64** 및 **IBM Z** 시스템 호스트에서 실행되는 KVM(가상

시스템)을 위한 기술 프리뷰로 제공됩니다. 이 기능을 사용하면 물리적 **RHEL 8** 호스트에서 실행되는 **RHEL 7** 또는 **RHEL 8 VM**이 하이퍼바이저 역할을 하며 고유한 **VM**을 호스팅할 수 있습니다.

RHEL 8.2 이상에서는 **Intel 64** 호스트에서 실행되는 **VM**에서 중첩된 가상화가 완전히 지원됩니다.

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

Intel 네트워크 어댑터가 **Hyper-V**의 **RHEL** 게스트에서 **SR-IOV** 지원

Hyper-V 하이퍼바이저에서 실행되는 **Red Hat Enterprise Linux** 게스트 운영 체제는 이제 **ixgbev** 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 **NIC**에 대해 **SR-IOV** 지원이 활성화됨
- 가상 스위치에 **SR-IOV** 지원이 활성화됨
- **NIC**의 **VF(가상 기능)**가 가상 머신에 연결되어 있습니다.

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

(BZ#1348508)

5.5.10. 컨테이너

Podman 컨테이너 이미지는 기술 프리뷰로 사용할 수 있습니다.

registry.redhat.io/rhel8/podman 컨테이너 이미지는 **podman** 패키지의 컨테이너화된 구현입니다. **podman** 툴은 컨테이너 및 이미지, 해당 컨테이너에 마운트된 볼륨, 컨테이너 그룹에서 만든 포드를 관리하는 데 사용됩니다. **Podman**은 컨테이너 라이프사이클 관리를 위한 **libpod** 라이브러리를 기반으로 합니다. **libpod** 라이브러리는 컨테이너, 포드, 컨테이너 이미지 및 볼륨을 관리하는 **API**를 제공합니다. 이 컨테이너 이미지를 사용하면 시스템에 **podman** 패키지를 설치할 필요 없이 컨테이너 이미지를 생성, 수정 및 실행할 수 있습니다. 사용 사례는 루트가 아닌 사용자로 이 이미지를 **rootless** 모드에서 실행하는 것을 다

루지 않습니다. registry.redhat.io/rhel8/podman 컨테이너 이미지를 가져오려면 활성 Red Hat Enterprise Linux 서브스크립션이 필요합니다.

([BZ#1627899](#))

crun 은 기술 프리뷰로 사용 가능

crun OCI 런타임이 **container-roots:rhel8** 모듈에 추가되었습니다. **crun** 은 **cgroupsV2**로 실행할 수 있는 액세스 권한을 제공합니다. **crun** 은 컨테이너가 **rootless** 사용자 추가 그룹에 액세스할 수 있는 주석을 지원합니다. 이 기능은 사용자가 그룹만 액세스하거나 디렉터리가 **setgid**인 디렉터리에 볼륨을 마운트하는 데 유용합니다.

([BZ#1841438](#))

5.6. 사용되지 않는 기능

이 부분에서는 Red Hat Enterprise Linux 8에서 *더 이상 사용되지 않는* 기능에 대해 설명합니다.

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 사이클](#)을 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 최대한 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 8에서 *제거된* 기능에 관한 자세한 내용은 [RHEL 8 채택 고려 사항](#)을 참조하십시오.

5.6.1. 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)

RHEL 8에서는 이미지 빌더의 **Lorax -composer** 백엔드가 더 이상 사용되지 않음

이미지 빌더의 이전 백엔드 **lorax-composer**는 더 이상 사용되지 않는 것으로 간주됩니다. 나머지 **Red Hat Enterprise Linux 8** 라이프 사이클 기간 동안에는 일부 수정 사항이 제공되며 향후 주요 릴리스에서는 생략됩니다. 대신 **lorax-composer**에 대한 **lorax-composer**를 제거하고 **osbuild-composer** 백엔드를 설치 제거하는 것이 좋습니다.

자세한 내용은 사용자 지정 **RHEL 시스템 이미지** 구성을 참조하십시오.

(BZ#1893767)

5.6.2. 소프트웨어 관리

rpmbuild --sign이 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)

5.6.3. 셸 및 명령행 툴

curl에 대한 **metalink** 지원이 비활성화되었습니다.

Metalink를 사용하여 다운로드한 콘텐츠와 자격 증명 및 파일 해시 불일치 처리 방식에 **curl** 기능에서 취약점이 발견되었습니다. 이 취약점으로 인해 호스팅 서버를 제어하는 악의적인 행위자가 다음을 수행할 수 있습니다.

- 악의적인 콘텐츠 다운로드에 대한 사용자를 속입니다.
- 사용자의 지식 없이 제공된 자격 증명에 대한 무단 액세스 권한 얻기

이 취약점으로 인한 가장 큰 위협은 기밀성 및 무결성입니다. 이를 방지하기 위해 **Red Hat Enterprise Linux 8.2.0.z**에서 **curl**에 대한 **Metalink** 지원이 비활성화되었습니다.

이 문제를 해결하려면 **Metalink** 파일이 다운로드된 후 다음 명령을 실행합니다.

```
wget --trust-server-names --input-metalink`
```

예를 들면 다음과 같습니다.

```
wget --trust-server-names --input-metalink <(curl -s $URL)
```

(BZ#1999620)

5.6.4. 인프라 서비스

mailman 이 더 이상 사용되지 않음

이번 업데이트를 통해 **mailman** 패키지가 더 이상 사용되지 않는 것으로 표시되었으며 향후 **Red Hat Enterprise Linux**의 주요 릴리스에서는 사용할 수 없습니다.

(BZ#1890976)

5.6.5. 보안

NSS SEED 암호가 더 이상 사용되지 않음

Mozilla Network Security Services(NSS) 라이브러리는 향후 릴리스에서 **SEED** 암호를 사용하는 **TLS** 암호화 제품군을 지원하지 않습니다. **NSS**에서 지원을 제거할 때 **SEED** 암호를 사용하는 배포를 원활하게 전환하려면 다른 암호화 제품군에 대한 지원을 활성화하는 것이 좋습니다.

SEED 암호는 **RHEL**에서 기본적으로 비활성화되어 있습니다.

([BZ#1817533](#))

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 Portal](#)의 [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 API**를 사용하여 활성화해야 합니다. 이 기능에 대한 지원은 **Red Hat Enterprise Linux 8**의 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 2.0**으로 업데이트되었습니다. **TPM 2.0**은 **TPM 1.2**보다 많은 개선 사항을 제공하며 이전 버전과는 역호환되지 않습니다. **RHEL 8**에서는 **TPM 1.2**가 더 이상 사용되지 않으며 다음 주요 릴리스에서 제거될 수 있습니다.

(BZ#1657927)

5.6.6. 네트워킹

RHEL 8에서 네트워크 스크립트가 더 이상 사용되지 않음

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

5.6.7. 커널

디스크리스 부팅을 사용하여 실시간 8용 RHEL 설치하는 데 이상 사용되지 않음

디스크리스 부팅을 사용하면 여러 시스템에서 네트워크를 통해 루트 파일 시스템을 공유할 수 있습니다. 편리한 디스크 없는 부팅은 실시간 워크로드에서 네트워크 대기 시간을 도입하기 쉽습니다. 향후 RHEL for Real Time 8의 마이너 업데이트에서는 더 이상 디스크리스 부팅 기능이 지원되지 않습니다.

(BZ#1748980)

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)

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)

5.6.8. 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 8**에서 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 설정](#)을 참조하십시오.

(BZ#1665295)

LVM 미러 가 더 이상 사용되지 않음

LVM 미러 세그먼트 유형이 더 이상 사용되지 않습니다. 미러 지원은 향후 **RHEL**의 주요 릴리스에서 제거될 예정입니다.

Red Hat은 미러 대신 세그먼트 유형이 **raid1** 인 **LVM RAID 1** 장치를 사용할 것을 권장합니다. **raid1** 세그먼트 유형은 기본 **RAID** 구성 유형이며 권장 솔루션으로 미러 를 바꿉니다.

미러 장치를 **raid1** 로 변환하려면 [미러링된 LVM 장치를 RAID1 장치로 변환](#)을 참조하십시오.

LVM 미러 에는 몇 가지 알려진 문제가 있습니다. 자세한 내용은 [파일 시스템 및 스토리지의 알려진 문제](#)를 참조하십시오.

(BZ#1827628)

peripety는 더 이상 사용되지 않음

peripety 패키지는 **RHEL 8.3** 이후 더 이상 사용되지 않습니다.

Peripety 스토리지 이벤트 알림 데몬은 시스템 스토리지 로그를 구조화된 스토리지 이벤트에 구문 분석합니다. 스토리지 문제를 조사하는 데 도움이 됩니다.

(BZ#1871953)

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)

cramfs 가 더 이상 사용되지 않음

사용자가 부족하기 때문에 **cramfs** 커널 모듈이 더 이상 사용되지 않습니다. 대체 솔루션으로 **squashfs** 를 사용하는 것이 좋습니다.

(BZ#1794513)

5.6.9. IdM (Identity Management)

OpenSSH-Idap 이 더 이상 사용되지 않음

openssh-Idap 하위 패키지는 Red Hat Enterprise Linux 8에서 더 이상 사용되지 않으며 RHEL 9에서 제거됩니다. **openssh-Idap** 하위 패키지가 업스트림에서 유지 관리되지 않으므로 Red Hat은 **SSSD** 및 **sss_ssh_authorizedkeys** 도우미를 사용할 것을 권장합니다. 이 도우미는 다른 IdM 솔루션과 더 잘 통합되고 더 안전합니다.

기본적으로 **SSSD Idap** 및 **ipa** 공급자는 사용 가능한 경우 사용자 오브젝트의 **sshPublicKey LDAP** 속성을 읽습니다. AD에는 공개 키를 저장할 기본 LDAP 특성이 없으므로 **ad provider** 또는 IdM 신뢰할 수 있는 도메인에 기본 **SSSD** 구성을 사용하여 AD(Active Directory)에서 SSH 공개 키를 검색할 수 없습니다.

sss_ssh_authorizedkeys 도우미가 **SSSD**에서 키를 가져올 수 있도록 하려면 **sssd.conf** 파일의 **services** 옵션에 **ssh**를 추가하여 **ssh** 응답자 를 활성화합니다. 자세한 내용은 **sssd.conf(5)** 도움말 페이지를 참조하십시오.

sshd 가 **sss_ssh_authorizedkeys** 를 사용할 수 있도록 하려면 **AuthorizedKeysCommand**

`/usr/bin/sss_ssh_authorizedkeys` 및 `AuthorizedKeysCommandUser nobody` 옵션에 `sss_ssh/sshd_config` 파일에 설명된 대로 `sss_ssh_authorizedkeys(1)` 도움말 페이지를 추가합니다.

(BZ#1871025)

DES 및 3DES 암호화 유형이 제거되었습니다.

보안상의 이유로 RHEL 7 이후 기본적으로 DES(데이터 암호화 표준) 알고리즘이 더 이상 사용되지 않고 비활성화되어 있습니다. 최근 Kerberos 패키지 리베이스를 변경하면서 단일 DES(DES) 및 Triple-DES(3DES) 암호화 유형이 RHEL 8에서 제거되었습니다.

DES 또는 3DES 암호화만 사용하도록 서비스 또는 사용자를 구성한 경우 다음과 같은 서비스 중단이 발생할 수 있습니다.

- Kerberos 인증 오류
- 알 수 없는 enctype 암호화 오류
- K/M(DESed-encrypted Database Master Keys)이 포함된 KDC(Kerberos Distribution Centers)가 시작되지 않습니다.

업그레이드를 준비하려면 다음 작업을 수행합니다.

1. KDC가 `krb5check` 오픈소스 Python 스크립트와 함께 DES 또는 3DES 암호화를 사용하는지 확인하십시오. GitHub의 [krb5check](#) 를 참조하십시오.
2. Kerberos 주체와 함께 DES 또는 3DES 암호화를 사용하는 경우 AES(Advanced Encryption Standard)와 같은 지원되는 암호화 유형으로 키를 다시 입력합니다. 재키징에 대한 지침은 MIT Kerberos 문서에서 [DES를 폐기](#) 하는 것을 참조하십시오.
3. 업그레이드하기 전에 다음 Kerberos 옵션을 일시적으로 설정하여 DES 및 3DES에서 독립성을 테스트합니다.
 - a. KDC의 `/var/kerberos/krb5kdc/kdc.conf` 에서 `supported_enctypes` 를 설정하고 `des` 또는 `des 3` 를 포함하지 마십시오.

b.

모든 호스트에 대해 `/etc/krb5.conf` 및 `/etc/krb5.conf.d` 의 모든 파일에 대해 `allow_weak_crypto` 를 `false`로 설정합니다. 기본적으로 `false`입니다.

c.

모든 호스트에 대해 `/etc/krb5.conf` 및 `/etc/krb5.conf.d` 에 있는 모든 파일에 대해 `allowed_encetypes`, `default_tgs_encetypes` 및 `default_tkt_encetypes` 를 설정하고 `des` 또는 `des 3` 을 포함하지 마십시오.

4.

이전 단계에서 테스트 **Kerberos** 설정으로 서비스가 중단되지 않으면 해당 서비스를 제거하고 업그레이드합니다. 최신 **Kerberos** 패키지로 업그레이드한 후에는 이러한 설정이 필요하지 않습니다.

(BZ#1877991)

5.6.10. 데스크탑

libgnome-keyring 라이브러리가 더 이상 사용되지 않음

libgnome-keyring 은 업스트림에서 유지 관리되지 않으며 **RHEL**에 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)

AlternateTab 확장 기능이 제거되었습니다

AlternateTab GNOME Shell 확장을 제공하는 **gnome-shell-extension-alternate-tab** 패키지가 제거되었습니다.

창 전환 동작을 구성하려면 키보드 설정에서 키보드 바로 가기를 설정합니다. 자세한 내용은 다음 문서를 참조하십시오. [Gnome 3.32 이상에서 Alternate-Tab 사용. \(BZ#1922488\)](#)

5.6.11. 그래픽 인프라

AGP 그래픽 카드는 더 이상 지원되지 않습니다.

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

(BZ#1569610)

5.6.12. 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)

5.6.13. Red Hat Enterprise Linux 시스템 역할

geoipupdate 패키지가 더 이상 사용되지 않음

geoipupdate 패키지에는 타사 서브스크립션이 필요하며 독점 콘텐츠도 다운로드합니다. 따라서 **geoipupdate** 패키지는 더 이상 사용되지 않으며 다음 주요 **RHEL** 버전에서 제거됩니다.

(BZ#1874892)

5.6.14. 가상화

virt-manager가 더 이상 사용되지 않음

virt-manager라고도 하는 **Virtual Machine Manager** 애플리케이션은 더 이상 사용되지 않습니다. **Cockpit**라고도 하는 **RHEL 8** 웹 콘솔은 후속 릴리스에서 교체될 예정입니다. 따라서 **GUI**에서 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 8**에서 **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)

SPICE가 더 이상 사용되지 않음

RHEL 8.3에서는 **SPICE** 원격 디스플레이 프로토콜이 더 이상 사용되지 않습니다. **SPICE**는 RHEL 8에서 계속 지원되지만 원격 디스플레이 스트리밍에 대체 솔루션을 사용하는 것이 좋습니다.

- 원격 콘솔 액세스의 경우 **VNC** 프로토콜을 사용합니다.
- 고급 원격 디스플레이 기능의 경우 **RDP**, **HP RGS** 또는 **Mechdyne TGX**와 같은 타사 툴을 사용하십시오.

(BZ#1849563)

5.6.15. 컨테이너

podman varlink 기반 **REST API V1**이 더 이상 사용되지 않음

Podman varlink 기반 **REST API V1**은 새 **Podman REST API V2** 대신 업스트림에서 더 이상 사용되지 않습니다. 이 기능은 Red Hat Enterprise Linux 8의 이후 릴리스에서 제거됩니다.

(JIRA:RHELPLAN-60226)

5.6.16. 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**
- **lorax-composer**
- **Mercurial**
- **net-tools**
- **network-scripts**
- **nss-pam-ldapd**
- **sendmail**
- **jp-tools**
- **ypbind**

•

ypserv**5.7. 확인된 문제**

이 부분에서는 **Red Hat Enterprise Linux 8.3**의 알려진 문제에 대해 설명합니다.

5.7.1. 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 **authconfig**가 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)

설치 프로그램에서는 네트워크 액세스가 기본적으로 활성화되어 있지 않습니다

몇 가지 설치 기능에는 네트워크 액세스(예: **CDN**(콘텐츠 전달 네트워크), **NTP** 서버 지원, 네트워크 설치 소스)를 사용하여 시스템 등록이 필요합니다. 그러나 네트워크 액세스는 기본적으로 활성화되어 있지 않으므로 네트워크 액세스가 활성화될 때까지 이러한 기능을 사용할 수 없습니다.

이 문제를 해결하려면 **ip=dhcp**를 추가하여 설치가 시작될 때 네트워크 액세스를 활성화하도록 옵션을 부팅합니다. 선택적으로 부팅 옵션을 사용하여 네트워크에 있는 **Kickstart** 파일 또는 리포지토리를 전

달하면 문제가 해결됩니다. 결과적으로 네트워크 기반 설치 기능을 사용할 수 있습니다.

(BZ#1757877)

새로운 **osbuild-composer** 백엔드는 업그레이드 시 **lorax-composer** 에서 청사진 상태를 복제하지 않습니다.

lorax-composer 백엔드에서 새로운 **osbuild-composer** 백엔드로 업그레이드하는 이미지 빌더 사용자는 청사진이 사라질 수 있습니다. 결과적으로 업그레이드가 완료되면 청사진이 자동으로 표시되지 않습니다. 이 문제를 해결하려면 다음 단계를 수행합니다.

사전 요구 사항

- **composer-cli CLI** 유틸리티가 설치되어 있어야 합니다.

절차

1. 명령을 실행하여 이전 **lorax-composer** 기반 청사진을 새 **osbuild-composer** 백엔드로 로드합니다.

```
$ for blueprint in $(find /var/lib/lorax/composer/blueprints/git/workspace/master -name
*.toml); do composer-cli blueprints push "${blueprint}"; done
```

그 결과 **osbuild-composer** 백엔드에서 동일한 청사진을 사용할 수 있습니다.

추가 리소스

- 이 알려진 문제에 대한 자세한 내용은 [Red Hat Enterprise Linux 8.3 문서의 업데이트에 따라 Image Builder 청사진이 더 이상 표시되지 않습니다.](#)

(BZ#1897383)

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)

저장소 새로 고침을 완료하기 전에 **CDN**을 사용하여 등록 해제를 시도하면 **GUI** 설치에 실패할 수 있습니다.

RHEL 8.2부터 **CDN(Content Delivery Network)**을 사용하여 시스템을 등록하고 서브스크립션을 연결할 때 **GUI** 설치 프로그램에 의해 리포지토리 메타데이터의 새로 고침이 시작됩니다. 새로 고침 프로세스는 등록 및 서브스크립션 프로세스의 일부가 아니며, 결과적으로 **Connect to Red Hat** 창에서 **Unregister** 버튼이 활성화됩니다. 네트워크 연결에 따라 새로 고침 프로세스를 완료하는 데 1분 이상이 걸릴 수 있습니다. 새로 고침 프로세스가 완료되기 전에 **Unregister** 단추를 클릭하면 **unregister** 프로세스가 **CDN** 리포지토리 파일과 **CDN**과 통신하는 데 필요한 인증서가 제거되므로 **GUI** 설치가 실패할 수 있습니다.

이 문제를 해결하려면 **Connect to Red Hat** 창에서 **Register(등록)** 버튼을 클릭한 후 **GUI** 설치에서 다음 단계를 완료합니다.

1. **Connect to Red Hat** 창에서 **Done(완료)**을 클릭하여 **Installation Summary (설치 요약)** 창으로 돌아갑니다.
2. **Installation Summary(설치 요약)** 창에서 *italics*의 **Installation Source(설치 소스)** 및 **Software Selection (소프트웨어 선택)** 상태 메시지에 처리 정보가 표시되지 않는지 확인합니다.
3. 설치 소스 및 소프트웨어 선택 범주가 준비되면 **Connect to Red Hat** 을 클릭합니다.
4. **Unregister(등록 취소)** 버튼을 클릭합니다.

이러한 단계를 수행한 후에는 **GUI**를 설치하는 동안 시스템을 안전하게 등록 취소할 수 있습니다.

(BZ#1821192)

여러 조직에 속한 사용자 계정의 등록 실패

현재 여러 조직에 속하는 사용자 계정으로 시스템을 등록하려고 하면 오류 메시지와 함께 등록 프로세스가 실패합니다. 새 유닛의 조직을 지정해야 합니다.

이 문제를 해결하려면 다음 중 하나를 수행할 수 있습니다.

- 여러 조직에 속하지 않는 다른 사용자 계정을 사용합니다.
- GUI 및 Kickstart 설치를 위한 **Connect to Red Hat** 기능에서 제공되는 활성화 키 인증 방법을 사용합니다.
- **Connect to Red Hat**의 등록 단계를 건너뛰고 서브스크립션 관리자를 사용하여 시스템 설치 후 등록합니다.

(BZ#1822880)

설치 프로그램 부팅 옵션을 사용하여 **InfiniBand** 네트워크 인터페이스를 구성할 때 **RHEL** 설치 프로그램이 시작되지 않습니다.

설치 프로그램 부팅 옵션(예: **PXE** 서버를 사용하여 설치 프로그램 이미지 다운로드)을 사용하여 **RHEL** 설치 초기 단계에서 **InfiniBand** 네트워크 인터페이스를 구성할 때 설치 프로그램에서 네트워크 인터페이스를 활성화하지 못합니다.

이 문제는 **RHEL NetworkManager**가 **InfiniBand** 모드에서 네트워크 인터페이스를 인식하지 못하고 대신 인터페이스에 대한 이더넷 연결을 구성하지 못하기 때문에 발생합니다.

그 결과 연결 활성화가 실패하고 초기 단계에서 **InfiniBand** 인터페이스를 통한 연결이 필요한 경우 **RHEL** 설치 프로그램이 설치를 시작할 수 없습니다.

이 문제를 해결하려면 **Lorax** 툴을 사용하여 업데이트된 **Anaconda** 및 **NetworkManager** 패키지를 포함하여 새 설치 미디어를 생성합니다.

업데이트된 **Anaconda** 및 **NetworkManager** 패키지를 포함하여 **Lorax** 툴을 사용하여 새 설치 미디어를 생성하는 방법에 대한 자세한 내용은 [InfiniBand 네트워크 인터페이스를 사용하여 Red Hat Enterprise Linux 8.3.0을 설치할 수 없음](#)을 참조하십시오.

(BZ#1890261)

NVDIMM 장치 네임스페이스가 **devdax** 모드로 설정된 경우 **Anaconda** 설치에 실패합니다.

GUI를 설치하기 전에 **NVDIMM** 장치 네임스페이스를 **devdax** 모드로 설정한 후 부팅한 후 **Anaconda** 설치에 실패합니다.

이 문제를 해결하려면 설치를 시작하기 전에 **NVDIMM** 장치를 재구성하여 네임스페이스를 **devdax** 모드와 다른 모드로 설정합니다. 결과적으로 설치를 진행할 수 있습니다.

(BZ#1891827)

타사 툴을 사용하여 생성된 **USB**에서 설치를 부팅할 때 로컬 미디어 설치 소스가 탐지되지 않습니다.

타사 툴을 사용하여 생성된 **USB**에서 **RHEL** 설치를 부팅할 때 설치 프로그램에서 로컬 미디어 설치 소스를 감지하지 못합니다('Red Hat CDN'만 감지됨).

이 문제는 기본 부팅 옵션 **inst.stage2=** 에서 **iso9660** 이미지 형식을 검색하려고 하므로 발생합니다. 그러나 타사 툴에서 다른 형식으로 **ISO** 이미지를 생성할 수 있습니다.

이 문제를 해결하려면 다음 솔루션 중 하나를 사용하십시오.

- 설치를 부팅할 때 **Tab** 키를 클릭하여 커널 명령줄을 편집하고 부팅 옵션 **inst.stage2=**를 **inst. repo=**로 변경합니다.
- **Windows**에서 부팅 가능한 **USB** 장치를 만들려면 **Fedora Media Writer**를 사용합니다.
- **Rufus**와 같은 타사 도구를 사용하여 부팅 가능한 **USB** 장치를 생성하는 경우 먼저 **Linux** 시스템에서 **RHEL ISO** 이미지를 다시 생성한 다음 타사 툴을 사용하여 부팅 가능한 **USB** 장치를 생성합니다.

지정된 해결 방법 수행과 관련된 단계에 대한 자세한 내용은 [RHEL 8.3 설치 중에 설치 미디어가 자동으로 탐지되지 않음](#)을 참조하십시오.

(BZ#1877697)

Anaconda는 텍스트 모드에서 **lidl** 또는 포맷되지 않은 **DASD** 디스크에 대한 대화 상자 표시

이전에는 텍스트 모드로 설치하는 동안 **Anaconda**가 **Linux** 디스크 레이아웃(**lidl**) 또는 포맷되지 않은 **DASD(Direct-Access Storage Device)** 디스크에 대한 대화 상자를 표시하지 못했습니다. 이로 인해 사용자가 이러한 디스크를 설치할 수 없었습니다.

이번 업데이트를 통해 **Anaconda**는 텍스트 모드에서 **lidl** 및 포맷되지 않은 **DASD** 디스크를 인식하고 사용자가 설치의 향후 사용률에 맞게 올바르게 포맷할 수 있는 대화 상자를 표시합니다.

(BZ#1874394)

그래픽 설치 프로그램을 사용할 때 **Red Hat Insights** 클라이언트가 운영 체제를 등록하지 못합니다.

현재 **Insights** 클라이언트를 가리키는 끝에 오류와 함께 설치가 실패합니다.

이 문제를 해결하려면 설치 프로그램에서 시스템을 등록하기 전에 **Connect to Red Hat** 단계에서 **Connect to Red Hat Insights** 옵션을 선택 취소합니다.

결과적으로 다음 명령을 사용하여 설치를 완료하고 **Insights**에 등록할 수 있습니다.

```
# insights-client --register
```

(BZ#1931069)

5.7.2. 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.

[\(BZ#1687900\)](#)

5.7.3. 인프라 서비스

dnf 업데이트를 실행할 때 **libmaxminddb-devel-debuginfo.rpm** 이 제거됨

dnf update 명령을 수행할 때 바이너리 **mmdblookup** 툴은 **libmaxminddb-devel** 하위 패키지에서 기본 **libmaxminddb** 패키지로 이동합니다. 결과적으로 **libmaxminddb-devel-debuginfo.rpm** 이 제거되어 이 패키지에 대해 손상된 업데이트 경로를 생성할 수 있습니다. 이 문제를 해결하려면 **dnf update** 명령을 실행하기 전에 **libmaxminddb-devel-debuginfo** 를 제거합니다.

참고: **libmaxminddb-debuginfo** 는 **new debuginfo** 패키지입니다.

[\(BZ#1642001\)](#)

5.7.4. 보안

사용자는 잠긴 사용자로 **sudo** 명령을 실행할 수 있습니다.

sudoers 권한이 **ALL** 키워드로 정의된 시스템에서 권한이 있는 **sudo** 사용자는 계정이 잠겨 있는 사용자로 **sudo** 명령을 실행할 수 있습니다. 따라서 잠김 및 만료된 계정은 명령을 실행하는 데 계속 사용할 수 있습니다.

이 문제를 해결하려면 **/etc/shells** 에서 유효한 셸의 적절한 설정과 함께 새로 구현된 **runas_check_shell** 옵션을 활성화하십시오. 이렇게 하면 공격자가 시스템 계정(예: **bin**)에서 명령을 실행하지 못합니다.

[\(BZ#1786990\)](#)

Gnutls가 **NSS** 서버로 현재 세션을 다시 시작하지 못했습니다

TLS(Transport Layer Security) 1.3 세션을 다시 시작할 때 **GnuTLS** 클라이언트는 60밀리초 동안 서버에 세션 재개 데이터를 보낼 때까지 예상 왕복 시간을 기다립니다. 서버가 이 시간 내에 재사용 데이터를 전송하지 않으면 클라이언트는 현재 세션을 다시 시작하지 않고 새 세션을 만듭니다. 이로 인해 정기적인 세션 협상에 약간의 성능에 영향을 미치는 것을 제외하고는 심각한 부정적인 영향이 발생하지 않습니다.

[\(BZ#1677754\)](#)

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=podman**으로 시작되는 경우에만 **UBI 8** 컨테이너를 처리합니다.

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)

성능에 대한 기본 로깅 설정의 부정적인 영향

기본 로깅 환경 설정은 **rsyslog** 를 사용하여 **systemd-journald**를 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)

`/etc/passwd-` 의 파일 권한은 CIS RHEL 8 벤치마크 1.0.0과 일치하지 않습니다.

CIS 벤치마크의 문제로 인해 `/etc/passwd-` 백업 파일에 대한 권한을 보장하는 SCAP 규칙의 수정으로 인해 권한을 0644로 구성합니다. 그러나 CIS Red Hat Enterprise Linux 8 벤치마크 1.0.0에는 해당 파일에 대한 파일 권한 0600이 필요합니다. 결과적으로 수정 후 `/etc/passwd-` 의 파일 권한이 벤치마크와 정렬되지 않습니다.

(BZ#1858866)

`/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 누수가 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)

`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)

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)

FIPS 모드에서 **OpenSSL**은 특정 **D-H** 매개변수만 허용

FIPS 모드에서 **OpenSSL**을 사용하는 **TLS(Transport Security Layer)** 클라이언트는 잘못된 **dh** 값 오류를 반환하고 수동으로 생성된 매개 변수를 사용하는 서버에 대한 **TLS** 연결을 중단합니다. 이는 **FIPS 140-2**를 준수하도록 구성된 경우 **OpenSSL**이 **NIST SP 800-56A rev3** 부록 **D(RFC 3526** 및 **RFC 7919)**에 정의된 그룹과 **RFC 7919**을 준수하는 **D-H** 매개변수에서만 작동하기 때문입니다. 또한 **OpenSSL**을 사용하는 서버는 다른 모든 매개 변수를 무시하고 대신 유사한 크기의 알려진 매개 변수를 선택합니다. 이 문제를 해결하려면 규정 준수 그룹만 사용하십시오.

(BZ#1810911)

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

rpm-plugin-selinux 패키지를 제거하면 시스템에서 **SELinux**가 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 **SELinux**가 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 **SELinux**가 활성화되어 이전과 동일한 정책을 실행합니다.

(BZ#1641631)

systemd 서비스는 임의의 경로에서 명령을 실행할 수 없습니다.

systemd 서비스는 **SELinux** 정책 패키지에 이러한 규칙을 포함하지 않기 때문에 **/home/user/bin** 임의의 경로에서 명령을 실행할 수 없습니다. 결과적으로 비 시스템 경로에서 실행되는 사용자 지정 서비스가 실패하고 **SELinux**가 액세스를 거부하면 **AVC**(액세스 벡터 캐시) 거부 감사 메시지를 기록합니다. 이 문제를 해결하려면 다음 중 하나를 수행하십시오.

•

셸 스크립트를 **-c** 옵션과 함께 사용하여 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
bash -c command
```

•

/bin, **/sbin**, **/usr/sbin**, **/usr/local/bin** 및 **/usr/local/sbin** 공통 디렉토리를 사용하여 공통 경로에서 명령을 실행합니다.

(BZ#1860443)

CIS 프로파일에서 **rpm_verify_permissions** 실패

rpm_verify_permissions 규칙은 파일 권한을 패키지 기본 권한과 비교합니다. 그러나 **scap-security-guide** 패키지에서 제공하는 **CIS(Center for Internet Security)** 프로파일은 일부 파일 권한을 기본 값보다 더 엄격하게 변경합니다. 그 결과 **rpm_verify_permissions** 를 사용한 특정 파일 확인에 실패했습니다.

이 문제를 해결하려면 이러한 파일에 다음 권한이 있는지 수동으로 확인합니다.

•

/etc/cron.d (0700)

- /etc/cron.hourly (0700)
- /etc/cron.monthly (0700)
- /etc/crontab (0600)
- /etc/cron.weekly (0700)
- /etc/cron.daily (0700)

(BZ#1843913)

kickstart에서는 RHEL 8에서 `com_redhat_oscaped` 대신 `org_fedora_oscaped` 을 사용합니다.

Kickstart는 OSCAP(Open Security Content Automation Protocol) Anaconda 애드온을 `com_redhat_oscaped` 대신 `org_fedora_oscaped` 으로 참조하여 혼동을 일으킬 수 있습니다. 이는 Red Hat Enterprise Linux 7과 이전 버전과의 호환성을 유지하기 위해 수행됩니다.

(BZ#1665082)

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)

OSCAP Anaconda 애드온은 모든 패키지를 텍스트 모드에 설치하지 않음

OSCAP Anaconda Addon 플러그인은 설치가 텍스트 모드에서 실행 중인 경우 시스템 설치 프로그램에서 설치에 대해 선택한 패키지 목록을 수정할 수 없습니다. 결과적으로 Kickstart를 사용하여 보안 정책 프로파일 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 애드온이 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 **DS**에서 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)

OSPP 기반 프로필은 **GUI** 패키지 그룹과 호환되지 않습니다.

GUI 패키지 그룹과 함께 서버에서 설치한 **GNOME** 패키지에는 **OSPP**(Operating System Protection Profile)와 호환되지 않는 **nfs-utils** 패키지가 필요합니다. 결과적으로 **OSPP** 또는 **OSPP** 기반 프로필(예: **STIG**(Security Technical Implementation Guide))을 사용하여 시스템을 설치하는 동안 **GUI** 패키지 그룹이 포함된 서버를 선택하면 **OpenSCAP**에 선택한 패키지 그룹이 보안 정책과 호환되지 않는다는 경고가 표시됩니다. **OSPP** 기반 프로필이 설치 후 적용되는 경우 시스템을 부팅할 수 없습니다. 이 문제를 해결하려면 **GUI** 패키지 그룹이나 **OSPP** 프로파일과 **OSPP** 기반 프로필을 사용할 때 **GUI**를 설치하는 다른 그룹을 사용하여 서버를 설치하지 마십시오. 대신 **Server** 또는 **Minimal Install** 패키지 그룹을 사용하는 경우 시스템이 문제 없이 설치되고 올바르게 작동합니다.

(BZ#1787156)

GUI 또는 워크스테이션 소프트웨어 선택 및 **CIS** 보안 프로파일을 사용하여 서버를 설치할 수 없습니다.

CIS 보안 프로필은 **GUI** 및 워크스테이션 소프트웨어 선택과 호환되지 않습니다. 결과적으로 **GUI** 소프트웨어 선택 및 **CIS** 프로파일을 사용하여 서버를 사용하여 **RHEL 8**을 설치할 수 없습니다. **CIS** 프로필을 사용하여 시도한 설치와 이러한 소프트웨어 선택 중 하나가 오류 메시지를 생성합니다.

package xorg-x11-server-common has been added to the list of excluded packages, but it can't be removed from the current software selection without breaking the installation.

이 문제를 해결하려면 **GUI** 또는 워크스테이션 소프트웨어 선택이 포함된 서버와 함께 **CIS** 보안 프로필을 사용하지 마십시오.

([BZ#1843932](#))

kickstart 설치 중에 서비스 관련 규칙을 수정하는 데 실패할 수 있습니다.

Kickstart를 설치하는 동안 **OpenSCAP** 유틸리티에서 서비스가 상태 수정을 활성화하거나 비활성화할 필요가 없음을 잘못 표시한 경우가 있습니다. 결과적으로 **OpenSCAP**은 설치된 시스템의 서비스를 준수하지 않는 상태로 설정할 수 있습니다. 이 문제를 해결하려면 **kickstart** 설치 후 시스템을 스캔하고 교정할 수 있습니다. 그러면 서비스 관련 문제가 해결됩니다.

([BZ#1834716](#))

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](#))

암호화 정책이 **Camellia** 암호를 잘못 허용

RHEL 8 시스템 전체 암호화 정책은 제품 문서에 명시된 대로 모든 정책 수준에서 **Camellia** 암호를 비활성화해야 합니다. 그러나 **Kerberos** 프로토콜에서는 기본적으로 암호를 활성화합니다.

이 문제를 해결하려면 **NO-CAMELLIA** 하위 정책을 적용합니다.

```
# update-crypto-policies --set DEFAULT:NO-CAMELLIA
```

이전 명령에서 **DEFAULT** 에서 이전에 전환한 경우 **DEFAULT** 를 암호화 수준 이름으로 바꿉니다.

결과적으로 **Camellia** 암호는 해결 방법을 통해 비활성화하는 경우에만 시스템 전체 암호화 정책을 사용하는 모든 애플리케이션에서 올바르게 허용하지 않습니다. ([BZ#1919155](#))

5.7.5. 네트워킹

iptables 유틸리티는 이제 **NLM_F_CREATE** 플래그에 관계없이 체인을 업데이트하는 명령에 대한 모듈 로드를 요청합니다.

이전에는 체인의 정책을 설정할 때 **iptables-nft** 유틸리티에서 **NEWCHAIN** 메시지를 생성했지만 **NLM_F_CREATE** 플래그를 설정하지 않았습니다. 결과적으로 연결된 커널 모듈을 수동으로 로드하지 않은 경우 **RHEL 8** 커널이 모듈을 로드하지 않았으며 결과 **update chain** 명령이 실패했습니다. 이번 업데이트를 통해 **iptables-nft** 유틸리티에서 체인을 업데이트하는 모든 명령에 대한 모듈 로드를 요청하고 사용자가 관련 모듈을 수동으로 로드하지 않고 **iptables-nft** 유틸리티를 사용하여 체인의 정책을 설정할 수 있습니다.

([BZ#1812666](#))

RHEL 7과 **RHEL 8** 사이에서 커널의 패킷/바이트 카운터 업데이트 지원이 잘못 변경되었습니다.

ipset 항목 일치에 대한 추가 제약 조건을 지정하는 **iptables** 규칙에서 활성화된 카운터를 사용하여 **ipset** 명령을 참조할 때 **ipset** 카운터는 모든 추가 제약 조건이 일치하는 경우에만 업데이트됩니다. 이는 또한 **--packets-gt** 또는 **--bytes-gt** 제약 조건에 문제가 있습니다.

결과적으로 **RHEL 7**에서 **RHEL 8**로 **iptables** 규칙 세트를 마이그레이션할 때 **ipset** 조회와 관련된 규칙을 중지하고 조정해야 할 수 있습니다. 이 문제를 해결하려면 **--packets-gt** 또는 **--bytes-gt** 옵션을 사용하지 말고 **--packets-lt** 또는 **--bytes-lt** 옵션으로 교체하십시오.

([BZ#1806882](#))

XDP 프로그램 언로드가 **nfp** 드라이버를 사용하는 **Netronome** 네트워크 카드에서 실패합니다.

Netronome 네트워크 카드의 **nfp** 드라이버에는 버그가 포함되어 있습니다. 따라서 해당 카드를 사용하고 **XDP_FLAGS_REPLACE** 플래그와 함께 **IFLA_XDP_EXPECTED_FD** 기능을 사용하여 **XDP** 프로

그램을 로드하면 **eXpress Data Path(X DP)** 프로그램을 언로드할 수 없습니다. 예를 들어 이 버그는 **libxdp** 라이브러리를 사용하여 로드되는 **XDP** 프로그램에 영향을 미칩니다. 현재 이 문제에 대한 해결 방법이 없습니다.

([BZ#1880268](#))

ip boot 옵션에서 **DHCP**를 사용할 때 **Anaconda**에 네트워크 액세스 권한이 없습니다

초기 **RAM** 디스크(**initrd**)는 **NetworkManager**를 사용하여 네트워킹을 관리합니다. **RHEL 8.3 ISO** 파일에서 제공하는 **dracut NetworkManager** 모듈은 **Anaconda** 부팅 옵션의 첫 번째 필드가 항상 설정되었다고 잘못 가정합니다. 결과적으로 **DHCP**를 사용하고 **ip=::::dhcp**를 설정하면 **NetworkManager**가 **IP** 주소를 검색하지 않고 **Anaconda**에서 네트워크를 사용할 수 없습니다.

문제를 해결할 수 있는 다음 옵션이 있습니다.

1.

ip'option의 첫 번째 필드를 **'** (**period**)로 설정합니다.

```
ip=.::::<host_name>::dhcp
```

문제가 해결되면 이 해결 방법은 향후 **RHEL** 버전에서는 해결되지 않습니다.

2.

버그 수정이 포함된 **BaseOS** 리포지토리의 최신 패키지를 사용하여 **boot.iso** 파일을 다시 생성합니다.

```
# lorax '--product=Red Hat Enterprise Linux' --version=8.3 --release=8.3 \
--source=<URL_to_BaseOS_repository> \
--source=<URL_to_AppStream_repository> \
--nomacboot --buildarch=x86_64 '--volid=RHEL 8.3' <output_directory>
```

Red Hat은 자체 생성된 **ISO** 파일을 지원하지 않습니다.

결과적으로 **RHEL**은 **DHCP** 서버에서 **IP** 주소를 검색하고 **Anaconda**에서 네트워크 액세스를 사용할 수 있습니다.

([BZ#1902791](#))

5.7.6. 커널

tboot-1.9.12-2 유틸리티로 인해 **RHEL 8**에서 부팅에 실패합니다.

버전 **1.9.12-2**의 **tboot** 유틸리티로 인해 **TPM (Trusted Platform Module) 2.0**이 있는 일부 시스템이 기존 모드에서 부팅되지 않습니다. 그 결과 시스템은 **tboot Grand Unified Bootloader (GRUB)** 항목에서 부팅하려고 하면 시스템이 중단됩니다. 이 문제를 해결하려면 버전 **1.9.10**의 **tboot**로 다운그레이드하십시오.

(BZ#1947839)

커널이 **IBM Z** 시스템에서 오탐 경고 반환

RHEL 8에서는 사용자가 액세스할 수 있도록 **IBM Z** 시스템에 **ZONE_DMA** 메모리 영역에 대한 화이트리스트 항목이 누락되었습니다. 결과적으로 커널은 다음과 같은 오탐(**false positive**) 경고를 반환합니다.

```
...
Bad or missing usercopy whitelist? Kernel memory exposure attempt detected from SLUB object
'dma-kmalloc-192' (offset 0, size 144)!
WARNING: CPU: 0 PID: 8519 at mm/usercopy.c:83 usercopy_warn+0xac/0xd8
...
```

sysfs 인터페이스를 통해 특정 시스템 정보에 액세스할 때 경고가 표시됩니다. 예를 들어, **debuginfo.sh** 스크립트를 실행합니다.

이 문제를 해결하려면 **hardened_usercopy=off** 매개 변수를 커널 명령줄에 추가합니다.

따라서 설명된 시나리오에는 경고 메시지가 표시되지 않습니다.

(BZ#1660290)

대기 중인 **The rngd** 서비스가 **FIPS** 모드에서 총 **CPU** 사용량을 발생

버전 **4.18.0-193.10**부터 커널에 **FIPS** 모드용 새 커널 엔트로피 소스가 추가되었습니다. 결과적으로 **FIPS** 모드에서 **the rngd** 서비스는 **/dev/random** 장치에 대한 **poll()** 시스템 호출에서 대기하므로 **CPU** 시간의 **100%**가 소비됩니다. 이 문제를 해결하려면 다음을 실행하여 중지 및 비활성화하십시오.

```
# systemctl stop rngd
# systemctl disable rngd
```

따라서 **Rng d**는 설명된 시나리오에서 **poll()**에 대한 대기를 더 이상 사용하지 않습니다.

(BZ#1884857)

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)

메모리 핫플러그 또는 언플러그 작업 후 **vmcore** 캡처가 실패합니다.

메모리 핫플러그 또는 핫 플러그 해제 작업을 수행한 후에는 메모리 레이아웃 정보가 포함된 장치 트리를 업데이트한 후 이벤트가 제공됩니다. 따라서 **makedumpfile** 유틸리티는 존재하지 않는 실제 주소에 액세스를 시도합니다. 다음 모든 조건이 충족되면 문제가 표시됩니다.

- **RHEL 8**을 실행하는 **IBM Power System**의 **little-endian** 변형.
- **kdump** 또는 **fadump** 서비스가 시스템에서 활성화됩니다.

결과적으로 메모리 핫플러그 또는 핫 플러그 작업 후에 커널 충돌이 트리거되면 캡처 커널이 **vmcore**를 저장하지 못합니다.

이 문제를 해결하려면 핫 플러그 또는 핫 플러그 후 **kdump** 서비스를 다시 시작하십시오.

```
# systemctl restart kdump.service
```

결과적으로 설명된 시나리오에 **vmcore** 가 성공적으로 저장됩니다.

(BZ#1793389)

irqpoll 을 사용하면 **vmcore** 생성에 실패합니다.

AWS(Amazon Web Services) 클라우드 플랫폼에서 실행되는 64비트 **ARM** 아키텍처의 **nvme** 드라이버에 대한 기존 문제로 인해 첫 번째 커널에 **irqpoll** 커널 명령줄 매개변수를 제공할 때 **vmcore** 생성이 실패합니다. 결과적으로 커널 충돌 후 **/var/crash/** 디렉토리에 **vmcore** 파일이 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 **vmcore** 파일이 커널 충돌 시 캡처될 것으로 예상됩니다.

kdump 서비스는 상당한 양의 크래시 커널 메모리를 사용하여 **vmcore** 파일을 덤프할 수 있습니다. 캡처 커널에 **kdump** 서비스에 사용할 수 있는 메모리가 충분한지 확인합니다.

(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)

zlib 일부 압축 함수에서 **vmcore** 캡처 속도가 느려질 수 있습니다.

kdump 구성 파일은 기본적으로 **lzo** 압축 형식(**makedumpfile -l**)을 사용합니다. **zlib** 압축 형식(**makedumpfile -c**)을 사용하여 구성 파일을 수정할 때 **vmcore** 캡처 프로세스의 속도를 저하시키는 대신 압축 요인이 향상될 수 있습니다. 그 결과 **lzo**에 비해 **kdump**가 **zlib**를 사용하여 **vmcore**를 캡처하는 데 최대 4배 더 걸립니다.

따라서 속도가 주요 추진 요인인 경우에는 기본 **lzo**를 사용하는 것이 좋습니다. 그러나 대상 시스템이 사용 가능한 공간이 부족한 경우 **zlib**가 더 나은 옵션입니다.

(BZ#1790635)

HP NMI 위치독이 항상 크래시 덤프를 생성하지는 않음

경우에 따라 **HP NMI** 위치독의 **hpwdt** 드라이버는 **perfmon** 드라이버에서 **NMI(maskable interrupt)**를 사용했기 때문에 **HPE** 위치독 타이머에서 생성한 **NMI(NMI)**를 요청할 수 없습니다.

누락된 **NMI**는 다음 두 가지 조건 중 하나로 시작됩니다.

1. **iLO(Integrated Lights-Out)** 서버 관리 소프트웨어에서 **Generate NMI** 버튼. 이 버튼은 사용자가 트리거합니다.
2. **hpwdt watchdog**. 만료는 기본적으로 서버로 **NMI**를 보냅니다.

두 시퀀스 모두 시스템이 응답하지 않는 경우 일반적으로 발생합니다. 정상적인 상황에서 이러한 두 상황에 대한 **NMI** 핸들러는 커널 **panic()** 함수를 호출하고 구성된 경우 **kdump** 서비스에서 **vmcore** 파일을 생성합니다.

그러나 누락된 **NMI**로 인해 **kernel panic()**은 호출되지 않으며 **vmcore**는 수집되지 않습니다.

첫 번째 사례(1.)에서 시스템이 응답하지 않는 경우 그대로 유지됩니다. 이 시나리오를 수행하려면 **virtual Power(가상 전원)** 버튼을 사용하여 서버를 재설정하거나 전원을 끕니다.

두 번째 경우(2.) 누락된 NMI는 AAS(Automated System Recovery)에서 9초 후에 재설정됩니다.

HPE Gen9 Server 라인은 이 문제를 한 자리 숫자 비율로 경험합니다. Gen10은 훨씬 더 작은 빈도입니다.

(BZ#1602962)

`tuned-adm profile powersave` 명령을 사용하면 시스템이 응답하지 않습니다.

`tuned-adm profile powersave` 명령을 실행하면 이전 Thunderx(CN88x) 프로세서가 있는 Penguin Valkymaster 2000 2소켓 시스템이 응답하지 않는 상태가 됩니다. 그 결과 시스템을 재부팅하여 작동을 재개합니다. 이 문제를 해결하려면 시스템에서 언급된 사양과 일치하는 경우 **powersave** 프로필을 사용하지 마십시오.

(BZ#1609288)

기본값 7 4 1 7 `printk` 값으로 인해 임시 시스템이 응답하지 않는 경우가 있습니다.

기본값 7 4 1 7 `printk` 값을 사용하면 커널 활동을 더 효과적으로 디버깅할 수 있습니다. 그러나 직렬 콘솔과 결합되는 경우 이 출력으로 인해 I/O 버스트가 발생하여 RHEL 시스템이 일시적으로 응답하지 않을 수 있습니다. 이 문제를 해결하기 위해 새로운 **optimize-serial-console TuneD** 프로파일을 추가하여 기본 인쇄 장치 값을 4 4 1 7 로 줄였습니다. 사용자는 다음과 같이 시스템을 계측할 수 있습니다.

```
# tuned-adm profile throughput-performance optimize-serial-console
```

재부팅 시 인쇄자 값을 영구적으로 유지하면 시스템이 중단될 가능성이 줄어듭니다.

이 설정은 추가 디버깅 정보를 손실하는 대신 발생합니다.

새로 추가된 기능에 대한 자세한 내용은 [printk 값을 줄여서 I/O를 직렬 콘솔로 줄이는 새로운 optimize-serial-console TuneD 프로파일](#) 을 참조하십시오.

(JIRA:RHELPLAN-28940)

커널 ACPI 드라이버는 PCIe ECAM 메모리 리전에 액세스할 수 없음을 보고합니다.

펌웨어에서 제공하는 **ACPI(Advanced Configuration and Power Interface)** 표는 **PCI** 버스 장치의 현재 리소스 설정(**_CRS**) 방법의 **PCI** 버스에서 메모리 영역을 정의하지 않습니다. 결과적으로 시스템 부팅 중에 다음 경고 메시지가 발생합니다.

```
[ 2.817152] acpi PNP0A08:00: [Firmware Bug]: ECAM area [mem 0x300000000-0x31ffffff] not
reserved in ACPI namespace
[ 2.827911] acpi PNP0A08:00: ECAM at [mem 0x300000000-0x31ffffff] for [bus 00-1f]
```

그러나 커널이 **0x300000000-0x31ffff** 메모리 영역에 계속 액세스할 수 있으며 해당 메모리 지역을 **PCI ECAM(Enhanced Configuration Access Mechanism)**에 올바르게 할당할 수 있습니다. 다음 출력으로 **256**바이트 오프셋을 통해 **PCIe** 구성 공간에 액세스하여 **PCI ECAM**이 올바르게 작동하는지 확인할 수 있습니다.

```
03:00.0 Non-Volatile memory controller: Sandisk Corp WD Black 2018/PC SN720 NVMe SSD (prog-
if 02 [NVM Express])
```

```
...
```

```
Capabilities: [900 v1] L1 PM Substates
```

```
L1SubCap: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2+ ASPM_L1.1- L1_PM_Substates+
PortCommonModeRestoreTime=255us PortTPowerOnTime=10us
```

```
L1SubCtl1: PCI-PM_L1.2- PCI-PM_L1.1- ASPM_L1.2- ASPM_L1.1-
T_CommonMode=0us LTR1.2_Threshold=0ns
```

```
L1SubCtl2: T_PwrOn=10us
```

결과적으로 경고 메시지를 무시할 수 있습니다.

문제에 대한 자세한 내용은 "[Firmware Bug를 참조하십시오. ECAM 영역 mem 0x300000000-0x31ffffff in ACPI namespace](#)"는 시스템 부팅 솔루션 중에 표시됩니다.

(BZ#1868526)

OPEN MPI 라이브러리는 기본 **PML**을 사용하여 런타임 오류를 트리거할 수 있습니다.

OPEN MPI(Open Message Passing Interface) 구현 **4.0.x** 시리즈에서 **UKX(Unified Communication X)**는 기본 **PML(Point-to-Point Communicator)**입니다. 최신 버전의 **OPEN MPI 4.0.x** 시리즈의 경우 **openib Byte Transfer Layer(BTL)**가 더 이상 사용되지 않습니다.

그러나 동일 하드웨어 및 소프트웨어 구성 (동일한 하드웨어 및 소프트웨어 구성)을 통해 실행되는 경우, **UCX**는 여전히 **MPI** 단면 작업에 **openib BTL**을 사용합니다. 결과적으로 실행 오류가 발생할 수 있습니다. 이 문제를 해결하려면 다음을 수행합니다.

-

다음 매개변수를 사용하여 **mpirun** 명령을 실행합니다.

```
-mca btl openib -mca pml ucx -x UCX_NET_DEVICES=mlx5_ib0
```

다음과 같습니다.

- **mca btl openib** 매개 변수는 **openib BTL**을 비활성화합니다.
- **mca pml ucx** 매개 변수는 **OPEN MPI**를 구성하여 **PML**을 사용합니다.
- **x UCX_NET_DEVICES=** 매개 변수는 지정된 장치를 사용하도록 **UCX**를 제한합니다.

OPEN MPI는 이기종 클러스터(다양한 하드웨어 및 소프트웨어 구성)를 통해 실행할 때 **UCX**를 기본 **PML**으로 사용합니다. 결과적으로 **OPEN MPI** 작업이 잘못된 성능, 응답 없는 동작 또는 크래시 오류로 실행될 수 있습니다. 이 문제를 해결하려면 **UCX** 우선 순위를 다음과 같이 설정합니다.

- 다음 매개 변수를 사용하여 **mpirun** 명령을 실행합니다.

```
-mca pml_ucx_priority 5
```

결과적으로 **OPEN MPI** 라이브러리는 **UCX**를 통해 사용 가능한 대체 전송 계층을 선택할 수 있습니다.

(BZ#1866402)

5.7.7. 파일 시스템 및 스토리지

/boot 파일 시스템을 **LVM**에 배치할 수 없습니다.

LVM 논리 볼륨에 **/boot** 파일 시스템을 배치할 수 없습니다. 이 제한은 다음과 같은 이유로 존재합니다.

- **EFI** 시스템에서 **EFI 시스템 파티션**은 일반적으로 **/boot** 파일 시스템 역할을 합니다. **UEFI** 표준에는 이 파티션에 대한 특정 **GPT** 파티션 유형과 특정 파일 시스템 유형이 필요합니다.
- **RHEL 8**에서는 시스템 부팅 항목에 부트 로더 사양(**BLS**)을 사용합니다. 이 사양을 사용하려면 플랫폼 펌웨어에서 **/boot** 파일 시스템을 읽을 수 있어야 합니다. **EFI** 시스템에서 플랫폼 펌웨

어는 **uEFI** 표준에 정의된 **/boot** 구성만 읽을 수 있습니다.

- **GRUB 2** 부트 로더의 **LVM** 논리 볼륨에 대한 지원은 불완전합니다. 이 기능의 사용 사례 수가 **uEFI** 및 **BLS**와 같은 표준으로 인해 감소하기 때문에 **Red Hat**은 지원을 개선하지 않을 계획입니다.

Red Hat은 **LVM**에서 **/boot** 를 지원할 계획도 없습니다. 대신 **Red Hat**은 **/boot** 파일 시스템을 **LVM** 논리 볼륨에 배치할 필요가 없는 시스템 스냅샷 및 롤백을 관리하는 툴을 제공합니다.

(BZ#1496229)

LVM에서 더 이상 혼합 블록 크기가 있는 볼륨 그룹을 생성할 수 없습니다.

vgcreate 또는 **vgextend** 와 같은 **LVM** 유틸리티는 더 이상 물리 볼륨(**PV**)에 논리 블록 크기가 다른 **VG**(볼륨 그룹)를 만들 수 없습니다. **LVM**은 다른 블록 크기의 **PV**로 기본 논리 볼륨(**LV**)을 확장하는 경우 파일 시스템이 마운트되지 않으므로 이러한 변경을 채택했습니다.

혼합 블록 크기를 사용하여 **VG** 생성을 다시 활성화하려면 **lvm.conf** 파일에 **allow_embedded_block_sizes=1** 옵션을 설정합니다.

(BZ#1768536)

LVM writecache의 제한 사항

writecache **LVM** 캐싱 방법에는 캐시 방법에 없는 다음과 같은 제한 사항이 있습니다.

- **pvmove** 명령을 사용할 때는 **writecache** 논리 볼륨의 이름을 지정할 수 없습니다.
- 썬 폴 또는 **VDO**와 함께 **writecache** 가 있는 논리 볼륨을 사용할 수 없습니다.

다음 제한 사항은 캐시 메서드에도 적용됩니다.

- 캐시 또는 **writecache** 가 연결된 동안 논리 볼륨의 크기를 조정할 수 없습니다.

(JIRA:RHELPLAN-27987, [BZ#1798631](#), BZ#1808012)

LUKS 볼륨을 저장하는 **LVM** 미러 장치가 응답하지 않는 경우가 있음

LUKS 볼륨을 저장하는 세그먼트 유형의 미러 가 있는 **LVM** 장치는 특정 조건에서 응답하지 않을 수 있습니다. 응답하지 않는 장치는 모든 **I/O** 작업을 거부합니다.

이 문제를 해결하려면 복원력 있는 소프트웨어 정의 스토리지 위에 **LUKS** 볼륨을 스택해야 하는 경우 미러 대신 **RAID 1** 장치를 미러 유형인 **raid1** 과 함께 사용하는 것이 좋습니다.

raid1 세그먼트 유형은 기본 **RAID** 구성 유형이며 권장 솔루션으로 미러 를 바꿉니다.

미러 장치를 **RAID** 로 변환하려면 [미러링된 LVM 장치를 RAID1 장치로 변환](#)을 참조하십시오.

([BZ#1730502](#))

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](#))

5.7.8. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

getpwnam() 은 32비트 애플리케이션에 의해 호출될 때 실패할 수 있습니다.

NIS 사용자가 **getpwnam()** 함수를 호출하는 32비트 애플리케이션을 사용하는 경우 **nss_nis.i686** 패키지가 누락된 경우 호출이 실패합니다. 이 문제를 해결하려면 **yum install nss_nis.i686** 명령을 사용하여 누락된 패키지를 수동으로 설치합니다.

([BZ#1803161](#))

OpenLDAP 라이브러리 간의 기호 충돌로 인해 **httpd**에서 충돌이 발생할 수 있습니다.

OpenLDAP에서 제공하는 **libldap** 및 **libldap_r** 라이브러리가 모두 로드되고 단일 프로세스 내에서 사용되는 경우 이러한 라이브러리 간의 기호 충돌이 발생할 수 있습니다. 결과적으로 **httpd** 구성을 통해 **mod_security** 또는 **mod_auth_openidc** 모듈도 로드하는 경우 **PHP ldap** 확장을 사용하는 **Apache httpd** 하위 프로세스가 예기치 않게 종료될 수 있습니다.

APR(Apache Portable Runtime) 라이브러리에 대한 이번 업데이트를 통해 **httpd** 모듈을 로드할 때 **RTLD_DEEPBIND** 동적 링커 옵션을 사용할 수 있는 **APR_DEEPBIND** 환경 변수를 설정하여 문제를 해결할 수 있습니다. **APR_DEEPBIND** 환경 변수가 활성화되면 라이브러리를 로드하는 **httpd** 구성에서 충돌이 발생하지 않습니다.

(BZ#1819607)

PAM 플러그인이 **MariaDB**에서 작동하지 않음

MariaDB 10.3 은 **PAM**(Pluggable Authentication Modules) 플러그인 버전 **1.0**을 제공합니다. **MariaDB PAM** 플러그인 버전 **1.0**은 **RHEL 8**에서 작동하지 않습니다. 이 문제를 해결하려면 **RHEL 8.4**에서 사용할 수 있는 **mariadb:10.5** 모듈 스트림에서 제공하는 **PAM** 플러그인 버전 **2.0**을 사용합니다.

(BZ#1942330)

5.7.9. IdM (Identity Management)

모든 **KRA** 멤버가 숨겨진 복제본인 경우 **KRA** 설치에 실패합니다.

첫 번째 **KRA** 인스턴스가 숨겨진 복제본에 설치된 경우 **ipa-kra-install** 유틸리티는 **KRA**(키 복구 기관)가 이미 있는 클러스터에서 실패합니다. 결과적으로 클러스터에 **KRA** 인스턴스를 추가할 수 없습니다.

이 문제를 해결하려면 새 **KRA** 인스턴스를 추가하기 전에 **KRA** 역할이 있는 숨겨진 복제본을 숨기지 않습니다. **ipa-kra-install** 이 성공적으로 완료되면 다시 숨길 수 있습니다.

(BZ#1816784)

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)

PKI CA에 연결된 **PKI ACME** 응답자가 발행한 인증서는 **OCSP** 검증에 실패할 수 있습니다.

PKI CA에서 제공하는 기본 **ACME** 인증서 프로필에는 실제 **OCSP** 서비스를 가리키지 않는 샘플 **OCSP URL**이 포함되어 있습니다. 결과적으로 **PKI ACME** 응답자가 **PKI CA** 발행자를 사용하도록 구성된 경우 응답자가 발급한 인증서가 **OCSP** 검증에 실패할 수 있습니다.

이 문제를 해결하려면 `policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0` 속성을 `/usr/share/pki/ca/profiles/ca/acmeServerCert.cfg` 구성 파일의 빈 값으로 설정해야 합니다.

1. **ACME** 응답자 구성 파일에서 `policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=http://ocsp.example.com` 행을 `policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=` 로 변경합니다.
2. 서비스를 다시 시작하고 인증서를 다시 생성합니다.

결과적으로 **PKI CA**는 자동으로 생성된 **OCSP URL**을 사용하여 실제 **OCSP** 서비스를 가리키는 **ACME** 인증서를 생성합니다.

(BZ#1868233)

freeradswitch는 **249**자보다 긴 터널 암호를 자동으로 잘립니다.

터널 비밀번호가 **249**자를 초과하면 **FreeRADIUS** 서비스가 자동으로 잘립니다. 이로 인해 다른 시스템과 예기치 않은 암호 비호환성이 발생할 수 있습니다.

문제를 해결하려면 **249**자 이하의 암호를 선택하십시오.

(BZ#1723362)

IdM 호스트의 `/var/log/lastlog` 스파스 파일에서 성능 문제가 발생할 수 있습니다.

IdM 설치 중에 총 **10,000**개의 가능한 범위의 **UID** 범위가 임의로 선택되어 할당됩니다. 이와 같이 임의의 범위를 선택하면 향후 두 개의 별도의 **IdM** 도메인을 병합하기로 결정한 경우 **ID** 충돌 가능성이 크게 줄

어듭니다.

그러나 **UID**가 높으면 **/var/log/lastlog** 파일에 문제가 발생할 수 있습니다. 예를 들어 **UID**가 **1280000008**인 사용자가 **IdM** 클라이언트에 로그인하면 로컬 **/var/log/lastlog** 파일 크기가 거의 **400GB**로 증가합니다. 실제 파일은 스파스이고 모든 공간을 사용하지 않지만, 특정 애플리케이션은 기본적으로 스파스 파일을 식별하도록 설계되지 않으며 이를 처리하기 위해 특정 옵션이 필요할 수 있습니다. 예를 들어 설정이 복잡하고 백업이 있고 **copy** 애플리케이션이 스파스 파일을 올바르게 처리하지 않으면 파일이 크기가 **400GB**인 것처럼 복사됩니다. 이 동작으로 인해 성능 문제가 발생할 수 있습니다.

이 문제를 해결하려면 다음을 수행합니다.

- 표준 패키지의 경우 해당 문서를 참조하여 스파스 파일을 처리하는 옵션을 식별합니다.
- 사용자 지정 애플리케이션의 경우 **/var/log/lastlog** 와 같은 스파스 파일을 올바르게 관리할 수 있는지 확인합니다.

(JIRA:RHELPLAN-59111)

5.7.10. 데스크탑

소프트웨어 리포지토리에서 **flatpak** 리포지토리를 비활성화할 수 없습니다.

현재 **GNOME** 소프트웨어 유틸리티의 **Software Repositories**(소프트웨어 리포지토리) 도구에서 **flatpak** 리포지토리를 비활성화하거나 제거할 수 없습니다.

(BZ#1668760)

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)

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 8**을 게스트 운영 체

제로 사용하는 경우, 경우에 따라 VM이 부팅되지 않고 GRUB 부팅 메뉴로 돌아갑니다. 또한 Hyper-V 이벤트 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 2019를 호스트로 사용합니다.

(BZ#1583445)

5.7.11. 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 에서 radeon 을 비활성화합니다.

```
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)

단일 MST 토폴로지의 여러 디스플레이의 전원이 켜지지 않을 수 있습니다.

no 독립형 드라이버 와 함께 NVIDIA rpmsg GPU를 사용하는 시스템에서는 DisplayPort 허브(예: 랩탑 소켓)를 여러 모니터와 함께 사용하여 여기에 연결되면 켜지지 않을 수 있습니다. 이는 시스템이 모든 디스플레이를 지원하는 허브에 대역폭이 충분하지 않다고 잘못 생각하기 때문입니다.

(BZ#1812577)

sudo 명령을 사용하여 그래픽 애플리케이션을 실행할 수 없습니다

상승된 권한이 있는 사용자로 그래픽 애플리케이션을 실행하려고 하면 애플리케이션이 오류 메시지와 함께 열 수 없습니다. 인증에 일반 사용자 자격 증명을 사용하도록 **X authority** 파일에 의해 **X wayland**가 제한되므로 오류가 발생합니다.

이 문제를 해결하려면 **sudo -E** 명령을 사용하여 그래픽 애플리케이션을 루트 사용자로 실행합니다.

([BZ#1673073](#))

VNC 뷰어는 **IBM Z**에서 16비트 색상 깊이로 잘못된 색상 표시

16비트 색상 깊이의 **IBM Z** 서버의 **VNC** 세션에 연결할 때 **VNC** 뷰어 애플리케이션은 잘못된 색상으로 표시합니다.

이 문제를 해결하려면 **VNC** 서버에서 24비트 색상 깊이를 설정합니다. **Xvnc** 서버와 함께 **-depth 16** 옵션을 **Xvnc** 구성에서 **-depth 24**로 바꿉니다.

결과적으로 **VNC** 클라이언트는 올바른 컬러를 표시하지만 서버와 함께 더 많은 네트워크 대역폭을 사용합니다.

([BZ#1886147](#))

ARM에서는 하드웨어 가속 기능이 지원되지 않습니다.

내장 그래픽 드라이버는 64비트 **ARM** 아키텍처에서 하드웨어 가속 또는 **Vulc API**를 지원하지 않습니다.

하드웨어 가속 또는 **ARM**을 사용하려면 독점형 **Nvidia** 드라이버를 설치합니다.

([JIRA:RHELPLAN-57914](#))

NVIDIA Ampere로 **RHEL** 설치 프로그램이 응답하지 않음

RHEL 8.3.0은 **NVIDIA Ampere GPU**를 지원하지 않습니다. **NVIDIA Ampere GPU**가 있는 시스템에서 **RHEL** 설치를 시작하면 설치 프로그램이 응답하지 않습니다. 결과적으로 설치가 성공적으로 완료될 수

없습니다.

NVIDIA Ampere 제품군에는 다음과 같은 **GPU** 모델이 포함되어 있습니다.

- **redhat RTX 3060 Ti**
- **스키마 RTX 3070**
- **GeForce RTX 3080**
- **GeForce RTX 3090**
- **RTX A6000**
- **NVIDIA A40**
- **NVIDIA A100**
- **NVIDIA A100 80GB**

이 문제를 해결하려면 **no bootstrap graphics** 드라이버를 비활성화하고 텍스트 모드로 **RHEL**을 설치합니다.

1. 설치 프로그램의 부팅 메뉴로 부팅합니다.
2. 커널 명령줄에 **noCenter.modeset=0** 옵션을 추가합니다.

자세한 내용은 [부팅 옵션 편집](#)을 참조하십시오.

3. 시스템에 **RHEL**을 설치합니다.
4. 새로 설치한 **RHEL**으로 부팅합니다. 부팅 메뉴에 커널 명령줄에 **no Center.modeset=0** 옵션을 추가합니다.
5. **no proper department** 드라이버를 영구적으로 비활성화합니다.

```
# echo 'blacklist nouveau' >> /etc/modprobe.d/blacklist.conf
```

결과적으로 설치가 성공적으로 완료되고 **RHEL**이 텍스트 모드에서 실행됩니다.

선택적으로 전용 **NVIDIA GPU** 드라이버를 설치하여 그래픽을 활성화할 수 있습니다. 자세한 내용은 **RHEL 8에 NVIDIA 독점 드라이버를 설치하는 방법**을 참조하십시오.

(BZ#1903890)

5.7.12. 웹 콘솔

권한이 없는 사용자는 서브스크립션 페이지에 액세스할 수 있습니다.

관리자가 아닌 사용자가 웹 콘솔의 서브스크립션 페이지로 이동하면 웹 콘솔에 일반 오류 메시지 **Cockpit**에 예기치 않은 내부 오류가 표시되었습니다.

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)

5.7.13. Red Hat Enterprise Linux 시스템 역할

ovirt 입력 및 **elasticsearch** 출력 기능은 시스템 역할 로깅에서 지원되지 않습니다.

oVirt 입력 및 **elasticsearch** 출력은 **README** 파일에 언급되어 있지만 시스템 역할 로깅에서는 지원되지 않습니다. 현재 해결방법은 없습니다.

([BZ#1889468](#))

5.7.14. 가상화

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- destroy**와 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](#))

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](#))

virtio-blk를 사용하여 가상 머신에 LUN 장치를 연결하는 것은 작동하지 않습니다

q35 시스템 유형은 전환된 **virtio 1.0** 장치를 지원하지 않으므로 RHEL 8에는 **virtio 1.0**에서 더 이상 사용되지 않는 기능에 대한 지원이 없습니다. 특히 RHEL 8 호스트에서는 **virtio-blk** 장치에서 SCSI 명령을 보낼 수 없습니다. 결과적으로 **virtio-blk** 컨트롤러를 사용하면 가상 머신에 LUN 장치로 물리적 디스크를 연결할 수 없습니다.

실제 디스크를 게스트 운영 체제로 전달할 수 있지만 **device='lun'**이 아닌 **device='disk'** 옵션을 사용하여 구성해야 합니다.

(BZ#1777138)

호스트에서 **TSX** 가 비활성화된 경우 **lake** 를 사용하는 가상 머신을 부팅할 수 없습니다.

QCOW lake CPU 모델을 사용하는 **VM**(가상 머신)은 현재 호스트에서 **TSX CPU** 플래그를 조정할 때 부팅되지 않습니다. 대신 호스트에 다음 오류 메시지가 표시됩니다.

```
the CPU is incompatible with host CPU: Host CPU does not provide required features: hle, rtm
```

이러한 호스트에서 가상 머신을 사용할 수 있도록 하려면 **VM** 구성에서 **HLE**, **RTM** 및 **TAA_NO** 플래그를 비활성화합니다.

```
<feature policy='disable' name='hle'/>
<feature policy='disable' name='rtm'/>
<feature policy='disable' name='taa-no'/>
```

(BZ#1860743)

Witherspoon 호스트에서 가상 머신을 부팅할 수 없는 경우가 있습니다

경우에 따라 **DD2.2** 또는 **DD2.3 CPU**를 사용하는 **HPC 호스트**(*Forderpoon*이라고도 함)용 **Power9 S922LC**에서 **pseries-rhel7.6.0-sxxm** 시스템 유형을 사용하는 **VM**(가상 머신)에서 부팅하지 못할 수도 있습니다.

이러한 **VM**을 부팅하려고 하면 다음과 같은 오류 메시지가 생성됩니다.

```
qemu-kvm: Requested safe indirect branch capability level not supported by kvm
```

이 문제를 해결하려면 다음과 같이 **VM**의 **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)

5.7.15. 클라우드 환경의 RHEL

Azure NV6 인스턴스의 GPU 문제

Microsoft Azure NV6 인스턴스에서 RHEL 8을 게스트 운영 체제로 실행하는 경우 **hibernation**에서 VM(가상 머신)을 다시 시작하면 VM의 GPU가 잘못 작동하는 경우가 있습니다. 이 경우 커널은 다음 메시지를 기록합니다.

```
hv_irq_unmask() failed: 0x5
```

(BZ#1846838)

Kdump가 Azure 및 Hyper-V에서 시작되지 않는 경우가 있습니다.

Microsoft Azure 또는 Hyper-V 하이퍼바이저에서 호스팅되는 RHEL 8 게스트 운영 체제에서는 실행 후 알림기를 활성화하면 kdump 커널을 시작할 수 없는 경우가 있습니다.

이 문제를 해결하려면 크래시 **kexec** 후 알림기를 비활성화합니다.

```
# echo N > /sys/module/kernel/parameters/crash_kexec_post_notifiers
```

(BZ#1865745)

VMWare 호스트의 RHEL 8 가상 머신에서 고정 IP 설정이 작동하지 않음

현재 RHEL 8을 VMWare 호스트에서 VM(가상 머신)의 게스트 운영 체제로 사용할 때 **DatasourceOVF** 기능이 제대로 작동하지 않습니다. 결과적으로 **cloud-init** 유틸리티를 사용하여 VM의 네트워크를 고정 IP로 설정한 다음 VM을 재부팅하면 VM의 네트워크가 **DHCP**로 변경됩니다.

(BZ#1750862)

특정 NIC가 있는 코어 덤프 RHEL 8 가상 머신을 Azure의 원격 머신에 추가하는 데 예상보다 시간이 오래 걸립니다.

현재 **kdump** 유틸리티를 사용하여 Microsoft Azure 하이퍼바이저에 RHEL 8 가상 머신(VM)의 코어 덤프 파일을 원격 머신에 저장하면 VM이 가속화된 네트워킹이 활성화된 NIC를 사용하는 경우 올바르게 작동하지 않습니다. 결과적으로 덤프 파일은 즉시 대신 약 200초 후에 저장됩니다. 또한 덤프 파일을 저장하기 전에 다음 오류 메시지가 콘솔에 기록됩니다.

```
device (eth0): linklocal6: DAD failed for an EUI-64 address
```

(BZ#1854037)

가상 머신이 최대 절전 모드를 시작한 후 **TX/RX** 패킷 카운터가 증가하지 않습니다.

CX4 VF NIC와 함께 **RHEL 8** 가상 시스템(**VM**)이 있는 경우 **TX/RX** 패킷 카운터가 증가하지 않으며 **Microsoft Azure**에서 최대 절전 모드가 다시 시작됩니다. 카운터가 작동 상태로 유지하려면 **VM**을 다시 시작합니다. 이렇게 하면 카운터가 재설정됩니다.

(BZ#1876527)

RHEL 8 가상 머신이 **Azure**의 최대 절전 모드로 다시 시작되지 않음

SR-IOV가 활성화된 **RHEL 8** 가상 머신(**VM**)이 활성화된 경우 **VF**(가상 기능), **vmbus** 장치의 **GUID**가 최대 절전 상태이며 **Microsoft Azure**에 할당될 때 변경됩니다. 결과적으로 **VM**이 다시 시작되면 다시 시작하고 충돌하지 못합니다. 이 문제를 해결하려면 **Azure** 직렬 콘솔을 사용하여 **VM**을 하드 재설정합니다.

(BZ#1876519)

RHEL 7-ALT 호스트에서 **RHEL 8**로 **POWER9** 게스트 마이그레이션에 실패

현재 **POWER9** 가상 머신을 **RHEL 7-ALT** 호스트 시스템에서 **RHEL 8**로 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)

5.7.16. 지원 관련 기능

redhat-support-tool이 **FUTURE** 암호화 정책에서 작동하지 않음

고객 포털 **API**의 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 **API**에 연결하는 동안 **DEFAULT** 암호화 정책을 사용하십시오.

([BZ#1802026](#))

5.7.17. 컨테이너

UDICA는 1.0의 안정적인 스트림을 사용할 것으로 예상되지 않습니다.

컨테이너에 대한 **SELinux** 정책을 생성하는 도구인 **UDICA**는 **container-tools:1.0** 모듈 스트림에서 **podman 1.0.x**를 통해 실행되는 컨테이너와 호환되지 않습니다.

([JIRA:RHELPLAN-25571](#))

Podman 시스템 연결 추가가 기본 연결을 자동으로 설정하지 않음

podman system connection add 명령은 첫 번째 연결을 기본 연결로 자동 설정하지 않습니다. 기본 연결을 설정하려면 **podman system connection default <connection_name>** 명령을 수동으로 실행해야 합니다.

([BZ#1881894](#))

6장. 국제화

6.1. 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, libhangul

6.2. 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 사용](#)을 참조하십시오.
- 다수의 **glibc** 로케일이 **Unicode Common Locale Data Repository(CLDLDR)**와 동기화되었습니다.

부록 A. 구성 요소별 티켓 목록

Bugzilla 및 **JIRA ID**는 참조를 위해 이 문서에 나열되어 있습니다. 공개적으로 액세스할 수 있는 **Bugzilla** 버그에는 티켓 링크가 포함되어 있습니다.

구성 요소	티켓
389-ds-base	BZ#1816862 , BZ#1638875 , BZ#1728943
NetworkManager	BZ#1814746 , BZ#1626348
anaconda	BZ#1665428 , BZ#1775975 , BZ#1630299 , BZ#1823578 , BZ#1672405 , BZ#1644662 , BZ#1745064 , BZ#1821192 , BZ#1822880 , BZ#1862116 , BZ#1890261 , BZ#1891827 , BZ#1691319 , BZ#1931069
apr	BZ#1819607
authselect	BZ#1654018
bcc	BZ#1837906
bind	BZ#1818785
buildah-container	BZ#1627898
buildah	BZ#1806044
clevis	BZ#1716040 , BZ#1818780 , BZ#1436735 , BZ#1819767
cloud-init	BZ#1750862
cloud-utils-growpart	BZ#1846246
cockpit-session-recording	BZ#1826516
cockpit	BZ#1710731 , BZ#1666722
corosync-qdevice	BZ#1784200
crun	BZ#1841438
crypto-policies	BZ#1832743 , BZ#1660839
cyrus-sasl	BZ#1817054
distribution	BZ#1815402 , BZ#1657927

구성 요소	티켓
dnf	BZ#1793298 , BZ#1832869 , BZ#1842285
elfutils	BZ#1804321
fapolicyd	BZ#1897090 , BZ#1817413 , BZ#1714529
fence-agents	BZ#1830776 , BZ#1775847
firewalld	BZ#1790948 , BZ#1682913 , BZ#1809225 , BZ#1817205 , BZ#1809636
freeradius	BZ#1672285 , BZ#1859527 , BZ#1723362
gcc-toolset-10-gdb	BZ#1838777
gcc	BZ#1784758
gdb	BZ#1659535
Git	BZ#1825114
glibc	BZ#1812756 , BZ#1743445 , BZ#1783303 , BZ#1642150 , BZ#1810146 , BZ#1748197 , BZ#1774115 , BZ#1807824 , BZ#1757354 , BZ#1836867 , BZ#1780204 , BZ#1821531 , BZ#1784525
gnome-session	BZ#1739556
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1724302
gnome-software	BZ#1668760
gnutls	BZ#1677754 , BZ#1789392 , BZ#1849079 , BZ#1855803
go-toolset	BZ#1820596
gpgme	BZ#1829822
grafana-container	BZ#1823834
grafana-pcp	BZ#1807099
grafana	BZ#1807323

구성 요소	티켓
grub2	BZ#1583445
httpd	BZ#1209162
initial-setup	BZ#1676439
ipa-healthcheck	BZ#1852244
ipa	BZ#1816784 , BZ#1810154 , BZ#913799 , BZ#1651577 , BZ#1851139 , BZ#1664719 , BZ#1664718
iperf3	BZ#1665142 , BZ#1700497
jss	BZ#1821851
kernel-rt	BZ#1818138
kernel	BZ#1758323 , BZ#1812666 , BZ#1793389 , BZ#1694705 , BZ#1748451 , BZ#1654962 , BZ#1792125 , BZ#1708456 , BZ#1812577 , BZ#1757933 , BZ#1847837 , BZ#1791664 , BZ#1666538 , BZ#1602962 , BZ#1609288 , BZ#1730502 , BZ#1806882 , BZ#1660290 , BZ#1846838 , BZ#1865745 , BZ#1868526 , BZ#1884857 , BZ#1854037 , BZ#1876527 , BZ#1876519 , BZ#1823764 , BZ#1822085 , BZ#1735611 , BZ#1281843 , BZ#1828642 , BZ#1825414 , BZ#1761928 , BZ#1791041 , BZ#17965 , BZ#1834769 , BZ#1785660 , BZ#1683394 , BZ#1817752 , BZ#1782831 , BZ#1821646 , BZ#1519039 , BZ#1627455 , BZ#1501618 , BZ#1495358 , BZ#1633143 , BZ#1503672 , BZ#1570255 , BZ#1696451 , BZ#1348508 , BZ#1778762 , BZ#1839311 , BZ#1783396 , BZ#1665295 , BZ#1658840 , BZ#1660627 , BZ#1569610
krb5	BZ#1791062 , BZ#1784655 , BZ#1820311 , BZ#1802334 , BZ#1877991
libbpf	BZ#1759154
libcap	BZ#1487388
libdb	BZ#1670768
libffi	BZ#1723951
libgnome-keyring	BZ#1607766
libkcapi	BZ#1683123
libmaxminddb	BZ#1642001

구성 요소	티켓
libpcap	BZ#1806422
libreswan	BZ#1544463 , BZ#1820206
libseccomp	BZ#1770693
libselinux-python-2.8-module	BZ#1666328
libssh	BZ#1804797
libvirt	BZ#1664592 , BZ#1528684
lldb	BZ#1841073
llvm-toolset	BZ#1820587
llvm	BZ#1820319
lshw	BZ#1794049
lvm2	BZ#1496229 , BZ#1768536 , BZ#1598199 , BZ#1541165 , JIRA:RHELPLAN-39320
mariadb	BZ#1942330
Memcached	BZ#1809536
Mesa	BZ#1886147
microdnf	BZ#1781126
mod_http2	BZ#1814236
nfs-utils	BZ#1817756 , BZ#1592011
nginx	BZ#1668717 , BZ#1826632
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1817533 , BZ#1645153
opencryptoki	BZ#1780293

구성 요소	티켓
openmpi	BZ#1866402
opensc	BZ#1810660
openscap	BZ#1803116 , BZ#1870087 , BZ#1795563 , BZ#1824152 , BZ#1829761
openssh	BZ#1744108
openssl	BZ#1685470, BZ#1810911
oscap-anaconda-addon	BZ#1816199, BZ#1665082, BZ#1674001 , BZ#1691305, BZ#1787156 , BZ#1843932 , BZ#1834716
pacemaker	BZ#1828488 , BZ#1784601 , BZ#1837747, BZ#1718324
papi	BZ#1807346, BZ#1664056 , BZ#1726070
pcp-container	BZ#1497296
pcp	BZ#1792971
pcs	BZ#1817547, BZ#1684676 , BZ#1839637 , BZ#1619620
perl-5.30-module	BZ#1713592
perl-IO-Socket-SSL	BZ#1824222
perl-libwww-perl	BZ#1781177
php	BZ#1797661
pki-core	BZ#1729215 , BZ#1868233 , BZ#1770322, BZ#1824948
podman	BZ#1804193 , BZ#1881894 , BZ#1627899
powertop	BZ#1783110
pykickstart	BZ#1637872
python38	BZ#1847416
qemu-kvm	BZ#1719687 , BZ#1860743 , JIRA:RHELPLAN-45901, BZ#1651994
교체	BZ#1843809 , BZ#1729502 , BZ#1743303

구성 요소	티켓
redhat-support-tool	BZ#1802026
resource-agents	BZ#1814896
rhel-system-roles-sap	BZ#1844190 , BZ#1660832
rhel-system-roles	BZ#1889468 , BZ#1822158 , BZ#1677739
rpm	BZ#1688849
rsyslog	BZ#1659383 , JIRA:RHELPLAN-10431 , BZ#1679512 , BZ#1713427
ruby-2.7-module	BZ#1817135
ruby	BZ#1846113
rust-toolset	BZ#1820593
samba	BZ#1817557 , JIRA:RHELPLAN-13195
scap-security-guide	BZ#1843913 , BZ#1858866 , BZ#1750755 , BZ#1760734 , BZ#1832760 , BZ#1815007
scap-workbench	BZ#1640715
selinux-policy	BZ#1826788 , BZ#1746398 , BZ#1776873 , BZ#1772852 , BZ#1641631 , BZ#1860443
setools	BZ#1820079
skopeo-container	BZ#1627900
smartmontools	BZ#1671154
spice	BZ#1849563
squid	BZ#1829467
sssd	BZ#1827615 , BZ#1793727
stratis-cli	BZ#1734496
stunnel	BZ#1808365
subscription-manager	BZ#1674337

구성 요소	티켓
sudo	BZ#1786990
systemtap	BZ#1804319
Tang	BZ#1716039
tcpdump	BZ#1804063
tigervnc	BZ#1806992
tpm2-tools	BZ#1789682
tuned	BZ#1792264 , BZ#1840689 , BZ#1746957
udica	BZ#1763210
usbguard	BZ#1738590 , BZ#1667395 , BZ#1683567
valgrind	BZ#1804324
Wayland	BZ#1673073
xdp-tools	BZ#1880268 , BZ#1820670
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1698565
yum	BZ#1788154

구성 요소	티켓
기타	JIRA:RHELPLAN-45950, JIRA:RHELPLAN-57572, BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1790635, BZ#1823398, BZ#1757877, JIRA:RHELPLAN-25571, BZ#1777138, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, BZ#1897383, BZ#1900019, BZ#1839151, BZ#1780124, JIRA:RHELPLAN-42395, BZ#1889736, BZ#1842656, JIRA:RHELPLAN-45959, JIRA:RHELPLAN-45958, JIRA:RHELPLAN-45957, JIRA:RHELPLAN-45956, JIRA:RHELPLAN-45952, JIRA:RHELPLAN-45945, JIRA:RHELPLAN-45939, JIRA:RHELPLAN-45937, JIRA:RHELPLAN-45936, JIRA:RHELPLAN-45930, JIRA:RHELPLAN-45926, JIRA:RHELPLAN-45922, JIRA:RHELPLAN-45920, JIRA:RHELPLAN-45918, JIRA:RHELPLAN-45916, JIRA:RHELPLAN-45915, JIRA:RHELPLAN-45911, JIRA:RHELPLAN-45910, JIRA:RHELPLAN-45909, JIRA:RHELPLAN-45908, JIRA:RHELPLAN-45906, JIRA:RHELPLAN-45904, JIRA:RHELPLAN-45900, JIRA:RHELPLAN-45899, JIRA:RHELPLAN-45884, JIRA:RHELPLAN-37573, JIRA:RHELPLAN-37570, JIRA:RHELPLAN-49954, JIRA:RHELPLAN-50002, JIRA:RHELPLAN-43531, JIRA:RHELPLAN-48838, BZ#1873567, BZ#1866695, JIRA:RHELPLAN-14068, JIRA:RHELPLAN-7788, JIRA:RHELPLAN-40469, JIRA:RHELPLAN-42617, JIRA:RHELPLAN-30878, JIRA:RHELPLAN-37517, JIRA:RHELPLAN-55009, JIRA:RHELPLAN-42396, BZ#1836211, JIRA:RHELPLAN-57564, JIRA:RHELPLAN-57567, BZ#1890499, JIRA:RHELPLAN-40234, JIRA:RHELPLAN-56676, JIRA:RHELPLAN-14754, JIRA:RHELPLAN-51289, BZ#1893174, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1889737, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-41549, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057, BZ#1748980, BZ#1827628, BZ#1871025, BZ#1871953, BZ#1874892, BZ#1893767, JIRA:RHELPLAN-60226

부록 B. 개정 내역

0.3-4

4월 29일, LRKKKKKKKK (Ispackova@redhat.com)

- 더 이상 사용되지 않는 기능 소개가 업데이트되었습니다.
- [BZ#1605216](#) 의 고정 오타.
- 손상된 링크가 수정되었습니다.

0.3-3

Tue 05 2022, Jaroslav Klech (jklech@redhat.com)

- 버그 수정 [BZ#1666538](#) (Kernel)이 추가되었습니다.

0.3-2

Thu Mar 17 2022, Jaroslav Klech (jklech@redhat.com<mailto:jklech@redhat.com>)

- 알려진 문제(커널)를 추가했습니다.

0.3-1

2022년 2월 04일, Lucie Mahieraskovoctets([참조하십시오](#)).

- 더 이상 사용되지 않는 기능 [BZ#1794513](#) (Filesystem 및 스토리지)이 추가되었습니다.

0.3-0

2021년 12월 23일 목요일, 기니카 -파파산라(Ispackova@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.

0.2-9

2021년 10월 07일, 룰카 -파파산라(lspackova@redhat.com)

- 알려진 문제 [BZ#1942330](#) (동적 프로그래밍 언어, 웹 및 데이터베이스 서버) 업데이트.

0.2-8

2021년 10월 5일 화요일, Lucie Maás(Imanasko@redhat.com)

- 더 이상 사용되지 않는 기능 [BZ#1999620](#) (Shells 및 명령줄 툴)이 추가되었습니다.

0.2-7

2021년 8월 19일 목요일, Lucie Maás(Imanasko@redhat.com)

- [YUM/DNF](#)를 사용한 패키지 관리가 배포 장에 추가되었습니다.
- [BZ#1708456](#) (Krenel)의 텍스트를 업데이트합니다.

0.2-6

2021년 7월 9일 금요일, Lucie Maás(Imanasko@redhat.com)

- [JIRA](#)의 업데이트된 텍스트: [RHELPLAN-34199](#)(보안).

0.2-5

2021년 6월 23일 수요일, Lucie Maás(Imanasko@redhat.com)

- [BZ#1922488](#) (Desktop)에서 AlternateTab 제거에 대한 정보가 추가되었습니다.

0.2-4

2021년 5월 21일 금요일, 메카 -파파산라(lspackova@redhat.com)

- [개요](#)의 OS 변환에 대한 업데이트된 정보.

0.2-3

2021년 5월 20일, Valka pačá(lspackova@redhat.com)

- 알려진 문제 [BZ#1942330](#) (동적 프로그래밍 언어, 웹 및 데이터베이스 서버)에 해결 방법을 추가했습니다.

0.2-2

2021년 5월 14일 금요일, Lucie Maásá(Imanasko@redhat.com)

- .NET 5 지원(Compilers 및 개발 툴)에 대한 새로운 기능 [BZ#1944677](#) 추가.
- 새 기능 [xfer:BZ-1959289\[BZ#1959289\]](#) (RHEL 시스템 역할)를 추가했습니다.
- [BZ#1820670](#)(네트워킹) 및 [BZ #1780124](#) (Kernel)의 xdp-tools 패키지에 대한 정보가 업데이트되었습니다.

0.2-1

2021년 4월 19일, Lenka pačá(lspackova@redhat.com)

- 알려진 문제 [BZ#1942330](#) (동적 프로그래밍 언어, 웹 및 데이터베이스 서버) 추가.

0.2-0

2021년 4월 13일 화요일, 기니카 -파파산라(lspackova@redhat.com)

- 알려진 문제(설치 프로그램 및 이미지 생성)가 추가되었습니다.

0.1-9

2021년 4월 6일 화요일, 메카 -파파산라(lspackova@redhat.com)

- 지원되는 아키텍처 목록 개선.

0.1-8

2021년 3월 31일 수요일, 커넬카 -파파산라(lspackova@redhat.com)

- 지원되는 **Convert2RHEL** 유틸리티의 가용성과 함께 **OS** 변환에 대한 정보가 업데이트되었습니다.

0.1-7

2021년 3월 29일, Lucie Maásá(Imanasko@redhat.com)

- 새 기능 섹션(커널)을 업데이트합니다.

0.1-6

2021년 2월 25일, 커넬카 -파파산라(lspackova@redhat.com)

- 고정 **CentOS Linux** 이름.

0-1-5

2021년 2월 23일 화요일, Lucie Maásá(Imanasko@redhat.com)

- 알려진 문제(ID 관리) 추가.
- **podman** 유틸리티 리베이스에 대한 참고 사항을 **RHEL 8.3.1** 섹션에 추가합니다.

0-1-4

2021년 2월 18일 목요일, Jaroslav Klech(jklech@redhat.com)

- 알려진 문제(커널) 추가.
- 기능 향상을 위한 링크 수정(Kernel).

0-1-3

2021년 2월 16일 화요일, Lenka Pačá(lspackova@redhat.com)

- Red Hat Enterprise Linux 8.3.1 릴리스 노트.
- 개요에서 [RHBA-2021:0569](#) 권고 릴리스로 내부 업그레이드 섹션 업데이트.

0-1-2

2021년 2월 12일 금요일, Lucie Maášá(lmanasko@redhat.com)

- 두 가지 알려진 문제(Security, Installer)가 추가되었습니다.

0-1-1

2021년 2월 10일 수요일, Lucie Maášá(lmanasko@redhat.com)

- 알려진 문제(가상화) 추가.

0-1-0

2021년 2월 3일 수요일, Lenka Pačá(lspackova@redhat.com)

- **ip** 매개 변수(네트워킹) 아래의 커널 명령줄에서 네트워크 구성 통합에 대한 내용을 추가했습니다.
- 더 이상 사용되지 않는 패키지에 **Mercurial**이 추가되었습니다.

- **Witherspoon** 호스트(가상화)와 관련된 알려진 문제가 추가되었습니다.

0-0-9

2021년 1월 29일 금요일, Lucie Maásá(Imanasko@redhat.com)

- 새로운 버그 수정 설명 (**Security**)을 추가했습니다.
- **mailman** 패키지 사용 중단(소프트웨어 관리)에 대한 참고 사항이 추가되었습니다.
- 새 기능 섹션 업데이트(보안, ID 관리).
- **systemd-resolved** 서비스에 대한 기술 프리뷰 노트 추가.
- 기타 마이너 업데이트.

0.0-8

2020년 12월 14일, Lucie Maásá(Imanasko@redhat.com)

- 알려진 문제 섹션과 버그 수정 섹션이 업데이트되었습니다.

0.0-7

2020년 11월 27일 금요일, Lucie Maásá(Imanasko@redhat.com)

- **fapolicyd (Security)**와 관련된 버그 수정을 추가했습니다.
- 버그 수정 섹션의 추가 업데이트.
- **Podman varlink** 기반 **REST API V1**(컨테이너) 사용 중단에 대한 참고 사항이 추가되었습니다.

- 새 기능 섹션 업데이트.
- **lorax-composer** 백엔드에서 새로운 **osbuild-composer** 백엔드(**Image Builder**)로 청사진 복제에 대한 새로운 인식 문제가 추가되었습니다.

0.0-6

2020년 11월 20일 금요일, Lucie Maásá(Imanasko@redhat.com)

- **OpenSCAP** 버그 수정 설명(보안)을 추가했습니다.
- 새 기능 섹션(소프트웨어 관리) 업데이트.

0.0-5

2020년 11월 18일 수요일, Lenka Pačá(Ispackova@redhat.com)

- **Oracle Linux** 또는 **CentOS Linux**에서 **RHEL**로의 변환에 대한 정보 추가(**Overview**).

0.0-4

2020년 11월 12일 목요일, 기니카 -파파산라(Ispackova@redhat.com)

- **RHEA-2020:5101** 권고와 함께 릴리스된 **Node.js 14.15.0**에 대한 정보가 추가되었습니다.

0.0-3

2020년 11월 11일 수요일, Lucie Maásá(Imanasko@redhat.com)

- 새로운 기능에 대해 **OPA(Host software software)**에 대한 설명 추가.

0.0-2

2020년 11월 9일, 기니카 -파파산라(Ispackova@redhat.com)

- **Intel Tiger Lake graphics**를 기술 프리뷰(**Graphics 인프라**)로 추가.

0.0-1

2020년 11월 4일 수요일, [Lucie Maasko](mailto:Lucie.Maasko@redhat.com)(Lucie.Maasko@redhat.com)

- **Red Hat Enterprise Linux 8.3 릴리스 노트.**

0.0-0

2020년 7월 28일 화요일, [Lucie Maasko](mailto:Lucie.Maasko@redhat.com)(Lucie.Maasko@redhat.com)

- **Red Hat Enterprise Linux 8.3 베타 릴리스 노트 릴리스.**