Red Hat Enterprise Linux 8

8.4 릴리스 노트

Red Hat Enterprise Linux 8.4 릴리스 정보

Last Updated: 2022-07-03

Red Hat Enterprise Linux 8 8.4 릴리스 노트

Red Hat Enterprise Linux 8.4 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

초록

릴리스 노트에서는 Red Hat Enterprise Linux 8.4에서 구현된 개선 사항 및 추가 사항에 대해 개략적으로 설명하고 이번 릴리스의 알려진 문제와 주요 버그 수정, 기술 프리뷰, 사용되지 않는 기능 및 기타 세부 사항을 문서화합니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체 5

RED HAT 문서에 관한 피드백 제공 6

1장. 개요 7
1.1. RHEL 8.4의 주요 변경 사항 7
보안 7
네트워킹 7
커널 7
고가용성 및 클러스터 8
동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버 8
컴파일러 및 개발 도구 8
OpenJDK 11 사용 가능 8
IdM (Identity Management) 8
1.2. 즉각적 업그레이드 및 OS 변환 9
RHEL 7에서 RHEL 8으로의 즉각적 업그레이드 9
RHEL 6에서 RHEL 8로 즉각적 업그레이드 9
다른 Linux 배포판에서 RHEL로 변환 9
1.3. RED HAT CUSTOMER PORTAL 랩 9
1.4. 추가 리소스 10

2장. 아키텍처 11

3장. RHEL 8의 콘텐츠 배포 12
3.1. 설치 12
3.2. 리포지토리 12
3.3. APPLICATION STREAMS 12
3.4. YUM/DNF를 사용한 패키지 관리 13

4장. 새로운 기능 14
4.1. 설치 프로그램 및 이미지 생성 14
4.2. 에지용 RHEL 14
4.3. 소프트웨어 관리 15
4.4. 쉘 및 명령행 툴 16
4.5. 인프라 서비스 21
4.6. 보안 26
4.7. 네트워킹 34
4.8. 커널 37
4.9. 파일 시스템 및 스토리지 50
4.10. 고가용성 및 클러스터 55
4.11. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버 57
4.12. 컴파일러 및 개발 도구 69
4.13. IDM (IDENTITY MANAGEMENT) 85
4.14. 데스크탑 93
4.15. 그래픽 인프라 94
4.16. 웹 콘솔 99
4.17. RED HAT ENTERPRISE LINUX 시스템 역할 100
4.18. 가상화 103
4.19. 클라우드 환경의 RHEL 104
4.20. 지원 관련 기능 104
4.21. 컨테이너 107

5장. 외부 커널 매개변수로 중요한 변경 110

5.1. 새 커널 매개변수 110
5.2. 새로운 /PROC/SYS/USER 매개변수 112
5.3. 새로운 /PROC/SYS/VM 매개변수 112

6장. 장치 드라이버 114
6.1. 새 드라이버 114
네트워크 드라이버 114
그래픽 드라이버 및 기타 드라이버 114
6.2. 업데이트된 드라이버 116
그래픽 및 기타 드라이버 업데이트 116

7장. 버그 수정 118
7.1. 설치 프로그램 및 이미지 생성 118
7.2. 소프트웨어 관리 119
7.3. 쉘 및 명령행 툴 120
7.4. 인프라 서비스 121
7.5. 보안 122
7.6. 네트워킹 126
7.7. 커널 127
7.8. 파일 시스템 및 스토리지 130
7.9. 고가용성 및 클러스터 131
7.10. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버 131
7.11. 컴파일러 및 개발 도구 132
7.12. IDM (IDENTITY MANAGEMENT) 134
7.13. 그래픽 인프라 135
7.14. RED HAT ENTERPRISE LINUX 시스템 역할 135
7.15. 가상화 136
7.16. 클라우드 환경의 RHEL 136
7.17. 컨테이너 138

8장. 기술 프리뷰 139
8.1. 설치 프로그램 및 이미지 생성 139
8.2. 네트워킹 139
8.3. 커널 143
8.4. 파일 시스템 및 스토리지 145
8.5. 고가용성 및 클러스터 149
8.6. IDM (IDENTITY MANAGEMENT) 150
8.7. 데스크탑 153
8.8. 그래픽 인프라 153
8.9. RED HAT ENTERPRISE LINUX 시스템 역할 154
8.10. 가상화 155
8.11. 컨테이너 158

9장. 사용되지 않는 기능 159
9.1. 설치 프로그램 및 이미지 생성 159
9.2. 소프트웨어 관리 161
9.3. 쉘 및 명령행 툴 161
9.4. 보안 162
9.5. 네트워킹 164
9.6. 커널 165
9.7. 플랫폼 지원 166
9.8. 파일 시스템 및 스토리지 166
9.9. 고가용성 및 클러스터 169
9.10. 컴파일러 및 개발 도구 169

9.11. IDM (IDENTITY MANAGEMENT) 170
9.12. 데스크탑 173
9.13. 그래픽 인프라 173
9.14. 웹 콘솔 174
9.15. RED HAT ENTERPRISE LINUX 시스템 역할 174
9.16. 가상화 174
9.17. 컨테이너 176
9.18. 사용되지 않는 패키지 176
9.19. 사용되지 않는 장치 180

10장. 확인된 문제 183
10.1. 설치 프로그램 및 이미지 생성 183
10.2. 서브스크립션 관리 188
10.3. 인프라 서비스 188
10.4. 보안 189
10.5. 네트워킹 197
10.6. 커널 197
10.7. 하드웨어 활성화 205
10.8. 파일 시스템 및 스토리지 205
10.9. 고가용성 및 클러스터 207
10.10. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버 208
10.11. 컴파일러 및 개발 도구 209
10.12. IDM (IDENTITY MANAGEMENT) 211
10.13. 데스크탑 213
10.14. 그래픽 인프라 214
10.15. 가상화 216
10.16. 클라우드 환경의 RHEL 220
10.17. 지원 관련 기능 224

11장. 국제화 226
11.1. RED HAT ENTERPRISE LINUX 8 국제 언어 226
11.2. RHEL 8 국제화의 주요 변경 사항 227

부록 A. 구성 요소별 티켓 목록 228

부록 B. 개정 내역 237

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

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

1.1. RHEL 8.4의 주요 변경 사항

보안
Libreswan에서 제공하는 **IPsec VPN** 은 IKEv2에 대해 TCP 캡슐화 및 보안 레이블을 지원합니다.

scap-security-guide 패키지는 버전 0.1.54로 업데이트되었으며 **OpenSCAP** 은 버전 1.3.4로 업데이트되었습니다. 이러한 업데이트는 다음과 같이 대폭 개선되었습니다.

- 향상된 메모리 관리
- RHEL8 ANSSI-BP-028 최소, 중간 및 강화 프로파일 추가
- RHEL8 STIG 프로파일을 DISA STIG v1r1로 업데이트

fapolicyd 프레임워크는 이제 **무결성 검사를** 제공하며 RPM 플러그인은 이제 YUM 패키지 관리자 또는 RPM 패키지 관리자에서 처리하는 모든 시스템 업데이트를 등록합니다.

rhel8-tang 컨테이너 이미지는 OpenShift Container Platform(OCP) 클러스터 또는 별도의 가상 시스템에서 실행되는 Clevis 클라이언트에 Tang-server 암호 해독 기능을 제공합니다.

자세한 내용은 4.6절. "보안"를 참조하십시오.

네트워킹
NMState는 호스트용 네트워크 API이며 RHEL 8.4에서 완전하게 지원됩니다. **nmstate** 패키지는 선언적 방식으로 호스트 네트워크 설정을 관리하는 라이브러리와 **nmstatectl** 명령줄 유틸리티를 제공합니다.

MPLS(Multi-protocol Label Switching)는 엔터프라이즈 네트워크 전반에서 트래픽 흐름을 라우팅하는 커널 내 데이터 전달 메커니즘입니다. 예를 들어 특정 포트에서 수신된 패킷을 관리하거나 일관된 방식으로 특정 유형의 트래픽을 전달하기 위해 add **tc 필터를** 추가할 수 있습니다. MPLS 지원은 이번 릴리스에서 기술 프리뷰로 제공됩니다.

iproute2 유틸리티는 3개의 새로운 트래픽 제어(**tc**) 작업을 도입합니다. **mac_push**,**push_eth**, **pop_eth** 는 MPLS 레이블을 추가하고, 패킷 시작 부분에 이더넷 헤더를 빌드하고, 외부 이더넷 헤더를 각각 삭제합니다.

bareudp 장치에 대한 지원은 이제 **ip link** 명령을 기술 프리뷰로 사용하여 사용할 수 있습니다.

이 릴리스에 도입된 기능과 기존 기능의 변경 사항에 대한 자세한 내용은 4.7절. "네트워킹" 을 참조하십시오.

커널
kpatch-dnf 패키지는 RHEL 시스템을 커널 라이브 패치 업데이트에 등록하기 위한 **DNF** 플러그인을 제공합니다. 플러그 인은 시스템이 현재 사용하는 모든 커널에 대해 자동 서브스크립션을 활성화하고 나중에 커널에 설치할 수 있습니다.

사전 압축 은 할당 요청을 수행하기 **전에** 메모리 압축 작업을 정기적으로 시작합니다. 따라서 특정 메모리 할당 요청에 대한 대기 시간이 낮아집니다.

RHEL 8에서는 **제어 그룹** 기술을 위한 새로운 slab 메모리 컨트롤러 구현을 사용할 수 있습니다. 슬랩 메모리 컨트롤러는 슬랩 사용률을 개선하고 메모리 계정을 페이지 수준에서 개체 수준으로 이동할 수 있습니다. 결과적으로 총 커널 메모리 풋프린트의 감소와 메모리 조각화에 긍정적인 영향을 확인할 수 있습니다.

시간 네임스페이스 기능은 RHEL 8.4에서 사용할 수 있습니다. 이 기능은 Linux 컨테이너 내에서 날짜와 시간을 변경하는 데 적합합니다. checkpoint에서 복원한 후 컨테이너 내 클록 조정도 가능합니다.

RHEL 8은 8세대 및 9세대 Intel 코어 프로세서에 설정된 오류 감지 및 수정(EDAC) 커널 모듈 세트를 지원합니다.

이 릴리스에 도입된 기능과 기존 기능의 변경 사항에 대한 자세한 내용은 4.8절. "커널" 을 참조하십시오.

고가용성 및 클러스터
상태 데이터를 유지 관리하는 영구 Pacemaker 리소스 에이전트는 오류를 비동기적으로 감지하고 다음 모니터 간격을 기다리지 않고 즉시 오류를 Pacemaker에 삽입할 수 있습니다. 또한 영구 리소스 에이전트는 상태 데이터를 유지하면 각 작업에 대해 상태를 별도로 호출하지 않고 시작, 중지 및 모니터링과 같은 클러스터 작업의 상태 오버헤드를 줄일 수 있으므로 상태 오버헤드가 높은 서비스의 클러스터 응답 시간을 단축할 수 있습니다.

영구 Pacemaker 리소스 에이전트 생성에 대한 자세한 내용은 이제 영구(Daemonized) Pacemaker 리소스 에이전트 생성 문서를 참조하십시오.

동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버
다음 구성 요소의 최신 버전을 새 모듈 스트림으로 사용할 수 있습니다.

- **Python 3.9**
- **SWIG 4.0**
- **Subversion 1.14**
- **redis 6**
- **PostgreSQL 13**
- **MariaDB 10.5**

자세한 내용은 4.11절. "동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버" 를 참조하십시오.

컴파일러 및 개발 도구
다음 컴파일러 툴 세트가 업데이트되었습니다.

- **GCC 툴 세트 10**
- **LLVM Toolset 11.0.0**
- **노르웨이 도구 세트 1.49.0**
- **Go Toolset 1.15.7**

자세한 내용은 4.12절. "컴파일러 및 개발 도구" 를 참조하십시오.

OpenJDK 11 사용 가능
새로운 버전의 OpenJDK(Open Java Development Kit)를 사용할 수 있습니다. 이 릴리스에 도입된 기능과 기존 기능의 변경 사항에 대한 자세한 내용은 OpenJDK 기능을 참조하십시오.

IdM (Identity Management)
RHEL 8.4에서는 IdM(Identity Management)의 역할 기반 액세스 제어(RBAC) 자동화 관리를 위한 Ansible 모듈, IdM 서버를 백업하고 복원하는 Ansible 역할 및 위치 관리를 위한 Ansible 모듈을 제공합니다.

자세한 내용은 4.13절. "IdM (Identity Management)" 를 참조하십시오.

1.2. 즉각적 업그레이드 및 OS 변환

RHEL 7에서 **RHEL 8**으로의 즉각적 업그레이드
현재 지원되는 즉각적 업그레이드 경로는 다음과 같습니다.

- 64비트 Intel, IBM POWER 8(little endian) 및 IBM Z 아키텍처의 RHEL 7.9에서 RHEL 8.4까지
- 커널 버전 4.14가 필요한 아키텍처의 RHEL 7.6에서 RHEL 8.4로: 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 SAP HANA 시스템이 계속 지원되도록 하려면 RHEL 8.2 Update Services for SAP Solutions(E4S) 리포지토리를 활성화하십시오.

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

RHEL 8.4가 릴리스되면서 이제 RHSM (Red Hat Subscription Manager)을 사용하고 업그레이드하지 않고 이전 필수 데이터 파일을 다운로드하지 않은 경우 cloud.redhat.com에서 필요한 추가 데이터 파일이 자동으로 다운로드됩니다.

RHEL 6에서 **RHEL 8**로 즉각적 업그레이드
RHEL 6.10에서 RHEL 8.4로 업그레이드하려면 RHEL 6에서 RHEL 8로 업그레이드하는 방법에 대한 지침을 따르십시오.

다른 **Linux** 배포판에서 **RHEL**로 변환
CentOS Linux 8 또는 Oracle Linux 8을 사용하는 경우 Red Hat에서 지원하는 **Convert2 RHEL 유틸리티**를 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 문서를 참조하십시오.

1.3. RED HAT CUSTOMER PORTAL 랩

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

- 등록 도우미
- 제품 라이프 사이클 검사기
- 킥스타트 생성기
- 킥스타트 킥스타트
- 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
- Red Hat Memory Analyzer
- 커널 Oops 분석기
- Red Hat 제품 에라타 권고 검사기

1.4. 추가 리소스

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

2장. 아키텍처

Red Hat Enterprise Linux 8.4는 다음 아키텍처를 지원하는 커널 버전 4.18.0-305와 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 방법은 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 매니페스트를 참조하십시오.

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

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

RHEL 8 리포지토리에 관한 자세한 내용은 패키지 매니페스트를 참조하십시오.

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 사용 가능한 모듈 목록은 패키지 매니페스트를 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 **yum이 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. 새로운 기능

이 부분에서는 Red Hat Enterprise Linux 8.4에 도입된 새로운 기능 및 주요 개선 사항에 대해 설명합니다.

4.1. 설치 프로그램 및 이미지 생성

Anaconda에서 원래 부팅 장치 NVRAM 변수 목록을 새 값으로 교체

이전에는 NVRAM에서 부팅하면 부팅 장치 목록에 잘못된 **값이** 있는 항목으로 인해 시스템이 부팅되지 않을 수 있었습니다.

이번 업데이트를 통해 문제가 해결되었지만 부팅 장치 NVRAM 변수를 업데이트할 때 이전 장치 목록은 지워집니다.

(BZ#1854307)

IBM Z에서 KVM 가상 머신의 그래픽 설치를 사용할 수 있습니다

IBM Z 하드웨어에서 KVM 하이퍼바이저를 사용할 때 이제 가상 시스템(VM)을 생성할 때 그래픽 설치를 사용할 수 있습니다.

이제 사용자가 KVM에서 설치를 실행하고 QEMU에서 **virtio-gpu 드라이버를 제공하면** 설치 프로그램에서 그래픽 콘솔을 자동으로 시작합니다. 사용자는 VM의 커널 명령줄에 **inst.text 또는 inst. vnc** 부팅 매개변수를 추가하여 텍스트 또는 VNC 모드로 전환할 수 있습니다.

(BZ#1609325)

더 이상 사용되지 않는 커널 부팅 인수 경고

inst. 접두사(예: **ks**,**stage2**,**repo** 등)가 없는 Anaconda 부팅 인수는 RHEL7부터 더 이상 사용되지 않습니다. 이러한 인수는 다음 주요 RHEL 릴리스에서 제거됩니다.

이번 릴리스에서는 **inst** 접두사 없이 부팅 인수를 사용할 때 적절한 경고 메시지가 표시됩니다. 설치를 부팅할 때와 터미널에서 설치 프로그램이 시작될 때도 경고 메시지가 **dracut** 에 표시됩니다.

다음은 터미널에 표시되는 샘플 경고 메시지입니다.

더 이상 사용되지 않는 부팅 인수 **%s** 를 **inst.** 접두사와 함께 사용해야 합니다. 대신 **inst.%s**를 사용하십시오. **inst.** 접두사가 없는 Anaconda 부팅 인수는 더 이상 사용되지 않으며 향후 주요 릴리스에서 제거됩니다.

다음은 **dracut** 에 표시되는 샘플 경고 메시지입니다.

$1 이 더 이상 사용되지 않음. **inst.** 접두사가 없는 Anaconda 부팅 인수의 모든 사용은 더 이상 사용되지 않으며 향후 주요 릴리스에서 제거됩니다. 대신 **$2** 를 사용하십시오.

(BZ#1897657)

4.2. 에지용 RHEL

에지 이미지 유형의 RHEL에 대한 사용자 지정으로 커널 이름을 지정하는 지원

에지 이미지에 대한 RHEL 에 대한 OSTree 커밋을 생성할 때 한 번에 하나의 커널 패키지만 설치할 수 있습니다. 그렇지 않으면 커밋 생성이 **rpm-ostree** 에서 실패합니다. 이를 통해 에지용 RHEL은 특히 실시간 커널(커널**-rt**)을 대체 커널을 추가하지 못합니다. 이번 개선된 기능을 통해 CLI를 사용하여 에지 이미지의 RHEL용 청사진을 생성할 때 customizations **.kernel.name** 키를 설정하여 이미지에 사용할 커널 이름을 정의할 수 있습니다. 커널 이름을 지정하지 않으면 이미지에 기본 커널 패키지가 포함됩니다.

(BZ#1960043)

4.3. 소프트웨어 관리

DNF API에서 새로운 fill_sack_from_repos_in_cache 함수 지원

이번 업데이트를 통해 캐시된 **solv,solv x** 파일 및 **repomd.xml** 파일에서만 리포지토리를 로드할 수 있는 새로운 DNF API **fill_sack_from_repos_in_cache** 함수가 도입되었습니다. 결과적으로 사용자가 **dnf** 캐시를 관리하는 경우 중복 정보(xml 및 **solv) 없이도 리소스를 절약할 수 있으며xml 을 solv 로** 처리하지 않고도 리소스를 절약할 수 있습니다 **.**

(BZ#1865803)

createrepo_c 는 이제 모듈식 메타데이터를 리포지토리에 자동으로 추가합니다.

이전에는 RHEL8 패키지에서 **createrepo_c** 명령을 실행하여 새 리포지토리를 생성해도 이 리포지토리에 모듈식 repodata가 포함되지 않았습니다. 이로 인해 리포지토리에 다양한 문제가 발생했습니다. 이번 업데이트를 통해 **createrepo_c**:

- 모듈식 메타데이터 스캔
- 검색된 모듈 YAML 파일을 단일 **모듈 문서 module.yaml**로 병합
- 이 문서를 리포지토리에 자동으로 추가합니다.

결과적으로 이제 리포지토리에 모듈식 메타데이터를 자동으로 추가할 수 있으며 **modifyrepo_c** 명령을 사용하여 별도의 단계로 더 이상 수행할 필요가 없습니다.

(BZ#1795936)

DNF 내의 시스템 간 트랜잭션 미러링 기능 지원

이번 업데이트를 통해 사용자는 DNF 내에서 트랜잭션을 저장하고 재생할 수 있습니다.

- DNF 기록의 트랜잭션을 JSON 파일에 저장하려면 **dnf 기록 저장소** 명령을 실행합니다.
- 나중에 동일한 시스템 또는 다른 시스템에서 트랜잭션을 재생하려면 **dnf history replay** 명령을 실행합니다.

comps 그룹 작업 저장 및 재생이 지원됩니다. 모듈 작업은 아직 지원되지 않으므로, 결과적으로 저장되거나 재생되지 않습니다.

(BZ#1807446)

createrepo_c 를 버전 0.16.2로 다시 기반

createrepo_c 패키지는 이전 버전에 대해 다음과 같은 주요 변경 사항을 제공하는 버전 0.16.2로 업데이트되었습니다.

- **createrepo_c에 대한 모듈 메타데이터 지원이 추가되었습니다**.
- 다양한 메모리 누수 수정

(BZ#1894361)

protect_running_kernel 구성 옵션을 사용할 수 있습니다.

이번 업데이트를 통해 **dnf** 및 **microdnf** 명령에 대한 **protect_running_kernel** 구성 옵션이 도입되었습니다. 이 옵션은 실행 중인 커널 버전에 해당하는 패키지가 제거되지 않도록 보호되는지 여부를 제어합니다. 결과적으로 사용자는 이제 실행 중인 커널의 보호를 비활성화할 수 있습니다.

(BZ#1698145)

4.4. 쉘 및 명령행 툴

OpenIPMI 버전 2.0.29로 업데이트

OpenIPMI 패키지가 버전 2.0.29로 업그레이드되었습니다. 이전 버전에 대한 주요 변경 사항은 다음과 같습니다.

- 메모리 누수, 변수 바인딩, 누락된 오류 메시지 수정.
- **IPMB에 대한 지원이 추가되었습니다**.
- **lanserv에 개별 그룹 확장 등록에 대한 지원이 추가되었습니다**.

(BZ#1796588)

Free ipmi 가 1.6.6 버전으로 업데이트

freeipmi 패키지가 버전 1.6.6으로 업그레이드되었습니다. 이전 버전에 대한 주요 변경 사항은 다음과 같습니다.

- 소스 코드에서 메모리 누수 및 오타 수정.
- 다음과 같은 알려진 문제에 대한 해결 방법을 구현했습니다.
  - 예기치 않은 완료 코드.
  - Dell Poweredge FC830.
  - **lan/rmcpplus ipmb** 가 있는 패킷의 순서가 부족합니다.
- 새로운 Dell, Intel 및 기가바이트 장치에 대한 지원이 추가되었습니다.
- 시스템 정보 및 이벤트 해석에 대한 지원이 추가되었습니다.

(BZ#1861627)

Opal-prd 가 6.6.3 버전으로 업데이트

opal-prd 패키지는 6.6.3 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- opal **-prd** 데몬에 대한 오프라인 작업자 프로세스 핸들 페이지가 추가되었습니다.
- 시스템이 포가드 레코드 **의 칩 대상을 식별할 수 있도록 POWER9P 에서 opal-gard 의 버그를 수정했습니다.**
- **occ 명령의 wait_for_all_occ_init() 에서 잘못된 부정을 수정했습니다.**

- hw/phys-map 의 고정된 OCAPI_MEM 값.
- hdata/memory.c 의 Inconsistent MSAREA 에 대한 수정 경고.
- occ의 센서의 경우:
  - 수정된 센서 값 0 버그.
  - GPU 감지 코드를 수정했습니다.
- MPIPL 부팅에서 검색 건너 뛰기.
- Mihawk 플랫폼에서 두 번 고정 IPMI.
- fsp/dump 에서 비MPIPL 시나리오 업데이트.
- hw/phb4의 경우:
  - AER regs를 초기화하기 전에 AER 지원 확인.
  - 오류 보고 활성화.
- hdata 에 새로운 smp-cable-connector VPD 키워드 추가.

(BZ#1844427)

opencryptoki 가 버전 3.15.1로 업데이트

opencryptoki 패키지는 버전 3.15.1로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- C_SetPin 의 고정된 segfault.
- EVP_CipherUpdate 및 EVP_Cipher Final 의 고정 사용.
- 토큰 리포지토리를 FIPS 호환 암호화로 마이그레이션하는 유틸리티가 추가되었습니다.
- pkcstok_migrate 툴의 경우:
  - Little Endian 플랫폼에서 고정 NVTOK.DAT 변환.
  - Little Endian 플랫폼에서 프라이빗 및 공용 토큰 개체 변환 수정.
- 새로운 데이터 형식으로 공개 토큰 오브젝트의 고정 저장.
- dh_pkcs_derive 에서 매개 변수 검사 메커니즘을 수정했습니다.
- 수정된 소프트 토큰 모델 이름.
- mech_ec.c 파일과 ICA,TPM, 소프트 토큰에서 더 이상 사용되지 않는 OpenSSL 인터페이스를 교체합니다.
- sw_crypt.c 파일에서 더 이상 사용되지 않는 OpenSSL AES/3DES 인터페이스를 교체했습니다.
- 소프트 토큰에 ECC 메커니즘에 대한 지원이 추가되었습니다.
- 소프트 토큰에 IBM 특정 SHA3 HMAC 및 SHA512/224/256 HMAC 메커니즘 추가.
- CCA에서 CKM_RSA_PKCS 로 키 래핑에 대한 지원이 추가되었습니다.

- EP11 암호화 스택의 경우:
  - CKM _DES2_KEY_GEN을 인식하도록 수정된 ep11_get_ keytype.
  - token_specific_rng 에서 수정된 오류 추적
  - HSM 시뮬레이션에서 특정 FW 버전 및 API 활성화.
- X9.63 KDF 의 Endian 버그 수정.
- p11sak remove-key 명령을 처리하기 위한 오류 메시지가 추가되었습니다.
- C++에 대한 컴파일 문제 해결.
- C_Get/SetOperationState 및 다이제스트 컨텍스트의 문제를 해결했습니다.
- usr/sb2 를 사용하면 고정 pkcs 마이그레이션이 실패합니다.

(BZ#1847433)

PowerPC-utils 를 버전 1.3.8로 업데이트

powerpc-utils 패키지는 버전 1.3.8로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- Perl 에 종속되지 않는 명령은 이제 core 하위 패키지로 이동됩니다.
- Linux Hybrid Network Virtualization 지원 추가.
- 업데이트된 안전한 부팅 목록.

- Added vcpustat 유틸리티.
- lparstat 명령에 cpu-hotplug 지원이 추가되었습니다.
- lparstat 명령에서 확장된 메트릭을 인쇄하는 추가 스위치.
- delta, scaled timebase 및 derive PURR/SPURR 값에 계산하는 도우미 함수가 추가되었습니다.
- ofpathname 유틸리티의 경우:
  - l2of_scsi() 의 속도를 개선했습니다.
  - udevadm 위치를 수정했습니다.
  - l2od_ide() 및 l2of_scsi() 를 지원하는 파티션이 추가되었습니다.
  - SCSI/SATA 호스트의 플러그 ID에 대한 지원이 추가되었습니다.
- 지원되지 않는 커넥터 유형에서 segfault 조건을 수정했습니다.
- SR_IOV 를 하이브리드 가상 네트워크로 마이그레이션할 수 있는 추가 툴.
- format-overflow 경고를 수정합니다.
- lsdevinfo 유틸리티를 사용하여 bash 명령 대체 경고를 수정합니다.
- 고정 부팅 시간 본딩 인터페이스 정리.

(BZ#1853297)

새로운 커널 cmdline 옵션이 네트워크 장치 이름을 생성합니다

systemd-udevd 서비스의 net_id 내장된 기능은 새로운 커널 cmdline 옵션 net.naming-scheme=SCHEME_VERSION 을 얻습니다. SCHEME_VERSION 값을 기반으로 사용자는 네트워크 장치 이름을 생성할 알고리즘 버전을 선택할 수 있습니다.

예를 들어 RHEL 8.4에 내장된 net_id 의 기능을 사용하려면 SCHEME_VERSION 의 값을 rhel-8.4 로 설정합니다.

마찬가지로 SCHEME_VERSION 의 값을 필요한 변경 또는 수정이 포함된 다른 마이너 릴리스로 설정할 수 있습니다.

(BZ#1827462)

4.5. 인프라 서비스

기본 postfix-3.5.8 동작의 차이점

RHEL-8 이전 버전과의 호환성을 높이기 위해 postfix-3.5.8 업데이트의 동작은 기본 업스트림 postfix-3.5.8 동작과 다릅니다. 기본 업스트림 postfix-3.5.8 동작의 경우 다음 명령을 실행합니다.

```
# postconf info_log_address_format=external

# postconf smtpd_discard_ehlo_keywords=

# postconf rhel_ipv6_normalize=yes
```

자세한 내용은 /usr/share/doc/postfix/README-RedHat.txt 파일을 참조하십시오. 호환되지 않는 기능이 사용되지 않거나 RHEL-8 이전 버전과의 호환성이 우선 순위인 경우 단계가 필요하지 않습니다.

(BZ#1688389)

BIND 버전 9.11.26으로 업데이트

bind 패키지가 버전 **9.11.26**으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 기본 **EDNS** 버퍼 크기를 **4096**에서 **1232**바이트로 변경했습니다. 이러한 변경으로 인해 일부 네트워크에서 조각화된 패킷이 손실되지 않습니다.
- **max-recursion-queries**의 기본값이 **75**에서 **100**으로 증가했습니다. **CVE-2020-8616** 관련.
- 에서 **lib/dns/rbtdb.c** 파일에서 삭제된 노드의 문제를 해결했습니다.
- **lib/dns/rbtdb.c** 파일에서 재사용이 중단된 노드를 정리할 때 **named** 서비스에서 충돌 문제를 해결했습니다.
- 구성된 여러 전달자가 명명된 서비스에서 발생하는 경우가 있는 문제를 해결했습니다.
- 상위에 있는 **DS** 레코드가 없는 잘못된 서명된 영역을 **chgus**로 할당하는 명명된 서비스의 문제를 해결했습니다.
- **UDP** 를 통해 누락된 **DNS** 쿠키 응답을 수정했습니다.

(BZ#1882040)

unbound 구성에서 향상된 로깅 출력 제공

이 향상된 기능을 통해 바인딩되지 않은 구성에 다음 세 가지 옵션이 추가되었습니다.

- **log-servfail** 는 **SERVFAIL** 오류 코드의 이유를 클라이언트에 대한 이유를 설명하는 로그 행을 활성화합니다.
- **log-local-actions** 를 사용하면 모든 로컬 영역 작업을 로깅할 수 있습니다.

- **log-tag-queryreply** 는 로그 쿼리 태그 및 로그 파일에 대한 응답 태그를 활성화합니다.

(BZ#1850460)

ghostscript-9.27로 수정된 여러 취약점

- **ghostscript-9.27** 릴리스에는 다음 취약점에 대한 보안 수정 사항이 포함되어 있습니다.
  - CVE-2020-14373
  - CVE-2020-16287
  - CVE-2020-16288
  - CVE-2020-16289
  - CVE-2020-16290
  - CVE-2020-16291
  - CVE-2020-16292
  - CVE-2020-16293
  - CVE-2020-16294
  - CVE-2020-16295
  - CVE-2020-16296

- CVE-2020-16297
- CVE-2020-16298
- CVE-2020-16299
- CVE-2020-16300
- CVE-2020-16301
- CVE-2020-16302
- CVE-2020-16303
- CVE-2020-16304
- CVE-2020-16305
- CVE-2020-16306
- CVE-2020-16307
- CVE-2020-16308
- CVE-2020-16309
- CVE-2020-16310

- CVE-2020-17538

(BZ#1874523)

버전 2.15-1로 다시 기반으로 조정되었습니다.

주요 변경 사항은 다음과 같습니다.

- Linux 서비스 제어를 위한 추가 서비스 플러그인.
- 향상된 스케줄러 플러그인.

(BZ#1874052)

이제 DNSTAP 에서 들어오는 자세한 쿼리를 기록합니다.

DNSTAP 는 들어오는 이름 쿼리의 세부 정보를 모니터링하고 기록하는 고급 방법을 제공합니다. 또한 명명된 서비스에서 응답을 전송한 레코드입니다. 명명된 서비스의 전통적인 쿼리 로깅은 명명된 서비스의 성능에 부정적인 영향을 미칩니다.

결과적으로 DNSTAP는 성능 저하에 영향을 주지 않고 자세히 들어오는 쿼리의 지속적인 로깅을 수행하는 방법을 제공합니다. 새 dnstap-read 유틸리티를 사용하면 다른 시스템에서 실행되는 쿼리를 분석할 수 있습니다.

(BZ#1854148)

SpamAssassin 이 3.4.4 버전으로 다시 기반

SpamAssassin 패키지가 버전 3.4.4로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- OLEVBMacro 플러그인이 추가되었습니다.
- check_rbl_ns,check_rbl_rcvd,check_hashbl_bodyre 및 check_hashbl_uris 가 추가되었습니다.

(BZ#1822388)

키 알고리즘은API 쉘을 사용하여 변경할 수 있습니다.

이번 개선된 기능을 통해 사용자는 이제 키 알고리즘을 변경할 수 있습니다. HMAC-MD5 로 하드 코딩된 키 알고리즘은 더 이상 안전한 것으로 간주되지 않습니다. 결과적으로 omshell 명령을 사용하여 키 알고리즘을 변경할 수 있습니다.

(BZ#1883999)

sendmail에서 TLSFallbacktoClear 구성 지원

이 향상된 기능을 통해 나가는 TLS 연결이 실패하면 sendmail 클라이언트가 일반 텍스트로 대체됩니다. 이렇게 하면 다른 당사자와의 TLS 호환성 문제가 해결됩니다. Red Hat에서는 기본적으로 TLSFallbacktoClear 옵션이 비활성화된 sendmail을 제공합니다.

(BZ#1868041)

tcpdump에서 RDMA 가능 장치를 볼 수 있음

이 향상된 기능을 통해 tcpdump 로 RDMA 트래픽을 캡처할 수 있습니다. 사용자는 tcpdump 도구를 사용하여 오프로드된 RDMA 트래픽을 캡처하고 분석할 수 있습니다. 결과적으로 tcpdump 를 사용하여 RDMA 지원 장치를 보고, RoCE 및 VMA 트래픽을 캡처하고, 콘텐츠를 분석할 수 있습니다.

(BZ#1743650)

4.6. 보안

Libreswan이 4.3으로 다시 기반

libreswan 패키지가 버전 4.3으로 업그레이드되었습니다. 이전 버전에 대한 주요 변경 사항은 다음과 같습니다.

- IKE 및 ESP over TCP 지원(RFC 8229)
- IKEv2 레이블이 지정된 IPsec 지원

- IKEv2 leftikeport/rightikeport 지원
- 중간 교환에 대한 실험적 지원
- 로드 밸런싱에 대한 확장 리디렉션 지원
- 상호 운용성 향상을 위해 기본 IKE 수명이 1시간에서 8시간으로 변경되었습니다.
- :ip sec.secrets 파일의RSA 섹션은 더 이상 필요하지 않습니다.
- 고정 Windows 10 rekeying
- ECDSA 인증을 위한 인증서 전송 수정
- MOBIKE 및 NAT-T에 대한 수정 사항

(BZ#1891128)

IPsec VPN이 TCP 전송 지원

이번 libreswan 패키지 업데이트에서는 RFC 8229에 설명된 대로 TCP 캡슐화를 통한 IPsec 기반 VPN 지원이 추가되었습니다. 또한 ESP(Security Payload) 및 UDP를 사용하여 트래픽을 방지하는 네트워크에 IPsec VPN을 설정하는 데 도움이 됩니다. 결과적으로 관리자는 TCP를 대체 또는 기본 VPN 전송 프로토콜로 사용하도록 VPN 서버와 클라이언트를 구성할 수 있습니다.

(BZ#1372050)

Libreswan에서 라벨이 지정된 IPsec에 대해 IKEv2 지원

Libreswan Internet Key Exchange (IKE) 구현에는 이제 IPsec용 보안 레이블에 대한 IKEv2(Internet Key Exchange 버전 2) 지원이 포함됩니다. 이번 업데이트를 통해 IKEv1과 함께 보안 레이블을 사용하는 시스템을 IKEv2로 업그레이드할 수 있습니다.

(BZ#1025061)

libpwquality 1.4.4로 업데이트

libpwquality 패키지는 1.4.4 버전으로 업데이트되었습니다. 이 릴리스에는 여러 버그 수정 및 번역 업데이트가 포함되어 있습니다. 특히 다음 설정 옵션이 the pwquality.conf 파일에 추가되었습니다.

- 재시도
- enforce_for_root
- local_users_only

(BZ#1537240)

p11 키트 가 0.23.19로 업데이트

p11-kit 패키지가 버전 0.23.14에서 0.23.19 버전으로 업그레이드되었습니다. 새 버전은 여러 버그를 수정하고 다양한 개선 사항을 제공합니다.

- CVE-2020-29361, CVE-2020-29362, CVE-2020-29363 보안 문제 해결.
- p11-kit 은 이제 meson 빌드 시스템을 통해 빌드를 지원합니다.

(BZ#1887853)

pyOpenSSL 을 19.0.0으로 업데이트

pyOpenSSL 패키지가 업스트림 버전 19.0.0으로 업데이트되었습니다. 이 버전은 버그 수정 및 개선 사항을 제공하며 특히 다음과 같습니다.

- openssl 버전 1.1.1으로 개선된 TLS 1.3 지원.

- X509Store.add_cert로 중복 인증서를 추가하려고 할 때 더 이상 오류가 증가하지 않습니다

- 구성 요소에서 NUL 바이트를 포함하는 X509 인증서 처리 개선

(BZ#1629914)

SCAP 보안 가이드가 0.1.54로 업데이트

scap-security-guide 패키지는 여러 버그 수정 및 개선 사항을 제공하는 업스트림 버전 0.1.54로 업데이트되었습니다. 가장 중요한 것은 다음과 같습니다.

- OSPP(Operations System Protection Profile)가 Red Hat Enterprise Linux 8.4용 범용 운영 체제 보호 프로필에 따라 업데이트되었습니다.

- 프랑스AN SSI (National Security Agency)의 ANSSI BP-028 권장 사항을 기반으로 하는 ANSSI 프로필이 도입되었습니다. 콘텐츠에는 Minimum, Intermediary 및 Enhanced hardening 수준의 규칙을 구현하는 프로필이 포함되어 있습니다.

- STIG(보안 기술 구현 가이드) 보안 프로필이 업데이트되었으며 최근 릴리스된 버전 V1R1의 규칙을 구현합니다.

(BZ#1889344)

OpenSCAP을 1.3.4로 업데이트

OpenSCAP 패키지가 업스트림 버전 1.3.4로 업데이트되었습니다. 주요 수정 사항 및 개선 사항은 다음과 같습니다.

- 대량의 파일이 있는 시스템이 메모리 부족을 야기하는 특정 메모리 문제를 해결했습니다.

- 이제 OpenSCAP에서 GPFS를 원격 파일 시스템으로 처리합니다.

- 정의 간에 순환 종속성을 사용하여 OVAL을 올바르게 처리합니다.

- 향상된 **yamlfilecontent:** 업데이트된 **yaml-filter,** 맵의 값 세트로 작업할 수 있도록 스키마 및 프로브를 확장했습니다.
- 수많은 경고(**GCC** 및 **Clang**)를 수정했습니다.
- 수많은 메모리 관리 픽스.
- 수많은 메모리 누수 픽스.
- 이제 **XCCDF** 파일의 플랫폼 요소가 **XCCDF** 사양에 따라 올바르게 해결됩니다.
- 개선된 호환성 **uClibc.**
- 로컬 및 원격 파일 시스템 감지 방법 개선.
- 캐시를 수동으로 여는 대신 **pkgCacheFile** 을 사용하도록 수정된 **dpkginfo** 프로브.
- 이제 **OpenSCAP** 스캔 보고서가 유효한 **HTML5** 문서입니다.
- 파일 프로브에서 원하지 않는 반복이 고정되었습니다.

(**BZ#1887794**)

RHEL 8 STIG 보안 프로필이 버전 **V1R1**로 업데이트

RHBA-2021:1886 권고가 릴리스되면서 **SCAP** 보안 가이드의 **DISA STIG for Red Hat Enterprise Linux 8** 프로필이 최신 버전 **V1R1** 에 맞게 업데이트되었습니다. **RHEL 8 STIG(Security Technical Implementation Guide)** 매뉴얼 벤치마크가 보다 안정적이고 효과적으로 조정됩니다. 첫 번째 반복은 **STIG**와 관련하여 약 **60%**의 적용 범위를 제공합니다.

초안 프로필이 더 이상 유효하지 않으므로 이 프로필의 현재 버전만 사용해야 합니다.

주의

자동 수정을 통해 시스템이 작동하지 않을 수 있습니다. 먼저 테스트 환경에서 수정을 실행합니다.

(BZ#1918742)

서버와 GUI 설치와 호환되는 새로운 DISA STIG 프로파일

GUI를 사용한 DISA STIG 라는 새 프로필이 RHBA-2021:4098 권고 릴리스와 함께 SCAP 보안 가이드에 추가되었습니다. 이 프로필은 DISA STIG 프로필에서 파생되며 GUI 패키지 그룹과 서버를 선택한 RHEL 설치와 호환됩니다. DISA STIG는 그래픽 사용자 인터페이스를 제거해야 했기 때문에 이전의 기존 stig 프로파일은 GUI와 호환되지 않았습니다. 그러나 평가 중에 보안 책임자가 올바르게 문서화한 경우 이 값을 재정의할 수 있습니다. 결과적으로 새 프로필은 DISA STIG 프로필에 정렬된 GUI를 사용하여 RHEL 시스템을 서버로 설치할 때 도움이 됩니다.

(BZ#2005431)

이제 ANSSI-BP-028 최소, 중간 및 강화 수준에 대한 프로파일을 SCAP 보안 가이드에서 사용할 수 있습니다.

새 프로필을 사용하면 Minimal, Intermediary 및 Enhanced hardening 레벨에서 GNU/Linux 시스템의 GNU/Linux 시스템용 AMD(National Security Agency)의 권장 사항까지 시스템을 강화할 수 있습니다. 결과적으로 ANSSI Ansible 플레이북 및 ANSSI SCAP 프로필을 사용하여 필요한 ANSSI 강화 수준에 따라 RHEL 8 시스템의 규정 준수를 구성하고 자동화할 수 있습니다.

(BZ#1778188)

scap-workbench 가 sudo 권한을 사용하여 원격 시스템을 스캔할 수 있음

scap-workbench GUI 툴은 이제 암호 없는 sudo 액세스를 사용하여 원격 시스템 스캔을 지원합니다. 이 기능을 사용하면 루트의 자격 증명을 제공하여 보안 위험이 줄어듭니다.

scap-workbench 를 암호 없는 sudo 액세스 및 해결 옵션과 함께 사용할 때는 주의하십시오. Red Hat은 OpenSCAP 스캐너만을 위한 안전한 사용자 계정을 지정할 것을 권장합니다.

(BZ#1877522)

rhel8-tang 컨테이너 이미지를 사용할 수 있습니다

이번 릴리스에서는 **registry.redhat.io** 카탈로그에서 **rhel8/rhel8-tang** 컨테이너 이미지를 사용할 수 있습니다. 컨테이너 이미지는 **OCP(OpenShift Container Platform)** 클러스터 또는 별도의 가상 시스템에서 실행되는 **Clevis** 클라이언트에 대해 **Tang-server** 암호 해독 기능을 제공합니다.

(BZ#1913310)

Clevis가 버전 15로 업데이트

clevis 패키지가 업스트림 버전 **15**로 업데이트되었습니다. 이 버전은 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- **Clevis**는 이제 일반 **initramfs**를 생성하고 더 이상 **rd.neednet=1** 매개 변수를 커널 명령줄에 자동으로 추가하지 않습니다.
- **Clevis**는 이제 **sss pin**을 사용하는 잘못된 구성을 올바르게 처리하고 **clevis**는 **sss** 하위 명령을 암호화 하여 오류 원인을 나타내는 출력을 반환합니다.

(BZ#1887836)

Clevis가 더 이상 자동으로 add rd.neednet=1을 추가하지 않음

Clevis는 기본적으로 호스트별 구성 옵션 없이 일반적인 **initrd** (초기 **ramdisk**)를 올바르게 생성합니다. 결과적으로 **Clevis**는 더 이상 커널 명령줄에 **rd.neednet=1** 매개 변수를 자동으로 추가하지 않습니다.

구성이 이전 기능을 사용하는 경우 **--hostonly-cmdline** 인수를 사용하여 **dracut** 명령을 입력하거나 **/etc/dracut .conf.d**에 **clevis.conf** 파일을 생성하고 **hostonly_cmdline=yes** 옵션을 파일에 추가할 수 있습니다. **Tang** 바인딩은 **initrd** 빌드 프로세스 중에 있어야 합니다.

(BZ#1853651)

새 패키지: rsyslog-udpspoof

rsyslog-udpspoof 하위 패키지가 **RHEL 8**에 다시 추가되었습니다. 이 모듈은 일반 **UDP** 전달자와 유

사하지만 **syslog** 패킷에서 소스 **IP**를 유지 관리하는 동안 다양한 네트워크 세그먼트 간에 **syslog** 를 릴레이할 수 있습니다.

(BZ#1869874)

fapolicyd 가 **1.0.2**로 업데이트

fapolicyd 패키지는 업스트림 버전 **1.0.2**로 업데이트되었습니다. 이 버전은 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- 다음을 통해 무결성 검사를 활성화하기 위한 무결성 구성 옵션이 추가되었습니다.
  - 파일 크기 비교
  - **SHA-256** 해시 비교
  - 무결성 측정 아키텍처(**IMA**) 하위 시스템
- **fapolicyd RPM** 플러그인은 이제 **YUM** 패키지 관리자 또는 **RPM** 패키지 관리자에서 처리하는 모든 시스템 업데이트를 등록합니다.
- 이제 규칙에 **GID**가 제목에 포함될 수 있습니다.
- 이제 디버그 및 **syslog** 메시지에 규칙 번호를 포함할 수 있습니다.

(BZ#1887451)

RPM 트랜잭션 중 변경 사항에 대한 새로운 **RPM** 플러그인 알림

이번 **rpm** 패키지 업데이트에서는 **fapolicyd** 프레임워크를 **RPM** 데이터베이스와 통합하는 새로운 **RPM** 플러그인이 도입되었습니다. 플러그인은 **RPM** 트랜잭션 중에 설치 및 변경된 파일에 대한 **fapolicyd** 를 알립니다. 결과적으로 **fapolicyd** 는 이제 무결성 검사를 지원합니다.

RPM 플러그인은 **YUM** 트랜잭션에 국한되지 않고 **RPM**에 의한 변경 사항을 다루므로 **YUM** 플러그인을

대체합니다.

(BZ#1923167)

4.7. 네트워킹

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 XDP 하드웨어 오프로딩을 사용하지 않습니다

RHEL 8.4에서는 XDP_TX 및 XDP_REDIRECT 반환 코드가 XDP 프로그램에서 지원됩니다.

지원되지 않는 XDP 기능에 대한 자세한 내용은 기술 프리뷰로 사용 가능한 XDP 기능을참조하십시오.

(BZ#1952421)

NetworkManager가 버전 1.30.0으로 업데이트

NetworkManager 패키지가 업스트림 버전 1.30.0으로 업그레이드되어 이전 버전에 비해 여러 개선 사항 및 버그 수정이 제공됩니다.

- NetworkManager에서 임대 제공을 거부해야 하는 DHCP 서버 ID를 정의하기 위해 ipv4.dhcp-reject-servers 연결 속성이 추가되었습니다.
- 사용자 지정 벤더 클래스 식별자 DHCP 옵션 값을 보내도록 ipv4.dhcp-vendor-class-identifier 연결 속성이 추가되었습니다.
-

active_slave 본딩 옵션이 더 이상 사용되지 않습니다. 대신 controller 연결에서 기본 옵션을 설정합니다.

- nm-initrd-generator 유틸리티는 이제 MAC 주소를 지원하여 인터페이스를 나타냅니다.
- nm-initrd-generator 유틸리티 생성기는 이제 InfiniBand 연결 생성을 지원합니다.
- NetworkManager-wait-online 서비스의 시간 초과가 60초로 증가했습니다.
- RFC4361 을 준수하도록 ipv4.dhcp-client-id=ipv6-duid 연결 속성이 추가되었습니다.
- 추가 ethtool 오프로드 기능이 추가되었습니다.
- WPA3 Enterprise Suite-B 192비트 모드에 대한 지원이 추가되었습니다.
- veth(가상 이더넷) 장치에 대한 지원이 추가되었습니다.

주요 변경 사항에 대한 자세한 내용은 업스트림 릴리스 노트를 참조하십시오.

- NetworkManager 1.30.0
- NetworkManager 1.28.0

(BZ#1878783)

iproute2 유틸리티는 이더넷 헤더 앞에 MPLS 헤더를 추가하는 트래픽 제어 조치를 도입합니다.

이 향상된 기능을 통해 iproute2 유틸리티는 세 가지 새로운 트래픽 제어(tc) 작업을 제공합니다.

- mac_push - act_mpls 모듈은 원래 이더넷 헤더 앞에 MPLS 레이블을 추가하기 위해 이 작업을 제공합니다.

- **push_eth - act_vlan** 모듈은 패킷 시작 시 이더넷 헤더를 빌드하기 위해 이 작업을 제공합니다.

- **pop_eth - act_vlan** 모듈은 외부 이더넷 헤더를 제거하기 위해 이 작업을 제공합니다.

The s etc 작업은 이더넷 헤더 앞에 멀티프로토콜 라벨 전환(**MPLS**) 라벨을 추가하여 계층 **2** 가상 사설 네트워크(**L2VPN**) 구현에 도움이 됩니다. 이러한 작업은 네트워크 인터페이스에 필터를 추가하는 동안 사용할 수 있습니다.

Red Hat은 **MPLS** 자체는 기술 프리뷰 기능이므로 지원되지 않는 기술 프리뷰로 이러한 작업을 제공합니다.

이러한 작업 및 해당 매개변수에 대한 자세한 내용은 **the tc-mpls(8) and tc-vlan(8)** 도움말 페이지를 참조하십시오.

(BZ#1861261)

nmstate API가 완전히 지원됨

이전에 기술 프리뷰이었던 **NMState**는 호스트용 네트워크 **API**이며 **RHEL 8.4**에서 완벽하게 지원됩니다. **nmstate** 패키지는 선언적 방식으로 호스트 네트워크 설정을 관리하는 라이브러리와 **nmstatectl** 명령줄 유틸리티를 제공합니다. 네트워킹 상태는 사전 정의된 스키마에서 설명합니다. 현재 상태를 보고하고 원하는 상태로 변경 사항이 모두 스키마를 준수합니다.

자세한 내용은 네트워킹 구성 및 관리 설명서의 **/usr/share/doc/nmstate/README.md** 파일과 **nmstatectl** 에 대한 섹션을 참조하십시오.

(BZ#1674456)

새 패키지: **rshim**

rhsim 패키지는 **Mellanox BlueField rshim** 사용자 공간 드라이버를 제공하므로, 외부 호스트 시스템에서 **BlueField SmartNIC** 대상의 **rshim** 리소스에 액세스할 수 있습니다. 최신 버전의 **rshim** 사용자 공간 드라이버는 부팅 이미지 푸시 및 가상 콘솔 액세스를 위해 장치 파일을 구현합니다. 또한 **BlueField** 대

상에 연결하는 가상 네트워크 인터페이스를 만들고 내부 **rshim** 레지스터에 액세스할 수 있는 방법을 제공합니다.

가상 콘솔 또는 가상 네트워크 인터페이스가 작동하려면 대상에서 **tmfifo** 드라이버를 실행해야 합니다.

(BZ#1744737)

iptraf-ng 를 **1.2.1**로 업데이트

iptraf-ng 패키지가 업스트림 버전 **1.2.1**로 업데이트되어 몇 가지 버그 수정 및 개선 사항을 제공합니다. 가장 중요한 것은 다음과 같습니다.

- 삭제된 인터페이스의 세부 통계를 표시할 때 **iptraf-ng** 애플리케이션에서 더 이상 **100% CPU** 사용량이 발생하지 않습니다.
- **printf()** 함수의 안전하지 않은 처리 인수가 수정되었습니다.
- **IPOIB(IP over InfiniBand)** 인터페이스에 대한 부분 지원이 추가되었습니다. 커널이 인터페이스에 소스 주소를 제공하지 않으므로 **LAN** 스테이션 모니터 모드에서 이 기능을 사용할 수 없습니다.
- **iptraf-ng** 가 다중 기가비트 속도로 패킷을 캡처할 수 있도록 패킷 캡처 추상화가 추가되었습니다.
- 이제 **Home,End,Page up** 및 **Page down** 키보드 키를 사용하여 스크롤할 수 있습니다.
- 이제 애플리케이션에서 삭제된 패킷 수를 표시합니다.

(BZ#1906097)

4.8. 커널

RHEL 8.4의 커널 버전

Red Hat Enterprise Linux 8.4는 커널 버전 4.18.0-305와 함께 배포됩니다.

외부 커널 매개 변수 및 장치 드라이버에 중요한 변경 사항 도 참조하십시오.

(BZ#1839151)

RHEL 8.4 용 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 8.4에서는 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 라이브러리는 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.
- libbpf 패키지는 bpf trace 및 bpf /xdp 개발과 같은 bpf 관련 애플리케이션에 중요합니다.
- 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 프로그램, XDP가 활성화된 네트워크 인터페이스에서 패킷을 캡처하기 위한 xdpdump 유틸리티가 포함됩니다.

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 프리뷰를 참조하십시오.

(BZ#1780124)

새 패키지: kmod-redhat-oracleasm

이번 업데이트에서는 ASMLib 유틸리티의 커널 모듈 부분을 제공하는 새로운 kmod-redhat-oracleasm 패키지가 추가되었습니다. Oracle ASM(Automated Storage Management)은 Oracle 데이터베이스를 위한 데이터 볼륨 관리자입니다. ASMLib은 Linux 시스템에서 Oracle ASM 장치를 관리하는 데 사용할 수 있는 선택적 유틸리티입니다.

(BZ#1827015)

xmon 프로그램은 공격에 대해 Secure Boot 및 kernel_lock 복원력을 지원하도록 변경됩니다.

Secure Boot 메커니즘이 비활성화된 경우 커널 명령줄에서 xmon 프로그램을 읽기-쓰기 모드(xmon=rw)로 설정할 수 있습니다. 그러나 xmon=rw 를 지정하고 Secure Boot 모드로 부팅하면 kernel_lockdown 기능이 xmon=rw 를 재정의하여 읽기 전용 모드로 변경합니다. Secure Boot 활성화에 따라 xmon 의 추가 동작은 다음과 같습니다.

Secure Boot 가 설정되어 있습니다.

- **xmon=ro** (기본값)
- 스택 추적이 출력됨
- 메모리 읽기 작동
- 메모리 쓰기가 차단되었습니다

Secure Boot 가 꺼져 있습니다.

- **xmon=rw**설정 가능
- 스택 추적이 항상 인쇄됨
- 메모리 읽기 항상 작동
- 메모리 쓰기는 **xmon=rw**경우에만 허용됩니다.

이러한 **xmon** 동작 변경은 **root** 권한을 가진 공격자에 대한 **Secure Boot** 및 **kernel_lock** 복원력을 지원하는 것을 목표로 합니다.

커널 명령줄 매개 변수를 구성하는 방법에 대한 자세한 내용은 고객 포털에서 커널 명령줄 매개 변수 구성을 참조하십시오.

(BZ#1952161)

Cornelis-Path Architecture (OPA) 호스트 소프트웨어

Red Hat Enterprise Linux 8.4에서 **OPA(OPA-Path Architecture)** 호스트 소프트웨어가 완벽하게 지원됩니다. **OPA**는 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.

✓-Path 아키텍처 설치에 대한 자세한 내용은 다음을 참조하십시오. Cornelis✓-Path Fabric Software Release Notes 파일.

(BZ#1960412)

기본적으로 SLAB 캐시 병합 비활성화

CONFIG_SLAB_MERGE_DEFAULT 커널 구성 옵션이 비활성화되어 SLAB 캐시가 기본적으로 병합되지 않습니다. 이러한 변경은 할당자의 캐시 사용량의 안정성과 추적성을 향상시키기 위한 것입니다. 이전의 slab-cache 병합 동작이 필요한 경우 사용자는 slub_merge 매개 변수를 커널 명령줄에 추가하여 다시 활성화할 수 있습니다. 커널 명령줄 매개 변수를 설정하는 방법에 대한 자세한 내용은 고객 포털에서 커널 명령줄 매개변수 구성을 참조하십시오.

(BZ#1871214)

ima-evm-utils 패키지가 버전 1.3.2로 업데이트되었습니다.

The ima-evm-utils 패키지가 버전 1.3.2로 업그레이드되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 신뢰할 수 있는 플랫폼 모듈 (TPM2) 다중 은행 기능 처리 지원 추가
- RHEL(Platform Configuration Registers) 8 및 9로 부팅 집계 값 확장
- CLI 매개변수를 통해 미리 로드된 OpenSSL 엔진
- Intel Task State Segment (TSS2) PCR 읽기 지원 추가
- 원래 IMA(Integrity measurement Architecture) 템플릿 지원 추가

libimaevm.so.0 및 libimaevm.so.2 라이브러리는 모두 ima-evm-utils 의 일부입니다. 최신 애플리케이션이 libimaevm.so. 2를 사용하면 libimaevm.so. 0 사용자는 영향을 받지 않습니다.

(BZ#1868683)

지원되는 CPU 아키텍처에서 IMA 및 EVM 기능 수준을 높이는 방법

ARM을 제외한 모든 CPU 아키텍처는 무결성 측정 아키텍처(IMA) 및 EVM(Extended Verification Module) 기술에 대한 유사한 수준의 기능을 지원합니다. 활성화된 기능은 CPU 아키텍처마다 다릅니다. 지원되는 각 CPU 아키텍처에서 가장 중요한 변경 사항은 다음과 같습니다.

- **IBM Z: IMA 승인 및 신뢰할 수 있는 인증 키 활성화.**
- **AMD64 및 Intel 64: 보안 부팅 상태의 특정 아키텍처 정책.**
- **IBM Power System(little-endian): 안전하고 신뢰할 수 있는 부팅 상태의 특정 아키텍처 정책.**
- **지원되는 모든 아키텍처의 기본 해시 알고리즘으로 SHA-256.**
- **모든 아키텍처의 경우 측정 템플릿이 IMA-SIG로 변경되었습니다. 템플릿에 있는 서명 비트가 포함됩니다. 해당 형식은 d-ng|n-ng|sig 입니다.**

이 업데이트의 목표는 지원되는 모든 CPU 아키텍처에서 사용자 공간 애플리케이션이 동일하게 작동할 수 있도록 IMA 및 EVM의 기능 차이를 줄이는 것입니다.

(BZ#1869758)

RHEL 8에 기본적으로 비활성화됨으로 사전 예방적 압축 포함

지속적인 워크로드 활동을 통해 시스템 메모리가 조각화됩니다. 조각화로 인해 용량 및 성능 문제가 발생할 수 있습니다. 프로그램 오류도 발생할 수 있습니다. 따라서 커널은 메모리 압축이라는 반응 메커니즘을 사용합니다. 메커니즘의 원래 설계는 보수적이며 압축 작업은 할당 요청 요청에 따라 시작됩니다. 그러나 시스템 메모리가 이미 조각화된 경우 반응적 동작은 할당 대기 시간을 늘리는 경향이 있습니다. 사전 압축 은 할당 요청을 수행하기 전에 정기적으로 메모리 압축 작업을 시작하여 설계를 향상시킵니다. 이 향상된 기능으로 인해 메모리 할당 요청이 온디맨드로 생성되는 메모리 압축 없이 물리적 메모리 블록을 찾을 가능성이 높아집니다. 결과적으로 특정 메모리 할당 요청에 대한 대기 시간이 줄어듭니다.

주의

사전 압축 으로 인해 압축 활동이 증가할 수 있습니다. 다른 프로세스에 속한 메모리 페이지가 이동되고 다시 매핑되기 때문에 시스템 전체에 심각한 영향을 미칠 수 있습니다. 따라서 사전 압축을 활성화하려면 애플리케이션의 대기 시간 급증을 방지하기 위해 최대한 주의해야 합니다.

(BZ#1848427)

RHEL 8에 EDAC 지원이 추가되었습니다

이번 업데이트를 통해 **RHEL 8**은 **8**차 및 **9**세대 **Intel Core Processor(CoffeeLake)**에서 설정된 오류 감지 및 수정**(EDAC)** 커널 모듈 세트를 지원합니다. **EDAC** 커널 모듈은 주로 오류 코드 수정**(ECC)** 메모리를 처리하고 **PCI** 버스 패리티 오류를 감지 및 보고합니다.

(BZ#1847567)

새 패키지: kpatch-dnf

kpatch-dnf 패키지는 **DNF** 플러그인을 제공하므로 **RHEL** 시스템을 커널 라이브 패치 업데이트에 서브스크립션할 수 있습니다. 서브스크립션은 향후 설치될 커널을 포함하여 시스템에 현재 설치된 모든 커널에 영향을 미칩니다. **kpatch-dnf** 에 대한 자세한 내용은 **dnf-kpatch(8)** 매뉴얼 페이지 또는 커널 문서 관리, 모니터링 및 업데이트를 참조하십시오.

(BZ#1798711)

slab 메모리를 위한 새로운 cgroup 컨트롤러 구현

RHEL 8에서는 제어 그룹 기술을 위한 새로운 **slab** 메모리 컨트롤러 구현을 사용할 수 있습니다. 현재는 단일 메모리 슬랩에 다른 메모리 제어 그룹이 소유한 개체를 포함할 수 있습니다. 슬랩 메모리 컨트롤러는 슬랩 사용률**(**최대 **45%)**을 개선하고 메모리 계정을 페이지 수준에서 개체 수준으로 전환할 수 있도록 합니다. 또한 이러한 변경으로 인해 각 메모리 제어 그룹에 대해 각 **CPU**당 중복 및 노드당 **slab** 캐시 세트가 제거되고 모든 메모리 제어 그룹에 대해 하나의 공통 **CPU** 및 노드당 **slab** 캐시 세트가 설정됩니다. 결과적으로 총 커널 메모리 풋프린트를 대폭 감소하고 메모리 조각화에 긍정적인 영향을 확인할 수 있습니다.

새롭고 더 정확한 메모리 계정에는 더 많은 **CPU** 시간이 필요합니다. 그러나 실제로 차이점은 무시할 수 없는 것처럼 보입니다.

(BZ#1877019)

RHEL 8에 시간 네임스페이스가 추가되었습니다

시간 네임스페이스를 사용하면 시스템 **monotonic** 및 부팅 시간 클록이 **AMD64, Intel 64** 및 **64**비트 **ARM** 아키텍처에서 네임스페이스별 오프셋에서 작동할 수 있습니다. 이 기능은 **Linux** 컨테이너 내에서 날짜와 시간을 변경하고 체크포인트에서 복원한 후 컨테이너 내 클록을 조정하는 데 적합합니다. 결과적으로 사용자는 이제 개별 컨테이너에 대해 독립적으로 시간을 설정할 수 있습니다.

(BZ#1548297)

새로운 기능: 사용 가능한 메모리 페이지 반환

이번 업데이트를 통해 **RHEL 8** 호스트 커널은 **VM**(가상 머신)에서 하이퍼바이저로 다시 사용하지 않는 메모리 페이지를 반환할 수 있습니다. 이렇게 하면 호스트의 안정성과 리소스 효율성이 향상됩니다. 메모리 페이지가 작동하려면 **VM**에서 구성해야 하며 **VM**도 **virtio_balloon** 장치를 사용해야 합니다.

(BZ#1839055)

perf top의 정렬 순서 변경 지원

이번 업데이트를 통해 **perf top** 은 첫 번째 열에 따라 정렬하지 않고 그룹에 있는 여러 이벤트가 샘플링되는 경우 임의 이벤트 열별로 샘플을 정렬할 수 있습니다. 결과적으로 숫자 키를 누르면 일치하는 데이터 열에 따라 테이블이 정렬됩니다.

참고

열 번호는 **0** 에서 시작합니다.

group -sort-idx 명령줄 옵션을 사용하면 열 번호로 정렬할 수 있습니다.

(BZ#1851933)

kabi_whitelist 패키지의 이름이 **kabi_stablelist**로 변경되었습니다.

문제가 있는 언어 교체에 대한 **Red Hat**의 노력에 따라 **RHEL 8.4** 릴리스에서 **kabi_whitelist** 패키지의

이름을 kabi_stablelist 로 변경했습니다.

(BZ#1867910, BZ#1886901)

BPF를 버전 5.9로 업데이트

RHEL 8의 bpf 커널 기술은 커널 v5.9에서 업스트림 관련 기술을 최신 상태로 도입했습니다.

업데이트는 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 맵 요소를 위한 BPF(Berkeley Packet Filter) 반복기가 추가되어 커널 내 검사를 효율적으로 검사하기 위해 모든 BPF 프로그램을 반복합니다.
- 동일한 제어 그룹(cgroup)의 프로그램은 cgroup 로컬 스토리지 맵을 공유할 수 있습니다.
- BPF 프로그램은 소켓 조회 시 실행될 수 있습니다.
- SO_KEEPALIVE 및 관련 옵션은 bpf_setsockopt() 도우미에서 사용할 수 있습니다.

일부 BPF 프로그램은 소스 코드를 변경해야 할 수 있습니다.

(BZ#1874005)

bcc 패키지가 버전 0.16.0으로 업데이트

bcc 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 0.16.0으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 유틸리티 klockstat 및 funcinterval추가
- tcpconnect 도움말 페이지의 다양한 부분 수정

- tcptracer 도구 출력에서 IPv6 주소에 대한 SPORT 및 DPORT 열을 표시하도록 수정
- 손상된 종속성 수정

(BZ#1879411)

bpftrace가 0.11.0 버전으로 다시 기반

bpftrace 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 0.11.0으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 유틸리티 thread noop,tcpsynbl,tcplife,swapin,setuids, naptime추가
- tcpdrop.bt 및 syncs noop. bt 도구 실행 실패
- IBM Z 아키텍처에서 BPF(Berkeley Packet Filter) 프로그램을 로드하는 데 오류가 발생했습니다.
- 기호 조회 오류 수정

(BZ#1879413)

libbpf가 0.2.0.1 버전으로 업데이트

libbpf 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 0.2.0.1로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- BTF(BPF Type Format)가 액세스할 수 있는 프로그램에서 bpf_map 구조의 BPF(Berkeley Packet Filter) 맵 필드에 액세스하기 위한 지원이 추가되었습니다.
- 추가된 BPF 링 버퍼

- bpf 반복기 인프라 추가
- 개선된 bpf_link 가시성

(BZ#1919345)

perf는 perf 를 중지하거나 재시작할 필요 없이 실행 중인 컬렉터에서 추적 지점 추가 또는 제거 지원

이전에는 perf 레코드 인스턴스에서 추적 포인트를 추가하거나 제거하려면 perf 프로세스를 중지해야 했습니다. 그 결과 프로세스가 중지된 시간 동안 발생한 성능 데이터가 수집되지 않아 손실되었습니다. 이번 업데이트를 통해 perf 레코드 프로세스를 중지하지 않고도 제어 파이프 인터페이스를 통해 perf 레코드에서 수집하는 추적 지점을 동적으로 활성화 및 비활성화할 수 있습니다.

(BZ#1844111)

perf 툴은 추적 데이터에 대한 절대 타임스탬프를 기록하고 표시하는 기능을 지원합니다.

이번 업데이트를 통해 이제 perf 스크립트가 절대 타임스탬프를 사용하여 추적 데이터를 기록하고 표시할 수 있습니다.

참고: 절대 타임스탬프를 사용하여 추적 데이터를 표시하려면 지정된 클럭 ID를 사용하여 데이터를 기록해야 합니다.

절대 타임스탬프를 사용하여 데이터를 기록하려면 클럭 ID를 지정합니다.

```
# perf record -k CLOCK_MONOTONIC sleep 1
```

지정된 시계 ID로 기록된 추적 데이터를 표시하려면 다음 명령을 실행합니다.

```
# perf script -F+tod
```

(BZ#1811839)

버전 1.19.1로 변경되지 않음

dwarves 패키지가 버전 1.19.1로 업그레이드되어 여러 버그 수정 및 개선 사항을 제공합니다. 또한 이

번 업데이트에서는 관련 **ftrace** 항목이 있는 **DWARF** 디버그 데이터에서 기능을 확인하는 새로운 방법을 도입하여 **ftrace** 함수의 하위 집합이 생성되도록 합니다.

(BZ#1903566)

perf 는 지정된 이벤트를 사용하여 스냅샷을 트리거하는 순환 버퍼를 지원합니다.

이번 업데이트를 통해 지정한 이벤트가 감지될 때 **perf.data** 파일에 데이터를 쓰는 사용자 정의 원형 버퍼를 생성할 수 있습니다. 결과적으로 **perf** 레코드는 **perf. data** 파일에 데이터를 지속적으로 작성하여 과도한 오버헤드를 생성하지 않고 관심 있는 데이터만 기록하지 않고 시스템 백그라운드에서 계속 실행할 수 있습니다.

이벤트별 스냅샷을 기록하는 **perf** 툴을 사용하여 사용자 정의 원형 버퍼를 생성하려면 다음 명령을 사용합니다.

```
# perf record --overwrite -e _events_to_be_collected_ --switch-output-event
_snapshot_trigger_event_
```

(BZ#1844086)

커널 **DRBG** 및 **more** 엔트로피 소스는 **NIST SP 800-90A** 및 **NIST SP 800-90B**를 준수합니다.

DRBG(Kernel Deterministic Random BitGenerations) 및**tter** 엔트로피 소스는 **DRBG(NIST SP 800-90A)**를 사용하여 난수 생성에 대한 권장 사항과 임의 비트 생성**(NIST SP 800-90B)** 사양에 사용되는 엔트로피 소스에 대한 권장 사항을 준수합니다. 결과적으로 **FIPS** 모드의 애플리케이션은 이러한 소스를 **FIPS** 호환 임의성 및 잡음 소스로 사용할 수 있습니다.

(BZ#1905088)

Kdump는 **Virtual Local Area Network** 태그가 지정된 팀 네트워크 인터페이스를 지원

이번 업데이트에서는 **kdump** 에 대해 **Virtual Local Area Network** 태그가 지정된 팀 인터페이스를 구성하는 기능이 추가되었습니다. 결과적으로 이 기능을 사용하면 **kdump** 에서 **Virtual Local Area Network** 태그가 지정된 팀 인터페이스를 사용하여 **vmcore** 파일을 덤프할 수 있습니다.

(BZ#1844941)

kernel-rt 소스 트리가 **RHEL 8.4** 트리로 업데이트

최신 Red Hat Enterprise Linux 커널 소스 트리를 사용하도록 kernel-rt 소스가 업데이트되었습니다. 실시간 패치 세트도 최신 업스트림 버전 v5.10-rt7로 업데이트되었습니다. 이 두 업데이트 모두 여러 버그 수정 및 개선 사항을 제공합니다.

(BZ#1858099, BZ#1858105)

stalld 패키지가 RHEL 8.4 배포에 추가되었습니다.

이번 업데이트에서는 대기 시간이 짧은 애플리케이션을 실행하는 시스템의 스레드를 모니터링하는 데몬인 RHEL 8.4.0.에 stalld 패키지가 추가되었습니다. 이 스크립트는 지정된 임계값에 대해 CPU에 예약되지 않고 run-queue에 있는 작업 스레드를 확인합니다.

지연된 스레드를 감지하면 stalld는 스케줄링 정책을 SCHED_DEADLINE 으로 일시적으로 변경하고 진행하기 위해 CPU 시간 슬라이스를 할당합니다. 시간 슬라이스가 완료되거나 스레드 블록이 완료되면 스레드가 원래 스케줄링 정책으로 돌아갑니다.

(BZ#1875037)

hv_24x7 및 hv_ gpci PMUs에서 CPU 핫플러그 지원

이번 업데이트를 통해 PMU 카운터가 CPU 핫 플러그에 올바르게 반응합니다. 결과적으로 비활성화되는 CPU에서 hv_gpci 이벤트 카운터가 실행 중이면 개수가 다른 CPU로 리디렉션됩니다.

(BZ#1844416)

POWERPC hv_24x7 중첩 이벤트에 대한 메트릭 사용 가능

이제 POWERPC hv_24x7 중첩 이벤트에 대한 지표를 perf 에 사용할 수 있습니다. 이러한 지표는 여러 이벤트를 집계하여 perf 카운터에서 얻은 값과 CPU가 워크로드를 처리할 수 있는지에 대한 보다 효과적인 이해를 제공합니다.

(BZ#1780258)

Hwloc가 버전 2.2.0으로 다시 기반

hwloc 패키지가 버전 2.2.0으로 업그레이드되어 다음과 같은 변경 사항을 제공합니다.

- hwloc 기능은 총 디스크 크기 및 섹터 크기를 포함하여 NVMe(Nonvolatile Memory

Express) 드라이브에 대한 세부 정보를 보고할 수 있습니다.

(BZ#1841354)

igc 드라이버가 완전히 지원됨

igc Intel 2.5G 이더넷 Linux 유선 LAN 드라이버는 RHEL 8.1에서 기술 프리뷰로 도입되었습니다. RHEL 8.4부터 모든 아키텍처에서 완전하게 지원됩니다. ethtool 유틸리티는 igc 유선 LAN도 지원합니다.

(BZ#1495358)

4.9. 파일 시스템 및 스토리지

RHEL 설치에서 16TiB 크기의 스왑 파티션 생성 지원

이전에는 RHEL을 설치할 때 설치 프로그램에서 자동 및 수동 파티션을 위해 최대 128GB의 스왑 파티션을 생성했습니다.

이번 업데이트를 통해 설치 프로그램이 최대 128GB의 스왑 파티션을 계속 만들지만 수동 파티셔닝의 경우 16TiB의 스왑 파티션을 만들 수 있습니다.

(BZ#1656485)

NVMe 장치 갑작스러운 제거

이번 개선된 기능을 통해 운영 체제에 사전에 알리지 않고도 Linux 운영 체제에서 NVMe 장치를 제거할 수 있습니다. 이렇게 하면 서버 가동 중지 시간을 제거하여 서버를 사용할 수 있도록 장치를 준비하기 위해 추가 단계가 필요하지 않으므로 NVMe 장치의 서비스 성능이 향상됩니다.

다음을 확인합니다.

- NVMe 장치를 신속하게 제거하려면 kernel-4.18.0-193.13.2.el8_2.x86_64 버전 이상이 필요합니다.
- NVMe 장치를 성공적으로 제거하려면 하드웨어 플랫폼 또는 플랫폼에서 실행되는 소프트웨어의 추가 요구 사항이 필요할 수 있습니다.

- 시스템 작업에 중요한 NVMe 장치를 제거하는 것은 지원되지 않습니다. 예를 들어 운영 체제 또는 스왑 파티션이 포함된 NVMe 장치를 제거할 수 없습니다.

(BZ#1634655)

Stratis 파일 시스템 심볼릭 링크 경로가 변경되었습니다

이 향상된 기능을 통해 Stratis 파일 시스템 symlink 경로가 /stratis/*<stratis-pool>* /*<filesystem-name>* 에서 /dev/stratis/*<stratis-pool>* /*<filesystem-name>* 으로 변경되었습니다. 따라서 새 symlink 경로를 활용하려면 기존의 모든 Stratis symlink를 마이그레이션해야 합니다.

포함된 stratis_migrate_symlinks.sh 마이그레이션 스크립트를 사용하거나 시스템을 재부팅하여 symlink 경로를 업데이트합니다. Stratis 파일 시스템을 자동으로 마운트하도록 systemd 장치 파일 또는 /etc/fstab 파일을 수동으로 변경한 경우 새 symlink 경로로 업데이트해야 합니다.

참고

새 Stratis symlink 경로로 구성을 업데이트하지 않거나 자동 마운트를 일시적으로 비활성화하는 경우 다음번에 시스템을 재부팅하거나 시작할 때 부팅 프로세스가 완료되지 않을 수 있습니다.

(BZ#1798244)

Stratis에서 암호화된 풀을 보조 Clevis 암호화 정책에 바인딩 지원

이 향상된 기능을 통해 이제 Tang 서버를 사용하여 암호화된 Stratis 풀을 NBDE(네트워크 바운드 디스크 암호화) 또는 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0에 바인딩할 수 있습니다. 암호화된 Stratis 풀을 NBDE 또는 TPM 2.0에 바인딩하면 풀 자동 잠금 해제가 가능합니다. 결과적으로 각 시스템 재부팅 후 커널 인증 키 설명을 제공하지 않고도 Stratis 풀에 액세스할 수 있습니다. Stratis 풀을 보조 Clevis 암호화 정책에 바인딩하면 기본 커널 인증 키 암호화가 제거되지 않습니다.

(BZ#1868100)

XFS 및 ext4 파일 시스템에서 DAX가 활성화된 시기를 제어하는 새 마운트 옵션

이번 업데이트에서는 FS_XFLAG_DAX inode 플래그와 결합할 때 XFS 및 ext4 파일 시스템의 파일에 대해 DAX(직접 액세스) 모드를 세부적으로 제어할 수 있는 새로운 마운트 옵션이 도입되었습니다. 이전

릴리스에서는 **dax** 마운트 옵션을 사용하여 전체 파일 시스템에 대해 **DAX**가 활성화되었습니다. 이제 파일별로 직접 액세스 모드를 활성화할 수 있습니다.

디스크의 플래그 **FS_XFLAG_DAX** 는 특정 파일 또는 디렉터리에 대해 **DAX**를 선택적으로 활성화하거나 비활성화하는 데 사용됩니다. **dax** 마운트 옵션은 플래그가 적용되는지 여부를 지정합니다.

- **-o dax=inode - FS_XFLAG_DAX** 를 따르십시오. 이는 **dax** 옵션이 지정되지 않은 경우 기본값입니다.
- **-O dax=never - DAX**를 활성화하지 않고 **FS_XFLAG_DAX** 를 무시합니다.
- **-o dax=always -** 항상 **DAX**를 활성화하고 **FS_XFLAG_DAX** 를 무시합니다.
- **-O dax - "dax=always"**의 별칭인 레거시 옵션입니다. 이는 향후 제거될 수 있으므로 **"-o dax=always"**를 선호합니다.

xfs _io 유틸리티의 **chatter** 명령을 사용하여 **FS_XFLAG_ DAX** 플래그를 설정할 수 있습니다.

```
# xfs_io -c "chattr +x" filename
```

(BZ#1838876, BZ#1838344)

SMB Direct 지원

이번 업데이트를 통해 **SMB** 클라이언트는 이제 **SMB Direct**를 지원합니다.

(BZ#1887940)

파일 시스템 마운트를 위한 새로운 **API** 추가

이번 업데이트를 통해 파일 시스템 컨텍스트(**fs_context**구조)라는 내부 커널 구조를 기반으로 파일 시스템을 마운트하기 위한 새 **API**가 **RHEL 8.4**에 추가되어 사용자 공간, **VFS** 및 파일 시스템 간의 마운트 매개 변수 통신 유연성이 향상되었습니다. 이에 따라 파일 시스템 컨텍스트에서 작동하기 위한 다음과 같은 시스템 호출이 있습니다.

-

fsopen() - fsname 매개 변수에 이름이 지정된 파일 시스템에 대해 커널 내에 빈 파일 시스템 구성 컨텍스트를 만들고 이를 생성 모드로 추가하고 파일 설명자에 첨부하여 반환됩니다.

- **fsmount() - fsopen()** 에서 반환한 파일 설명자를 가져와서 여기에 지정된 파일 시스템 루트에 대한 마운트 오브젝트를 만듭니다.
- **fsconfig() - fs open(2)** 또는 **fspick(2)** 시스템 호출에 설정된 파일 시스템 구성 컨텍스트에 대해 매개 변수를 제공하고 명령을 실행합니다.
- **fspick() -** 커널 내에 새 파일 시스템 구성 컨텍스트를 생성하고 기존 수퍼 블록을 연결하여 재구성할 수 있도록 합니다.
- **move_mount() -** 한 위치에서 다른 위치로 마운트를 이동합니다. 또한 **OPEN_TREE_CLONE** 시스템 호출과 함께 **fsmount()** 또는 **open_tree()** 로 만든 연결되지 않은 마운트를 연결하는 데 사용할 수 있습니다.
- **open_tree() - pathname**에서 지정한 마운트 개체를 선택하여 새 파일 설명자에 연결하거나 복제하여 파일 설명자에 복제합니다.

mount() 시스템 호출을 기반으로 하는 이전 **API**는 계속 지원됩니다.

자세한 내용은 커널 소스 트리의 **Documentation/filesystems/mount_api.txt** 파일을 참조하십시오.

(BZ#1622041)

vfat 파일 시스템 **mtime** 의 불일치가 더 이상 발생하지 않음

이번 업데이트를 통해 메모리 내와 디스크의 쓰기 시간 간 **vfat** 파일 시스템 **mtime** 의 불일치가 더 이상 존재하지 않습니다. 이러한 불일치는 더 이상 발생하지 않는 메모리 내 및 디스크의 **mtime** 메타데이터의 차이로 인해 발생했습니다.

(BZ#1533270)

RHEL 8.4 에서 **close_range()** 시스템 호출 지원

이번 업데이트를 통해 **close_range()** 시스템 호출이 **RHEL 8.4**로 백포트되었습니다. 이 시스템 호출은 지정된 범위의 모든 파일 설명자를 효과적으로 닫아 애플리케이션이 매우 큰 제한을 구성하는 경우 다양한 파일 설명자를 순차적으로 닫을 때 표시되는 타이밍 문제를 방지합니다.

(BZ#1900674)

NFSv4.2 프로토콜을 통한 사용자 확장 속성 지원 추가

이번 업데이트에서는 사용자 확장 속성**(RFC 8276)**에 대한 **NFSV4.2** 클라이언트 측 및 서버 측 지원이 추가되어 새로 다음과 같은 프로토콜 확장이 포함됩니다.

새로운 작업**:**

- **- GETXATTR -** 파일의 확장 속성 가져오기
- **- SETXATTR -** 파일의 확장 속성 설정
- **- LISTXATTR -** 파일의 확장 속성 나열
- **- REMOVEXATTR -** 파일의 확장 속성 제거

새로운 오류 코드**:**

- **- NFS4ERR-NOXATTR - xattr** 이 존재하지 않습니다.
- **- NFS4ERR_XATTR2BIG - xattr** 값이 너무 큽니다.

새 속성**:**

- **- xattr_support - /-fs** 읽기 전용 특성으로 인해 **xattrs** 가 지원되는지 여부를 결정합니다. **True** 로 설정하면 오브젝트의 파일 시스템은 확장된 속성을 지원합니다.

(BZ#1888214)

4.10. 고가용성 및 클러스터

공동 배치 제한 조건의 중요하지 않은 리소스 지원

이 향상된 기능을 사용하면 제약 조건의 종속 리소스가 실패에 대한 마이그레이션 임계값에 도달하면 Pacemaker에서 해당 리소스를 오프라인 상태로 유지하고 두 리소스를 다른 노드로 이동하려고 시도하지 않고 현재 노드에 기본 리소스를 유지할 수 있습니다. 이 동작을 지원하기 위해 이제 공동 배치 제한 조건이 true 또는 false 로 설정될 수 있으며 리소스의 중요한 메타 기여도 true 또는 false로 설정할 수 있습니다. 중요한 리소스 메타 옵션의 값은 리소스를 종속 리소스로 포함하는 모든 공동 배치 제약 조건에 대한 impact 옵션의 기본값을 결정합니다.

영향 공동 배치 제한 조건 옵션에 true Pacemaker 값이 있는 경우 기본 리소스와 종속 리소스를 모두 활성 상태로 유지하려고 합니다. 종속 리소스가 실패에 대한 마이그레이션 임계값에 도달하면 가능하면 두 리소스 모두 다른 노드로 이동합니다.

영향 공동 배치 옵션의 값이 false인 경우 Pacemaker는 종속 리소스 상태의 결과로 기본 리소스를 이동하지 않습니다. 이 경우 종속 리소스가 실패에 대한 마이그레이션 임계값에 도달하면 기본 리소스가 활성 상태이며 현재 노드에 남아 있을 수 있는 경우 중지됩니다.

기본적으로 중요한 리소스 meta 옵션의 값은 true 로 설정되어, 그 다음, impact 옵션의 기본값이 true 임을 결정합니다. 이렇게 하면 Pacemaker에서 두 리소스를 모두 활성 상태로 유지하려고 하는 이전 동작이 유지됩니다.

(BZ#1371576)

Pacemaker 규칙에서 지원하는 새로운 수 데이터 유형

PCS는 이제 규칙을 수락 하는 PCS 명령에 Pacemaker 규칙을 정의할 때 사용할 수 있는 데이터 유형을 지원합니다. Pacemaker 규칙은 double -precision 부동 소수점 번호로 숫자를 구현하고 64비트 정수로 정수 를 구현합니다.

(BZ#1869399)

복제 리소스 또는 승격 가능한 복제 리소스를 생성할 때 사용자 정의 복제 ID를 지정하는 기능

복제 리소스 또는 promotable 복제 리소스를 생성하면 복제 리소스의 이름은 기본적으로 *resource-id* -clone 입니다. 해당 ID가 이미 사용 중인 경우 PCS는*정수* 값 1 부터 시작하여 추가 복제마다 하나씩 증가하여 접미사 - 정수를 추가합니다. pcs resource create 또는 pcs resource clone 명령으로 복제 리소스

를 생성할 때 *clone-id* 옵션으로 복제 리소스 ID 또는 promotable 복제 리소스 ID를 지정하여 이 기본값을 덮어쓸 수 있습니다. 복제 리소스 생성에 대한 자세한 내용은 여러 노드에서 활성 상태인 클러스터 리소스 생성을 참조하십시오.

(BZ#1741056)

Corosync 구성을 표시하는 새로운 명령

이제 새로운 pcs cluster config [show] 명령을 사용하여 여러 출력 형식으로 corosync.conf 파일의 내용을 출력할 수 있습니다. 기본적으로 pcs cluster config 명령은 텍스트 출력 형식을 사용하며 pcs cluster setup 및 pcs cluster config update 명령과 동일한 구조 및 옵션 이름과 함께 사람이 읽을 수 있는 형식으로 Corosync 구성을 표시합니다.

(BZ#1667066)

기존 클러스터의 Corosync 구성을 수정하기 위한 새로운 명령

새 pcs cluster config update 명령을 사용하여 corosync.conf 파일의 매개변수를 수정할 수 있습니다. 예를 들어 이 명령을 사용하여 임시 시스템이 응답하지 않는 동안 펜싱을 피하도록 totem 토큰을 늘릴 수 있습니다. corosync.conf 파일 수정에 대한 자세한 내용은 pcs 명령으로 corosync.conf 파일 수정을 참조하십시오.

(BZ#1667061)

기존 클러스터에서 Corosync 트래픽 암호화 활성화 및 비활성화

이전에는 새 클러스터를 생성할 때만 Corosync 트래픽 암호화를 구성할 수 있었습니다. 이번 업데이트로 다음이 가능합니다:

- pcs cluster config update 명령을 사용하여 Corosync crypto 암호화 암호 및 해시의 구성을 변경할 수 있습니다.
- pcs cluster authkey corosync 명령을 사용하여 Corosync authkey 를 변경할 수 있습니다.

(BZ#1457314)

공유 및 암호화된 GFS2 파일 시스템용 새로운 암호화 리소스 에이전트

RHEL HA는 이제 공유 및 암호화된 GFS2 파일 시스템을 제공하는 데 사용할 수 있는 LUKS 암호화된 블록 장치를 구성할 수 있는 새로운 암호화 리소스 에이전트를 지원합니다. crypt 리소스를 사용하는 것은 현재 GFS2 파일 시스템에서만 지원됩니다. 암호화된 GFS2 파일 시스템 구성에 대한 자세한 내용은 클러스터에서 암호화된 GFS2 파일 시스템 구성을 참조하십시오.

(BZ#1471182)

4.11. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

새 모듈: python39

RHEL 8.4에는 새 모듈 python39 및 ubi8/python-39 컨테이너 이미지에서 제공하는 Python 3.9가 도입되었습니다.

Python 3.8과 비교하여 주요 개선 사항은 다음과 같습니다.

- 병합(|) 및 업데이트(|=) 운영자가 dict 클래스에 추가되었습니다.
- 접두사 및 접미사를 제거하는 메서드가 문자열에 추가되었습니다.
- 유형 힌트 일반 항목이 list 및 dict 와 같은 특정 표준 유형에 추가되었습니다.
- 이제 새 zoneinfo 모듈을 통해 IANA 시간대 데이터베이스를 사용할 수 있습니다.

Python 3.9 및 여기에 빌드된 패키지는 동일한 시스템에 Python 3.8 및 Python 3.6과 병렬로 설치할 수 있습니다.

python39 모듈에서 패키지를 설치하려면 다음을 사용합니다.

```
# yum install python39
# yum install python39-pip
```

python39:3.9 모듈 스트림은 자동으로 활성화됩니다.

인터프리터를 실행하려면 다음을 사용합니다.

```
$ python3.9
$ python3.9 -m pip --help
```

자세한 내용은 Installing and using Python 에서 참조하십시오.

Red Hat은 RHEL 8의 라이프 사이클이 종료될 때까지 Python 3.6에 대한 지원을 계속 제공합니다. Python 3.8과 마찬가지로 Python 3.9는 라이프사이클이 짧습니다. Red Hat Enterprise Linux 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1877430)

Python urllib 구문 분석 함수의 기본 구분 기호 변경

Python urllib 라이브러리에서 CVE-2021-23336에 대한 웹 캐시를 완화하려면 urllib .parse.parse_qsl 및 urllib.parse.parse_qs 함수의 기본 구분 기호가 앰퍼샌드(&) 및 세미콜론(;)에서 앰퍼샌드(;)로만 변경됩니다.

이러한 변경 사항은 RHEL 8.4 릴리스와 함께 Python 3.6에서 구현되었으며 다음 RHEL 8의 마이너 릴리스에서 Python 3.8 및 Python 2.7으로 백포트됩니다.

기본 구분 기호의 변경은 이전 버전과 호환되지 않을 수 있으므로 Red Hat에서는 기본 구분 기호가 변경된 Python 패키지에서 동작을 구성하는 방법을 제공합니다. 또한 영향을 받는 urllib 구문 분석 기능은 고객의 애플리케이션이 변경의 영향을 받았음을 감지하면 경고 메시지가 표시됩니다.

자세한 내용은 Python urllib 라이브러리의 Mitigation of Web Cache Poisoning(CVE-2021-23336) 을 참조하십시오.

Python 3.9는 영향을 받지 않으며 Python 코드에서 urllib.parse.parse _qsl 및 urllib.parse.parse_q s 함수를 호출할 때 구분 기호 매개 변수를 전달하여 변경할 수 있는 새로운 기본 구분 기호(&)가 이미 포함되어 있습니다.

(BZ#1935686, BZ#1928904)

새 모듈 스트림: swig:4.0

RHEL 8.4에는 새 모듈 스트림인 swig:4.0 으로 사용할 수 있는 SWIG(Simplified Wrapper and Interface Generation) 버전 4.0이 도입되었습니다.

이전에 출시된 SWIG 3.0 의 주요 변경 사항은 다음과 같습니다.

- 지원되는 유일한 Python 버전은 다음과 같습니다. 2.7 및 3.2에서 3.8.
- Python 모듈이 개선되었습니다. 생성된 코드가 간소화되었으며 대부분의 최적화가 기본적으로 활성화됩니다.
- Ruby 2.7 에 대한 지원이 추가되었습니다.
- 이제 PHP 7 이 지원되는 유일한 PHP 버전입니다. PHP 5 에 대한 지원이 제거되었습니다.
- 대규모 인터페이스 파일에서 SWIG 를 실행할 때 성능이 크게 향상되었습니다.
- 명령줄 옵션 파일(응답 파일이라고도 함)에 대한 지원이 추가되었습니다.
- JavaScript Node.js 버전 2~10이 추가되었습니다.
- Octave 버전 4.4 ~ 5.1 지원이 추가되었습니다.

swig:4.0 모듈 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install swig:4.0
```

swig:3.0 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

swig 모듈 스트림에 대한 지원 기간에 대한 자세한 내용은 Red Hat Enterprise Linux 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1853639)

새 모듈 스트림: subversion:1.14

RHEL 8.4에는 새 모듈 스트림 subversion:1.14 가 도입되었습니다. Subversion 1.14 는 최신 LTS(장기 지원) 릴리스입니다.

RHEL 8.0에서 배포한 Subversion 1.10 이후의 주요 변경 사항은 다음과 같습니다.

- Subversion 1.14 에는 Subversion 을 고객의 빌드 및 릴리스 인프라에 통합하고 자동화를 위한 Python 3 바인딩이 포함되어 있습니다.
- 새 svnadmin rev-size 명령을 사용하면 사용자가 리버전의 총 크기를 확인할 수 있습니다.
- 새 svnadmin build-repcache 명령을 사용하면 관리자가 rep-cache 데이터베이스를 누락된 항목으로 채울 수 있습니다.
- 현재 작업 복사본 상태에 대한 개요를 제공하기 위해 새로운 실험적 명령이 추가되었습니다.
- svn 로그, svn info 및 svn list 명령에 대한 다양한 개선 사항이 구현되었습니다. 예를 들어 svn list --œ-readable 은 이제 파일 크기에 대해 사람이 읽을 수 있는 유닛을 사용합니다.
- 대규모 작업 복사본의 svn 상태가 상당히 향상되었습니다.

호환성 정보:

- Subversion 1.10 클라이언트 및 서버는 Subversion 1.14 서버 및 클라이언트와 상호 운용됩니다. 그러나 클라이언트와 서버가 최신 버전으로 업그레이드되지 않는 한 특정 기능을 사용할 수 없을 수 있습니다.
- Subversion 1.10에서 생성된 리포지토리를 Subversion 1.14 에 로드할 수 있습니다.
-

RHEL 8에서 배포된 Subversion 1.14 를 사용하면 클라이언트 측의 일반 텍스트로 암호를 캐시할 수 있습니다. 이 동작은 Subversion 1.10과 동일하지만 Subversion 1.14 업스트림 릴리스와는 다릅니다.

- 실험용 Shelving 기능이 크게 변경되었으며 Subversion 1.10 에서 생성된 와 호환되지 않습니다. 자세한 내용 및 업그레이드 지침은 업스트림 문서를 참조하십시오.

- 글로벌 및 리포지토리별 규칙과 경로 기반 인증 구성의 해석이 Subversion 1.14 에서 변경되었습니다. 영향을 받는 구성에 대한 자세한 내용은 업스트림 설명서 를 참조하십시오.

subversion:1:14 모듈 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install subversion:1.14
```

subversion:1.10 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

하위 버전 모듈 스트림에 대한 지원 기간에 대한 자세한 내용은 Red Hat Enterprise Linux 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1844947)

새 모듈 스트림: redis:6

이제 고급 키-값 저장소인 Redis 6 을 새 모듈 스트림 redis:6 으로 사용할 수 있습니다.

Redis 5 에 대한 주요 변경 사항은 다음과 같습니다.

- Redis 는 이제 모든 채널에서 SSL을 지원합니다.

- Redis 는 이제 명령 호출 및 키 패턴 액세스에 대한 사용자 권한을 정의하는 ACL(액세스 제어 목록)을 지원합니다.

- Redis 는 이제 더 많은 의미적 응답을 반환하는 새로운 RESP3 프로토콜을 지원합니다.

- 이제 Redis 에서 선택적으로 스레드를 사용하여 I/O를 처리할 수 있습니다.
- Redis 는 이제 주요 값의 클라이언트 측 캐싱에 서버 측 지원을 제공합니다.
- Redis 활성 만료 주기가 개선되어 만료된 키를 더 빠르게 제거할 수 있습니다.

Redis 6 은 이전 버전과 호환되지 않는 변경을 제외하고 Redis 5 와 호환됩니다.

- 세트 키가 없으면 SPOP <count> 명령이 더 이상 null을 반환하지 않습니다. Redis 6 에서 명령은 0 인수로 호출될 때와 유사하게 이 시나리오에서 빈 세트를 반환합니다.

redis:6 모듈 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install redis:6
```

redis:5 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

redis 모듈 스트림에 대한 지원 기간에 대한 자세한 내용은 Red Hat Enterprise Linux 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1862063)

새 모듈 스트림: postgresql:13

RHEL 8.4에는 버전 12에 비해 여러 가지 새로운 기능과 향상된 기능을 제공하는 PostgreSQL 13 이 도입되었습니다. 주요 변경 사항은 다음과 같습니다.

- B-tree 인덱스 항목의 중복 제거로 인한 성능 향상
- 집계 또는 파티셔닝 테이블을 사용하는 쿼리의 성능 향상

- 확장 통계를 사용할 때 쿼리 계획 개선
- 병렬화된 인덱스 봉인
- 증분 정렬

PostgreSQL 11 이후 업스트림에서 사용할 수 있는 JIT(Just-In-Time) 컴파일 지원은 postgresql:13 모듈 스트림에서 제공되지 않습니다.

PostgreSQL 사용을 참조하십시오.

postgresql:13 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install postgresql:13
```

RHEL 8에서 이전 postgresql 스트림에서 업그레이드하려면 이후 스트림으로 전환에 설명된 절차를 따라 PostgreSQL 8 버전으로 마이그레이션하십시오.

postgresql 모듈 스트림에 대한 지원 기간에 대한 자세한 내용은 Red Hat Enterprise Linux 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1855776)

새 모듈 스트림: mariadb:10.5

MariaDB 10.5 를 새 모듈 스트림 mariadb:10.5 로 사용할 수 있습니다. 이전에 사용 가능한 버전 10.3 에 비해 주요 개선 사항은 다음과 같습니다.

- 이제 MariaDB 에서 기본적으로 unix_socket 인증 플러그인을 사용합니다. 플러그인을 사용하면 로컬 Unix 소켓 파일을 통해 MariaDB 에 연결할 때 운영 체제 자격 증명을 사용할 수 있습니다.
- MariaDB 는 서버를 다시 시작하지 않고 SSL 인증서를 다시 로드하는 새 FLUSH SSL 명령을 지원합니다.

- **MariaDB** 는 **mariadb-*** 바이너리를 가리키는 바이너리와 **mysql*** 심볼릭 링크라는 **mariadb-*** 를 추가합니다. 예를 들어 **mysqladmin,mysqlaccess** 및 **mysqlshow symlink**는 **mariadb-admin,mariadb-access** 및 **mariadb-show** 바이너리를 각각 가리킵니다.

- **MariaDB** 는 **IPv 6** 주소를 저장하기 위한 새로운 **INET 6** 데이터 유형을 지원합니다.

- 이제 **MariaDB** 는 **Perl Compatible Regular Expressions(PCRE)** 라이브러리 버전 **2**를 사용합니다.

- **SUPER** 권한이 각 사용자 역할에 맞게 여러 권한으로 분할되었습니다. 결과적으로 특정 문이 필수 권한이 변경되었습니다.

- **MariaDB** 는 새로운 글로벌 변수 **binlog_row_metadata** 와 시스템 변수 및 상태 변수를 추가하여 기록된 메타데이터의 양을 제어합니다.

- **eq_range_index_dive_limit** 변수의 기본값이 **0** 에서 **200** 으로 변경되었습니다.

- 새 **SHUTDOWN FOR ALL SLAVES server** 명령과 새로운 **mysqladmin shutdown --wait-for-all-slaves** 옵션이 추가되어 마지막 **binlog** 이벤트가 연결된 모든 복제본에 전송된 경우에만 서버가 종료되도록 지시했습니다.

- 병렬 복제에서 **slave_parallel_mode** 변수는 이제 기본적으로 최적화되어 있습니다.

The InnoDB 스토리지 엔진에는 다음과 같은 변경 사항이 도입되었습니다.

- **InnoDB** 는 이제 인스턴트 **DROP COLUMN** 작업을 지원하고 사용자가 열 순서를 변경할 수 있습니다.

- **innodb_adaptive_hash_index**가 **OFF** 로, **innodb_ checksum_algorithm**을 **full_ crc32** 로 기본값이 변경되었습니다.

- Several InnoDB 변수가 제거되거나 더 이상 사용되지 않았습니다.

MariaDB Galera Cluster 가 다음과 같은 주요 변경 사항으로 버전 4로 업그레이드되었습니다.

- Galera 는 무제한 크기의 트랜잭션 복제를 지원하는 새로운 스트리밍 복제 기능을 추가합니다. 스트리밍 복제를 실행하는 동안 클러스터는 작은 조각으로 트랜잭션을 복제합니다.
- Galera 는 이제 글로벌 트랜잭션 ID(GTID)를 완벽하게 지원합니다.
- /etc/my.cnf.d/galera.cnf 파일의 wsrep_on 옵션의 기본값이 1 에서 0 으로 변경되어 추가 옵션을 구성하지 않고 최종 사용자가 wsrep 복제를 시작하지 않습니다.

MariaDB 사용을 참조하십시오.

mariadb:10.5 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install mariadb:10.5
```

mariadb:10.3 모듈 스트림에서 업그레이드하려면 MariaDB 10.3에서 MariaDB 10.5로 업그레이드를 참조하십시오.

mariadb 모듈 스트림에 대한 지원 기간에 대한 자세한 내용은 Red Hat Enterprise Linux 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1855781)

MariaDB 10.5 는 PAM 플러그인 버전 2.0을 제공합니다.

MariaDB 10.5 에서는 새 버전의 PAM(Pluggable Authentication Modules) 플러그인을 추가합니다. PAM 플러그인 버전 2.0은 별도의 setuid 루트 도우미 바이너리를 사용하여 PAM 인증을 수행합니다. 이 바이너리는 MariaDB 에서 추가 PAM 모듈을 활용할 수 있도록 합니다.

MariaDB 10.5 에서는 PAM(Pluggable Authentication Modules) 플러그인과 관련 파일이 새 패키지 mariadb-pam 으로 이동되었습니다. 이 패키지에는 PAM 플러그인 버전이 모두 포함되어 있습니다. 버전

2.0은 기본값이며 버전 1.0은 auth_pam_v1 공유 개체 라이브러리로 사용할 수 있습니다.

mariadb-pam 패키지는 MariaDB 서버와 함께 기본적으로 설치되지 않습니다. MariaDB 10.5 에서 PAM 인증 플러그인을 사용하려면 mariadb-pam 패키지를 수동으로 설치합니다.

알려진 문제 PAM 플러그인 버전 1.0이 MariaDB에서 작동하지 않음 도 참조하십시오.

(BZ#1936842)

새 패키지: mysql-selinux

RHEL 8.4는 SELinux 모듈에 MariaDB 및 MySQL 데이터베이스에 대한 규칙을 제공하는 새 mysql-selinux 패키지를 추가합니다. 패키지는 기본적으로 데이터베이스 서버와 함께 설치됩니다. 모듈의 우선 순위는 200 으로 설정됩니다.

(BZ#1895021)

Python-PyMySQL 이 0.10.1 버전으로 업데이트

pure -Python MySQL 클라이언트 라이브러리를 제공하는 python-PyMySQL 패키지가 0.10.1 버전으로 업데이트되었습니다. 패키지는 python36, python 38 및 python 39 모듈에 포함되어 있습니다.

주요 변경 사항은 다음과 같습니다.

- 이번 업데이트에서는 ed25519 및 caching_sha2_password 인증 메커니즘에 대한 지원이 추가되었습니다.
- python38 및 python 39 모듈의 기본 문자 집합은 업스트림과 일치하는 utf8mb4 입니다. python36 모듈은 이 모듈의 이전 버전과의 호환성을 유지하기 위해 기본 latin1 문자 집합을 유지합니다.
- python36 모듈에서 /usr/lib/python3.6/site-packages/pymysql/tests/ 디렉터리를 더 이상 사용할 수 없습니다.

(BZ#1820628, BZ#1885641)

새 패키지: python3-pyodbc

이번 업데이트에서는 python3-pyodbc 패키지가 RHEL 8에 추가됩니다. pyodbc Python 모듈은 ODBC(Open Database Connectivity) 데이터베이스에 액세스할 수 있습니다. 이 모듈은 Python DB API 2.0 사양을 구현하며 타사 ODBC 드라이버와 함께 사용할 수 있습니다. 예를 들어 Performance Co-Pilot(pcp)을 사용하여 SQL 서버의 성능을 모니터링할 수 있습니다.

(BZ#1881490)

새 패키지: micropipenv

이제 새로운 micropipenv 패키지를 사용할 수 있습니다. pip 패키지 설치 프로그램을 위한 경량 래퍼를 제공하여 nv 및 Poetry 잠금 파일을 지원합니다.

micropipenv 패키지는 AppStream 리포지토리에 배포되며 호환성 수준 4에서 제공됩니다. 자세한 내용은 Red Hat Enterprise Linux 8 애플리케이션 호환성 가이드를 참조하십시오.

(BZ#1849096)

새 패키지: py3c-devel 및 py3c-docs

RHEL 8.4에서는 새로운 py3c-devel 및 py3c-docs 패키지를 도입하여 Python 3으로 C 확장 이식을 간소화합니다. 이러한 패키지에는 자세한 가이드와 쉽게 이식하기 위한 일련의 매크로가 포함되어 있습니다.

py3c-devel 및 py3c-docs 패키지는 지원되지 않는 CodeReady Linux Builder(CRB) 리포지토리를 통해 배포됩니다.

(BZ#1841060)

httpd구성을 위한 향상된 ProxyRemote 지시문

Apache HTTP 서버의 ProxyRemote 구성 지시문은 선택적으로 사용자 이름 및 암호 자격 증명을 사용하도록 향상되었습니다. 이러한 자격 증명은 HTTP 기본 인증을 사용하여 원격 프록시에 인증하는 데 사용됩니다. 이 기능은 httpd 2.5 에서 백포트되었습니다.

(BZ#1869576)

엔드 포인트가 아닌 인증서는 SSLProxyMachineCertificateFile 및 SSLProxyMachineCertificate Path httpd 지시문과 함께 사용할 수 있습니다.

이번 업데이트를 통해 Apache HTTP Server의 SSLProxyMachineCertificateFile 및 SSLProxyMachineCertificate Path 구성 지시문과 함께 CA(인증 기관) 또는 중간 인증서와 같은 비종속성(비리프) 인증서를 사용할 수 있습니다. 이제 Apache HTTP 서버는 SSLProxyMachineCertificateFile 지시문과 함께 사용된 것처럼 이러한 인증서를 신뢰할 수 있는 CA로 처리합니다. 이전 버전에서는 SSLProxyMachineCertificateFile 및 SSLProxyMachineCertificate Path 지시문과 함께 엔드 엔드 인증서가 사용되지 않은 경우 httpd 가 구성 오류로 시작하지 못했습니다.

(BZ#1883648)

mod_security 모듈의 새 SecRemoteTimeout 지시문

이전에는 Apache HTTP Server의 mod_security 모듈에서 원격 규칙을 검색하기 위해 기본 시간 초과를 수정할 수 없었습니다. 이번 업데이트를 통해 새 SecRemoteTimeout 구성 지시문을 사용하여 사용자 지정 시간 초과를 초 단위로 설정할 수 있습니다.

시간 초과에 도달하면 이제 httpd 가 오류 메시지 Timeout에 도달하여 실패합니다. 이 시나리오에서는 구성 파일이 구문으로 유효한 경우에도 오류 메시지에 구문 오류도 포함됩니다. 타임아웃 시 httpd 동작은 SecRemoteRulesFailAction 구성 지시문 값에 따라 달라집니다(기본값은 Abort임).

(BZ#1824859)

mod_fcgid 모듈은 1024개의 환경 변수를 FCGI 서버 프로세스에 전달할 수 있습니다.

이번 업데이트를 통해 Apache HTTP Server의 mod_fcgid 모듈은 1024개의 환경 변수를 FastCGI(FCGI) 서버 프로세스에 전달할 수 있습니다. 이전 64개의 환경 변수 제한으로 인해 FCGI 서버에서 실행되는 애플리케이션이 작동하지 않을 수 있습니다.

(BZ#1876525)

AppStream 리포지토리에서 Perl-IO-String 사용 가능

Perl IO:: String 모듈을 제공하는 perl-IO- String 패키지는 이제 지원되는 AppStream 리포지토리를 통해 배포됩니다. RHEL 8의 이전 릴리스에서는 지원되지 않는 CodeReady Linux Builder 리포지토리에서 perl-IO-String 패키지를 사용할 수 있었습니다.

(BZ#1890998)

새 패키지: quota-devel

RHEL 8.4에는 quota-devel 패키지가 도입되어 RPC(원격 프로시저 호출) 서비스를 구현하기 위한 헤더 파일을 제공합니다.

quota-devel 패키지는 지원되지 않는 CRB(CodeReady Linux Builder) 리포지토리를 통해 배포됩니다.

(BZ#1868671)

4.12. 컴파일러 및 개발 도구

glibc 라이브러리는 최적화된 공유 라이브러리 구현을 로드하기 위한 glibc-hwcaps 하위 디렉토리를 지원

특정 아키텍처에서 하드웨어 업그레이드로 인해 glibc 가 이전 하드웨어 세대에 최적화된 라이브러리가 아니라 기준 최적화로 라이브러리를 로드하는 경우가 있었습니다. 또한 AMD CPU에서 실행할 때 최적화된 라이브러리가 로드되지 않았습니다.

이 향상된 기능을 통해 glibc -hwcaps 하위 디렉토리에 최적화된 라이브러리 구현을 찾을 수 있습니다. 동적 로더는 사용 중인 CPU와 해당 하드웨어 기능을 기준으로 하위 디렉터리에서 라이브러리 파일을 확인합니다. 이 기능은 다음 아키텍처에서 사용할 수 있습니다. IBM Power Systems(Lttle endian), IBM Z, 64비트 AMD 및 Intel.

(BZ#1817513)

glibc 동적 로더가 런타임 시 선택한 감사 모듈을 활성화합니다.

이전에는 binutils 링크 편집기 에서 --audit 옵션을 지원하여 런타임 시 활성화할 감사 모듈을 선택했지만 glibc 동적 로더는 요청을 무시했습니다. 이번 업데이트를 통해 glib 동적 로더는 더 이상 요청을 무시하고 표시된 감사 모듈을 로드하지 않습니다. 따라서 래퍼 스크립트를 작성하거나 유사한 메커니즘을 사용하지 않고 특정 프로그램에 대해 감사 모듈을 활성화할 수 있습니다.

(BZ#1871385)

Gli bc, IBM POWER9에서 향상된 성능 제공

이번 업데이트에서는 **IBM POWER9**용 **strlen,strcpy,stpcpy** 및 **rawmemchr** 함수의 새로운 구현을 소개합니다. 결과적으로 이러한 기능은 **IBM POWER9** 하드웨어에서 더 빨리 실행되므로 성능이 향상됩니다.

(BZ#1871387)

IBM Z에서 **memcpy** 및 **me mset** 의 최적화된 성능

이 향상된 기능을 통해 **memcpy** 및 **mem set API**의 코어 라이브러리 구현이 **IBM Z** 프로세서에서 작은**(64KiB)** 및 대용량 데이터 복사본을 모두 가속화하도록 조정되었습니다. 그 결과 인메모리 데이터로 작업하는 애플리케이션은 이제 다양한 워크로드에서 성능이 크게 향상되었습니다.

(BZ#1871395)

GCC는 **ARMv8.1 LSE atomic** 명령을 지원

이 향상된 기능을 통해 **GCC** 컴파일러는 **ARMv8.1** 사양으로 추가된 원자성 명령인 **LSE**(대규모 시스템 확장)를 지원합니다. 이러한 지침은 **ARMv8.0 Load-Exclusive** 및 **Store-Exclusive** 명령보다 다중 스레드 애플리케이션에서 더 나은 성능을 제공합니다.

(BZ#1821994)

GCC는 이제 특정 **IBM Z** 시스템에 대한 벡터 정렬 힌트를 제공합니다.

이번 업데이트를 통해 **GCC** 컴파일러가 **IBM z13** 프로세서의 벡터 로드 및 정렬 힌트를 저장할 수 있습니다. 이 향상된 기능을 사용하려면 어셈블러가 이러한 힌트를 지원해야 합니다. 결과적으로 사용자는 특정 벡터 작업의 성능이 향상됩니다.

(BZ#1850498)

Dyninst가 버전 **10.2.1**로 업데이트

Dyninst 바이너리 분석 및 수정 도구가 버전 **10.2.1**로 업데이트되었습니다. 주요 버그 수정 및 개선 사항은 다음과 같습니다.

- **elfutils debuginfod** 클라이언트 라이브러리 지원.

- 향상된 병렬 바이너리 코드 분석.
- 대형 바이너리의 분석 및 계측 개선.

(BZ#1892001)

elfutils 를 버전 **0.182**로 다시 기반

elfutils 패키지가 버전 **0.182**으로 업데이트되었습니다. 주요 버그 수정 및 개선 사항은 다음과 같습니다.

- **DW_CFA_AARCH64_negate_ra_state** 명령을 인식합니다. 포인터 인증 코드(**PAC**)가 활성화되지 않은 경우 **DW_CFA_AARCH64_negate_ra_state** 를 사용하여 **64**비트 **ARM** 아키텍처에서 **PAC**용으로 컴파일된 코드를 사용할 수 있습니다.
- **elf_update** 는 **SHF _COMPRESSED** 플래그를 설정한 섹션에서 잘못된 **sh_ addralign** 값을 수정합니다.
- **debuginfod-client** 는 **ZSTD**로 압축된 커널 **ELF** 이미지를 지원합니다.
- **debuginfod** 는 보다 효율적인 패키지를 통과하여 스캔 중에 다양한 오류를 허용합니다. 정리 프로세스는 더 표시되고 인터럽트 가능하며 더 많은 **Prometheus** 지표를 제공합니다.

(BZ#1875318)

SystemTap 버전 **4.4**로 업데이트

SystemTap 계측 툴이 버전 **4.4**로 업데이트되어 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 사용자 공간 프로파일링의 성능 및 안정성 개선.
- 사용자는 이러한 아키텍처에서 암시적 스레드 로컬 스토리지 변수에 액세스할 수 있습니다. **AMD64, Intel 64, IBM Z, IBM Power Systems**의 **littleendian** 변형.

- 부동 소수점 값 처리를 위한 초기 지원.
- 전역 변수를 사용하여 스크립트의 동시성 향상. 글로벌 변수에 대한 동시 액세스를 보호하는 데 필요한 잠금이 최적화되어 가능한 가장 작은 중요한 지역에 걸쳐 있습니다.
- 프로파일로그와 함께 별칭을 정의하는 새로운 구문.
- 새 @probewrite 서술자.
- syscall 인수는 다시 쓸 수 있습니다.

주요 변경 사항에 대한 자세한 내용은 업데이트하기 전에 업스트림 릴리스 노트 를 참조하십시오.

(BZ#1875341)

Valgrind에서 IBM z14 지침 지원

이번 업데이트를 통해 Valgrind 툴 제품군은 IBM z14 프로세서에 대한 지침을 지원합니다. 결과적으로 Valgrind 툴을 사용하여 z14 벡터 명령 및 기타 z14 명령 집합을 사용하여 프로그램을 디버깅할 수 있습니다.

(BZ#1504123)

CMake는 3.18.2 버전으로 업데이트

CMake 빌드 시스템이 버전 3.11.4에서 버전 3.18.2로 업그레이드되었습니다. RHEL 8.4에서 cmake-3.18.2-8.el8 패키지로 사용할 수 있습니다.

버전이 3.18.2 이하인 프로젝트에서 CMake를 사용하려면 cmake_minimum_required(버전 x.y.z) 명령을 사용합니다.

새로운 기능 및 사용되지 않는 기능에 대한 자세한 내용은 CMake 릴리스 노트 를 참조하십시오.

(BZ#1816874)

libmpc 를 버전 **1.1.0**으로 업데이트

libmpc 패키지가 버전 **1.1.0**으로 업데이트되어 이전 버전에 비해 여러 개선 사항 및 버그 수정을 제공합니다. 자세한 내용은 **GNU MPC 1.1.0** 릴리스 노트를 참조하십시오.

(BZ#1835193)

업데이트된 **GCC** 툴 세트 **10**

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

RHEL 8.4에서 도입한 주요 변경 사항은 다음과 같습니다.

- **GCC** 컴파일러가 업스트림 버전으로 업데이트되어 여러 버그 수정을 제공합니다.
- **elfutils** 가 버전 **0.182**으로 업데이트되었습니다.
- **Dyninst**가 버전 **10.2.1**로 업데이트되었습니다.
- **SystemTap**이 **4.4** 버전으로 업데이트되었습니다.

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

툴	버전
GCC	10.2.1
GDB	9.2
valgrind	3.16.0
SystemTap	4.4

툴	버전
Dyninst	10.2.1
binutils	2.35
elfutils	0.182
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
```

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

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

자세한 내용은 GCC Toolset 사용을 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 포함되

어 있습니다.

컨테이너 이미지를 가져오려면 다음 명령을 root로 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 사용을 참조하십시오.

(BZ#1918055)

GCC 툴 세트 10: GCC는 이제 bfloat16을 지원합니다.

GCC Toolset 10에서는 GCC 컴파일러가 ACLE Intrinsics를 통해 bfloat16 확장을 지원합니다. 이 향상된 기능을 통해 고성능 컴퓨팅이 제공됩니다.

(BZ#1656139)

GCC 툴 세트 10: GCC는 Intel Sapphire Rapids 프로세서에서 ENœMD 및 EN œMDS 명령을 지원합니다.

GCC Toolset 10에서는 GCC(GNU Compiler Collection)를 지원하므로 이 명령을 사용하여 자동으로 장치에 작업 설명자를 제출할 수 있습니다. 이 향상된 기능을 적용하려면 -menqcmd 옵션을 사용하여 GCC를 실행합니다.

(BZ#1891998)

GCC 툴 세트 10: Dyninst가 버전 10.2.1로 업데이트

GCC Toolset 10에서는 Dyninst 바이너리 분석 및 수정 도구가 버전 10.2.1로 업데이트되었습니다. 주요 버그 수정 및 개선 사항은 다음과 같습니다.

- elfutils debuginfod 클라이언트 라이브러리 지원.

- 향상된 병렬 바이너리 코드 분석.
- 대형 바이너리의 분석 및 계측 개선.

(BZ#1892007)

GCC Toolset 10: elfutils 를 버전 0.182로 업데이트

GCC Toolset 10에서는 elfutils 패키지가 버전 0.182으로 업데이트되었습니다. 주요 버그 수정 및 개선 사항은 다음과 같습니다.

- DW_CFA_AARCH64_negate_ra_state 명령을 인식합니다. 포인터 인증 코드(PAC)가 활성화되지 않은 경우 DW_CFA_AARCH64_negate_ra_state 를 사용하여 64비트 ARM 아키텍처에서 PAC용으로 컴파일된 코드를 사용할 수 있습니다.
- elf_update 는 SHF _COMPRESSED 플래그를 설정한 섹션에서 잘못된 sh_ addralign 값을 수정합니다.
- debuginfod-client 는 ZSTD로 압축된 커널 ELF 이미지를 지원합니다.
- debuginfod 는 보다 효율적인 패키지를 통과하여 스캔 중에 다양한 오류를 허용합니다. 정리 프로세스는 더 표시되고 인터럽트 가능하며 더 많은 Prometheus 지표를 제공합니다.

(BZ#1879758)

Go Toolset을 버전 1.15.7로 업데이트

Go Toolset이 1.15.7로 업그레이드되었습니다. 주요 개선 사항은 다음과 같습니다.

- 이제 연결 속도가 빨라졌으며 새로 구현된 오브젝트 파일 형식과 내부 단계의 동시성 증가로 인해 메모리가 줄어듭니다. 이번 개선된 기능을 통해 내부 연결이 기본값입니다. 이 설정을 비활성화하려면 컴파일러 플래그 -ldflags=-linkmode=external 을 사용합니다.

- 최악의 대기 시간을 포함하여 코어 수가 많은 소규모 개체 할당이 개선되었습니다.

- 주체 대체 이름이 지정되지 않은 경우 **X.509** 인증서에서 **CommonName** 필드를 호스트 이름으로 처리합니다. 이제 기본적으로 비활성화되어 있습니다. 활성화하려면 **x509ignoreCN=0** 값을 **GODEBUG** 환경 변수에 추가합니다.

- **GOPROXY** 는 이제 오류를 반환하는 프록시 건너뛰기를 지원합니다.

- 이제 새 패키지 **time/tzdata** 를 포함합니다. 시간대 데이터베이스를 로컬 시스템에서 사용할 수 없는 경우에도 시간대 데이터베이스를 프로그램에 포함할 수 있습니다.

Go Toolset에 대한 자세한 내용은 **Go Toolset**을 사용합니다.

(BZ#1870531)

jboss Toolset을 버전 **1.49.0**으로 업데이트

satellite Toolset이 **1.49.0** 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 이제 **footdoc** 페이지 항목의 경로를 사용하여 **capsuledoc** 페이지 항목에서 링크할 수 있습니다.

- 이제 테스트 프레임워크가 스레드 출력을 숨깁니다. 실패한 테스트의 출력은 여전히 터미널에 표시됩니다.

- 이제 **[T; N]**을(를) 사용할 수 있습니다: **tryFrom<Vec<T✓** 벡터를 모든 길이의 배열로 바꿉니다.

- 슬라이스**::select_nth_unstable** 을 사용하여 순서가 지정된 파티셔닝을 수행할 수 있습니다. 이 기능은 다음과 같은 변형에서도 사용할 수 있습니다.

  - 슬라이스**::select_nth_unstable_by** 는 **comparator** 함수를 제공합니다.

- 슬라이스::select_nth_unstable_by_key 는 주요 추출 기능을 제공합니다.

- 이제 ManuallyDrop 을 union 필드의 유형으로 사용할 수 있습니다. 또한 단순 드롭(impl Drop for Union)을 사용하여 기존 유니언에 드롭 특성을 추가할 수도 있습니다. 이를 통해 특정 필드를 수동으로 삭제해야 하는 경우 유니언을 정의할 수 있습니다.

- pvc Toolset의 컨테이너 이미지가 더 이상 사용되지 않으며, pvc Toolset이 UBI(Universal Base Images) 리포지토리에 추가되었습니다.

자세한 내용은 Automate Toolset 사용을 참조하십시오.

(BZ#1896712)

LLVM Toolset을 버전 11.0.0으로 다시 설정

LLVM Toolset이 버전 11.0.0으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- -fstack-clash-protection 명령줄 옵션에 대한 지원이 AMD 및 Intel 64비트 아키텍처, IBM Power Systems, Little Endian 및 IBM Z에 추가되었습니다. 이 새로운 컴파일러 플래그는 각 스택 페이지를 자동으로 확인하여 stack-clash 공격으로부터 보호합니다.

- 새로운 컴파일러 플래그 ffp-exception-behavior={ignore,maytrap,strict} 를 사용하면 유동 지점 예외 동작을 지정할 수 있습니다. 기본 설정은 ignore 입니다.

- 새로운 컴파일러 플래그 ffp-model={precise,strict,fast} 를 사용하면 단일 용도의 유동 지점 옵션을 간소화할 수 있습니다. 기본 설정은 정확합니다.

- 새로운 컴파일러 플래그 -fno-common 가 기본적으로 활성화되어 있습니다. 이 향상된 기능을 통해 여러 번역 단위에서 C로 작성된 코드는 이제 다중 정의 연결기 오류를 트리거합니다. 이 설정을 비활성화하려면 -fcommon 플래그를 사용합니다.

- LLVM Toolset의 컨테이너 이미지가 더 이상 사용되지 않으며 LLVM Toolset이 UBI(Universal Base Images) 리포지토리에 추가되었습니다.

자세한 내용은 LLVM Toolset 사용을 참조하십시오.

(BZ#1892716)

PCP 를 버전 5.2.5로 업데이트

pcp 패키지가 버전 5.2.5로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- SQL Server 지표는 보안 연결을 통해 지원합니다.
- 프로세스별 네트워크 지표가 포함된 eBPF/BCC netproc 모듈.
- hv_24x7 코어 수준 및 hv_ gpci 이벤트 지표에 대한 pmdaperfevent(1) 지원.
- 새로운 Linux 프로세스 회계 지표, Linux ZFS 지표, Linux XFS 지표, Linux 커널 소켓 지표, Linux 다중 경로 TCP 지표, Linux 메모리 및 ZRAM 지표, NVM Express 디스크에 대한 S.M.A.R.T. 지표 지원.
- 시스템 및 프로세스 지표를 시각화하는 새로운 pcp-htop(1) 유틸리티입니다.
- pmrep /pcp2xxx 구성을 생성하는 새로운 pmrep conf(1) 유틸리티.
- pmie 서비스 제어를 위한 새로운 pmie ctl(1) 유틸리티.
- pm logger 서비스를 제어하는 새로운 pm logctl(1) 유틸리티.
- 로그 문자열 지표를 작성하는 새로운 pmlogpaste(1) 유틸리티.
- 회계 통계 및 프로세스별 네트워크 통계 보고를 처리하는 새로운 pcp-atop(1) 유틸리티.

- 함수, 언어 확장 및 **REST API** 쿼리를 위한 새로운 **pmseries(1)** 유틸리티.
- **OOM**이 종료되고 소켓 연결 포화 상태를 감지하기 위한 새로운 **pmie(1)** 규칙.
- **pcp-atopsar(1)**, **pcp-free(1)**, **pcp- dstat(1)**, **pmlogger(1)** 및 **pmchart(1)** 유틸리티의 버그 수정.
- 컨텍스트별 파생 지표에 대한 **REST API** 및 **C API** 지원.
- **OpenMetrics** 지표 메타데이터(단위, 의미 체계) 개선.
- 설치된 **/var** 파일 시스템 레이아웃을 광범위하게 다시 정렬했습니다.

(BZ#1854035)

grafana-pcp에서 **Vector** 데이터 소스의 중앙 **pmproxy** 를 통해 원격 호스트에 액세스

일부 환경에서는 네트워크 정책에서 대시보드 뷰어 브라우저에서 모니터링된 호스트로의 연결을 직접 허용하지 않습니다. 이번 업데이트를 통해 요청을 개별 호스트에 전달하는 중앙 **pmproxy** 에 연결하기 위해 **hostspec** 을 사용자 지정할 수 있습니다.

(BZ#1845592)

Grafana 가 버전 **7.3.6**으로 업데이트

grafana 패키지가 버전 **7.3.6**으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 새로운 패널 편집기 및 새로운 데이터 변환 기능
- 시간대 지원 개선
- 이제 기본 프로비저닝 경로가 **/usr/share/grafana/conf/provisioning** 에서 **/etc/grafana/provisioning** 디렉터리로 변경되었습니다. **/etc/grafana/grafana.ini** 구성 파일에서

이 설정을 구성할 수 있습니다.

자세한 내용은 Grafana v7.0의 새로운 기능, Grafana v 7.1의 새로운 기능, Grafana v 7.2의 새로운 기능, Grafana v 7.3의 What's New in Grafana v 7.1을 참조하십시오.

(BZ#1850471)

Grafana-pcp 버전이 3.0.2로 업데이트

grafana-pcp 패키지가 버전 3.0.2로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- Redis:
  - Grafana에서 경고 생성 지원.
  - 성능상의 이유로 Grafana 변수 쿼리에서 label_values(metric, label) 를 사용하는 것은 더 이상 사용되지 않습니다. label_values(label) 쿼리는 계속 지원됩니다.
- 벡터:
  - 쿼리 내에서 산술 연산자 및 통계 함수를 사용할 수 있는 파생 지표를 지원합니다. 자세한 내용은 pmRegisterDerived(3) 도움말 페이지를 참조하십시오.
  - 구성 가능한 hostspec - 중앙 pmproxy 를 통해 원격 PMCD(성능 지표 수집기 데몬)에 액세스할 수 있습니다.
  - 패널의 유닛을 자동으로 구성합니다.
- 대시보드:
  - USE(Utilization Saturation and Errors) 방법을 사용하여 잠재적인 성능 문제를 탐지하고 체크리스트 대시보드에서 가능한 솔루션을 보여줍니다.

- CGroups v2 를 사용한 새로운 MS SQL 서버 대시보드, eBPF/BCC 대시보드 및 컨테이너 개요 대시보드.

- 이제 모든 대시보드가 데이터 소스 설정 페이지의 Dashboards(대시보드) 탭에 있으며 자동으로 가져오지 않습니다.

업그레이드 노트:

Grafana 구성 파일을 업데이트합니다.

1. /etc/grafana/grafana.ini Grafana 구성 파일을 편집하고 다음 옵션이 설정되었는지 확인합니다.

```
allow_loading_unsigned_plugins = pcp-redis-datasource
```

2. Grafana 서버를 다시 시작합니다.

```
# systemctl restart grafana-server
```

(BZ#1854093)

PCP에서 SQL Server 메트릭에 액세스하기 위한 Active Directory 인증

이번 업데이트를 통해 시스템 관리자는 AD(Active Directory) 인증을 사용하여 SQL Server 지표에 안전하게 연결하도록 pmdamssql(1) 을 구성할 수 있습니다.

(BZ#1847808)

Grafana-container 가 버전 7.3.6으로 다시 기반

rhel8/grafana 컨테이너 이미지는 Grafana를 제공합니다. Grafana는 지표 대시보드가 있는 오픈소스 유틸리티이며 Graphite, Elasticsearch, OpenTSDB, Prometheus, InfluxDB 및 PCP(Performance Co-Pilot)의 그래픽 편집기입니다. grafana-container 패키지가 버전 7.3.6으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- grafana 패키지가 이제 버전 7.3.6으로 업데이트되었습니다.
- grafana-pcp 패키지가 버전 3.0.2로 업데이트되었습니다.

리베이스는 Red Hat Container Registry의 rhel8/grafana 이미지를 업데이트합니다.

이 컨테이너 이미지를 가져오려면 다음 명령을 실행합니다.

```
# podman pull registry.redhat.io/rhel8/grafana
```

(BZ#1916154)

PCP 컨테이너 버전이 5.2.5로 업데이트

rhel8/pcp 컨테이너 이미지는 시스템 성능 분석 툴킷인 Performance Co-Pilot을 제공합니다. pcp-container 패키지가 버전 5.2.5로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- pcp 패키지가 버전 5.2.5로 업데이트되었습니다.
- 컨테이너 내부에서 시작할 PCP 서비스의 쉼표로 구분된 목록을 지정하는 새로운 PCP_SERVICES 환경 변수를 도입했습니다.

리베이스는 Red Hat Container Registry의 rhel8/pcp 이미지를 업데이트합니다.

이 컨테이너 이미지를 가져오려면 다음 명령을 실행합니다.

```
# podman pull registry.redhat.io/rhel8/pcp
```

(BZ#1916155)

버전 8.0.0으로 다시 기반 JDK Mission Control

jmc:rhel8 모듈 스트림에서 제공하는 HotSpot JVM에 대한 JDK Mission Control(JMC) 프로파일러가 버전 8.0.0으로 업그레이드되었습니다. 주요 개선 사항은 다음과 같습니다.

- 클래스별로 메모리 사용량을 시각화하기 위해 **JOverflow** 플러그인에 **Treemap** 뷰어가 추가되었습니다.
- 스레드 그래프는 더 많은 필터링 및 확대 옵션을 사용하여 향상되었습니다.
- **JDK Mission Control**은 이제 **LZ4** 알고리즘으로 압축된 **JDKœ Recorder**를 여는 기능을 지원합니다.
- 메모리 및 **TLAB** 뷰에 새 열이 추가되어 할당 부족 영역을 식별할 수 있습니다.
- 스택 추적의 시각화를 개선하기 위해 그래프 보기가 추가되었습니다.
- **The Percentage** 열이 히스토그램 테이블에 추가되었습니다.

RHEL 8의 **JMC**에는 **JDK** 버전 **8** 이상을 실행해야 합니다. **JMC**가 **JDK¢ Recorder** 기능에 액세스할 수 있도록 목표 **Java** 애플리케이션은 **OpenJDK** 버전 **8**에서 실행해야 합니다.

jmc:rhel8 모듈 스트림에는 두 개의 프로필이 있습니다.

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

jmc:rhel8 모듈 스트림의 공통 프로필을 설치하려면 다음을 사용합니다.

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

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

(BZ#1919283)

4.13. IDM (IDENTITY MANAGEMENT)

Identity Management를 더 포함하기

Red Hat은 중요한 언어를 사용하기 위해 최선을 다하고 있습니다. 이 이니셔티브에 대한 자세한 내용은 보다 포괄적 수용을 위한 오픈 소스 용어 교체 에서 참조하십시오.

Identity Management에서 계획된 용어 교체는 다음과 같습니다.

- *차단 목록* 대체 *블랙리스트*
- *목록 교체 허용 화이트리스트*
- ***2차*** 대체 *슬레이브*
- ***master*** 라는 단어는 컨텍스트에 따라 더 정확한 언어로 바뀝니다.
  - ***IdM** 서버가 **IdM** 마스터*교체
  - ***CA** 갱신 서버가 **CA** 갱신 마스터*교체
  - ***CRL** 게시자 서버가 **CRL** 마스터*교체
  - *멀티 공급자* 대체 *멀티 마스터*

(JIRA:RHELPLAN-73418)

dsidm 유틸리티는 이름 변경 및 항목 이동 지원

이 향상된 기능을 통해 **dsidm** 유틸리티를 사용하여 **Directory Server**의 사용자, 그룹, **POSIX** 그룹, 역

할 및 조직 단위(OU)의 이름을 변경하고 이동할 수 있습니다. 자세한 내용 및 예는 Directory Server 관리 가이드의 사용자 이름 변경, 그룹, POSIX 그룹 및 OUs 섹션을 참조하십시오.

(BZ#1859218)

IdM에서 하위 CA 삭제

이 향상된 기능을 통해 ipa ca-del 명령을 실행하고 Sub-CA를 비활성화하지 않은 경우 Sub-CA를 삭제할 수 없으며 비활성화해야 합니다. 먼저 ipa ca-disable 명령을 실행하여 Sub-CA를 비활성화한 다음 ipa ca-del 명령을 사용하여 삭제합니다.

IdM CA는 비활성화하거나 삭제할 수 없습니다.

(JIRA:RHELPLAN-63081)

IdM에서 새로운 Ansible 관리 역할 및 모듈 지원

RHEL 8.4에서는 IdM(Identity Management)의 역할 기반 액세스 제어(RBAC) 자동화 관리를 위한 Ansible 모듈, IdM 서버를 백업하고 복원하는 Ansible 역할 및 위치 관리를 위한 Ansible 모듈을 제공합니다.

- ipapermission 모듈을 사용하여 IdM RBAC에서 권한 및 권한 구성원을 생성, 수정, 삭제할 수 있습니다.
- ipaprivilege 모듈을 사용하여 IdM RBAC에서 권한 및 권한 구성원을 생성, 수정, 삭제할 수 있습니다.
- iparole 모듈을 사용하여 IdM RBAC에서 역할 및 역할 구성원을 생성, 수정 및 삭제할 수 있습니다.
- ipadelegation 모듈을 사용하여 IdM RBAC의 사용자에게 권한을 위임할 수 있습니다.
- ipaselfservice 모듈을 사용하여 IdM에서 셀프 서비스 액세스 규칙을 생성, 수정 및 삭제할 수 있습니다.
-

ipabackup 역할을 사용하여 IdM 서버 백업을 생성, 복사 및 제거하고 제어 노드에서 IdM 서버를 로컬로 복원할 수 있습니다.

- ipalocation 모듈을 사용하여 데이터 센터 랙과 같은 호스트의 실제 위치가 있는지 확인할 수 있습니다.

(JIRA:RHELPLAN-72660)

FIPS 모드의 IdM이 AD로 교차 포리스트 신뢰 지원

이번 개선된 기능을 통해 관리자는 FIPS 모드와 AD(Active Directory) 도메인이 활성화된 IdM 도메인 간에 교차 포리스트 신뢰성을 설정할 수 있습니다. IdM에서 FIPS 모드가 활성화된 동안 공유 보안을 사용하여 신뢰를 설정할 수 없습니다. FIPS 컴플라이언스 를 참조하십시오.

(JIRA:RHELPLAN-58629)

AD 사용자는 알려진 UPN 접미사에 하위로 UPN 접미사로 IdM에 로그인할 수 있습니다.

이전에는 AD(Active Directory) 사용자가 알려진 UPN 접미사(예: TLN)의 하위 도메인인 UN(Universal Principal Name)을 사용하여 IdM(Identity Management)에 로그인할 수 없었습니다 . 내부 Samba 프로세스가 하위 도메인을 TLN(상위 수준 이름)의 중복으로 필터링했기 때문입니다. 이번 업데이트에서는 알려진 UPN 접미사에 종속되어 있는지 테스트하여 UPN의 유효성을 검사합니다. 결과적으로 사용자는 설명된 시나리오에서 하위 UPN 접미사를 사용하여 로그인할 수 있습니다.

(BZ#1891056)

IdM에서 새 암호 정책 옵션 지원

이번 업데이트를 통해 IdM(Identity Management)은 추가 libpwquality 라이브러리 옵션을 지원합니다.

--maxrepeat

동일한 문자의 최대 개수를 순서대로 지정합니다.

--maxsequence

단일 문자 시퀀스(abcd)의 최대 길이를 지정합니다.

--dictcheck

암호가 사전 단어인지 확인합니다.

--usercheck

암호에 사용자 이름이 포함되어 있는지 확인합니다.

새 암호 정책 옵션이 설정된 경우 **--minlength** 옵션 값과 관계없이 최소 암호 길이는 **6**자입니다. 새 암호 정책 설정은 새 암호에만 적용됩니다.

RHEL 7 및 **RHEL 8** 서버와 혼합된 환경에서는 새 암호 정책 설정이 **RHEL 8.4** 이상에서 실행되는 서버에만 적용됩니다. 사용자가 **IdM** 클라이언트에 로그인하고 **IdM** 클라이언트가 **RHEL 8.3** 이하에서 실행되는 **IdM** 서버와 통신하는 경우 시스템 관리자가 설정한 새 암호 정책 요구 사항이 적용되지 않습니다. 일관된 동작을 보장하려면 모든 서버를 **RHEL 8.4** 이상으로 업그레이드하거나 업데이트합니다.

(BZ#1340463)

Active Directory 사이트 검색 프로세스 개선

이제 **SSSD** 서비스에서 여러 도메인 컨트롤러에 대한 연결 없는 **LDAP(CLDAP)**를 통해 **Active Directory** 사이트를 병렬로 검색하여 일부 도메인 컨트롤러에 연결할 수 없는 상황에서 사이트 검색 속도를 높일 수 있습니다. 이전에는 사이트 검색이 순차적으로 수행되었으며 도메인 컨트롤러에 연결할 수 없는 상황에서 시간 초과가 발생하고 **SSSD**가 오프라인 상태가 되었습니다.

(BZ#1819012)

처리량을 높이기 위해 **nsslapd-nagle** 의 기본값이 꺼져 있습니다.

이전에는 **cn=config** 항목의 **nsslapd-nagle** 매개변수가 기본적으로 활성화되어 있었습니다. 그 결과 **Directory Server**는 서버 속도를 늦추는 일련의 **setsocketopt** 시스템 호출을 수행했습니다. 이번 업데이트에서는 기본값 **nsslapd-nagle** 을 **off** 로 변경합니다. 결과적으로 **Directory Server**는 더 적은 수의 **setsocketopt** 시스템 호출을 수행하고 초당 더 많은 수의 작업을 처리할 수 있습니다.

(BZ#1996076)

sssd.conf 파일의 **[domain]** 섹션에서 **SSSD** 도메인 활성화 또는 비활성화

이번 업데이트를 통해 **sssd.conf** 파일에서 각각의 **[domain]** 섹션을 수정하여 **SSSD** 도메인을 활성화하거나 비활성화할 수 있습니다.

이전에는 SSSD 구성에 독립 실행형 도메인이 포함되어도 sssd.conf 파일의 [sssd] 섹션에서 도메인 옵션을 수정해야 했습니다. 이번 업데이트를 통해 도메인 구성에서 enabled= 옵션을 true 또는 false로 설정할 수 있습니다.

- 활성화된 옵션을 true로 설정하면 sssd.conf 파일의 [sssd] 섹션에 있는 domain 옵션 아래에 나열되지 않아도 도메인이 활성화됩니다.
- 활성화된 옵션을 false로 설정하면 sssd.conf 파일의 [sssd] 섹션에 있는 domain 옵션 아래에 나열되어 있더라도 도메인을 false로 설정합니다.
- 활성화된 옵션을 설정하지 않으면 sssd.conf 의 [sssd] 섹션에 있는 domain 옵션의 구성이 사용됩니다.

(BZ#1884196)

최대 오프라인 시간 초과를 수동으로 제어하는 옵션이 추가되었습니다.

offline_timeout 기간은 SSSD가 다시 온라인 상태가 되는 시도 사이의 시간 증가를 결정합니다. 이전에는 이 간격에 가능한 최대 값이 3600초로 하드 코딩되어 일반적인 사용량에 적합하지만 변경 속도가 빠르고 느려진 문제가 발생했습니다.

이번 업데이트에서는 각 간격의 최대 길이를 수동으로 제어하기 위해 offline_timeout_max 옵션을 추가하여 SSSD에서 서버 동작을 추적할 수 있는 유연성이 향상되었습니다.

offline_timeout 매개변수 값과 상관 관계에서 이 값을 설정해야 합니다. 값이 0이면 증가 동작을 비활성화합니다.

(BZ#1884213)

SSSD 세션 기록 구성에서 scope=all 을 사용하여 exclude_users 및 exclude_groups 지원

Red Hat Enterprise 8.4에서는 대규모 그룹 또는 사용자에 대한 세션 기록을 정의할 수 있는 새로운 SSSD 옵션을 제공합니다.

1. exclude_users

기록에서 제외할 사용자의 쉼표로 구분된 목록은 **scope=all** 구성 옵션에만 적용됩니다.

2. **exclude_groups**

쉼표로 구분된 그룹 목록으로, 의 멤버는 기록에서 제외해야 합니다. **scope=all** 구성 옵션에만 적용할 수 있습니다.

자세한 내용은 **sssd-session-recording** 도움말 페이지를 참조하십시오.

(BZ#1784459)

Samba 가 버전 **4.13.2**로 업데이트

samba 패키지가 업스트림 버전 **4.13.2**로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- 인증되지 않은 사용자가 **netlogon** 프로토콜을 사용하여 도메인을 인수할 수 있는 보안 문제를 방지하려면 **Samba** 서버가 서버 **schannel** 매개 변수의 기본값(**yes**)을 사용하는지 확인합니다. 확인하려면 **testparm -v | grep 'server schannel'** 명령을 사용합니다. 자세한 내용은 CVE-2020-1472 에서 참조하십시오.
- Samba "전체 링크" 기능이 VFS 모듈로 변환되었습니다.
- PDC 또는 BDC로 Samba를 실행하는 것은 더 이상 사용되지 않습니다.
- 이제 **FIPS** 모드가 활성화된 **RHEL**에서 **Samba**를 사용할 수 있습니다. **FIPS** 모드의 제한으로 인해:
  - **RC4** 암호가 차단되었으므로 **NT LAN Manager(NTLM)** 인증을 사용할 수 없습니다.
  - 기본적으로 **FIPS** 모드에서 **Samba** 클라이언트 유틸리티는 **AES** 암호로 **Kerberos** 인증을 사용합니다.
  -

AES 암호화를 사용하는 Kerberos 인증이 포함된 AD(Active Directory) 또는 Red Hat IdM(Identity Management) 환경에서만 Samba를 도메인 구성원으로 사용할 수 있습니다. Red Hat은 백그라운드에서 사용하는 기본 도메인 컨트롤러(PDC) 기능을 계속 지원합니다.

- 이제 서버 메시지 블록 버전 1(SMB1) 프로토콜에서만 사용할 수 있는 안전하지 않은 인증 방법에 대해 다음 매개 변수가 더 이상 사용되지 않습니다.
  - 클라이언트 일반 텍스트 인증
  - 클라이언트 NTLMv2 인증
  - 클라이언트 lanman 인증
  - 클라이언트 사용 spnego
- Samba와 함께 사용할 때 GlusterFS write-behind 성능 변환기에 문제가 해결되어 데이터 손상을 방지합니다.
- 최소 런타임 지원은 이제 Python 3.6입니다.
- 더 이상 사용되지 않는 ldap ssl ad 매개변수가 제거되었습니다.

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

주요 변경 사항에 대한 자세한 내용은 업데이트하기 전에 업스트림 릴리스 노트 를 참조하십시오.

(BZ#1878109)

SSSD를 사용한 암호 없는 sudo 인증을 위한 새로운 GSSAPI PAM 모듈

새로운 pam_ss_gss.so PAM(Pluggable Authentication Module)을 사용하여 SSSD(System

Security Services Daemon)를 구성하여 사용자를 **GSSAPI(Generic Security Service Application Programming Interface)**를 사용하여 **PAM** 서비스에 인증할 수 있습니다.

예를 들어 이 모듈을 사용하여 **Kerberos** 티켓과 암호 없는 **sudo** 인증을 사용할 수 있습니다. **IdM** 환경의 추가 보안을 위해 스마트 카드 또는 일회성 암호로 인증된 사용자와 같이 티켓의 특정 인증 표시기가 있는 사용자에게만 액세스 권한을 부여하도록 **SSSD**를 구성할 수 있습니다.

자세한 내용은 **IdM** 클라이언트에서 **IdM** 사용자에게 **sudo** 액세스 부여를 참조하십시오.

(BZ#1893698)

Directory Server 기반 버전 **1.4.3.16**

389-ds-base 패키지가 업스트림 버전 **1.4.3.16**으로 업그레이드되어 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항의 전체 목록은 업데이트하기 전에 업스트림 릴리스 노트를 읽어보십시오.

- **https://www.port389.org/docs/389ds/releases/release-1-4-3-16.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-15.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-14.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-13.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-12.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-11.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-10.html**
- **https://www.port389.org/docs/389ds/releases/release-1-4-3-9.html**

(BZ#1862529)

Directory Server는 이제 RESULT 항목에 작업 및 작업 시간을 기록합니다.

이번 업데이트를 통해 **Directory Server**는 **/var/log/dirsrv/slapd-<instance_name>/access** 파일의 **RESULT** 항목에 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 로그 참조 섹션을 참조하십시오.

(BZ#1850275)

Directory Server는 인덱싱되지 않은 내부 검색을 거부할 수 있음

이번 개선된 기능에서는 **nsslapd-require-internalop-index** 매개변수를 **cn=*<database_name>*,cn=ldbm** 데이터베이스,**cn=plugins,cn=config** 항목에 추가하여 내부 **unindexed** 검색을 거부합니다. 플러그인은 데이터를 수정하면 데이터베이스에 쓰기 잠금이 있습니다. 대규모 데이터베이스에서 플러그인이 인덱싱되지 않은 검색을 실행하는 경우 플러그인은 모든 데이터베이스 잠금을 사용하여 데이터베이스가 손상되거나 서버가 응답하지 않게 되는 경우가 있습니다. 이 문제를 방지하려면 **nsslapd-require-internalop-index** 매개변수를 활성화하여 내부 인덱싱되지 않은 검색을 거부할 수 있습니다.

(BZ#1851975)

4.14. 데스크탑

GNOME에서 응답하지 않는 애플리케이션 시간 초과를 구성할 수 있습니다.

GNOME은 애플리케이션이 응답하지 않는지 감지하기 위해 모든 애플리케이션에 주기적으로 신호를 보냅니다. **GNOME**이 응답하지 않는 애플리케이션을 감지하면 애플리케이션 창에 대한 대화 상자가 표시

되고 애플리케이션을 중지하거나 대기할지 여부를 묻는 대화 상자가 표시됩니다.

특정 애플리케이션은 시간 내에 신호에 응답할 수 없습니다. 그 결과 애플리케이션이 제대로 작동하는 경우에도 GNOME에 대화 상자가 표시됩니다.

이번 업데이트를 통해 신호 간 시간을 구성할 수 있습니다. 설정은 org.gnome.mutter.check-alive-timeout GSettings 키에 저장됩니다. 응답하지 않는 애플리케이션 탐지를 완전히 비활성화하려면 키를 0으로 설정합니다.

GSettings 키 구성에 대한 자세한 내용은 명령줄에서 GSettings 키 작업을 참조하십시오.

(BZ#1886034)

4.15. 그래픽 인프라

Intel Tiger Lake GPU 지원

이 릴리스에는 통합된 그래픽으로 Intel Tiger Lake CPU microarchitecture에 대한 지원이 추가되었습니다. 여기에는 다음과 같은 CPU 모델과 함께 발견된 Intel✓ Graphics 및 Intel Xe 통합 GPU가 포함됩니다.

- Intel Core i7-1160G7
- Intel Core i7-1185G7
- Intel Core i7-1165G7
- Intel Core i7-1165G7
- Intel Core i7-1185G7E
- Intel Core i7-1185GRE

- **Intel Core i7-11375H**
- **Intel Core i7-11370H**
- **Intel Core i7-1180G7**
- **Intel Core i5-1130G7**
- **Intel Core i5-1135G7**
- **Intel Core i5-1135G7**
- **Intel Core i5-1145G7E**
- **Intel Core i5-1145GRE**
- **Intel Core i5-11300H**
- **Intel Core i5-1145G7**
- **Intel Core i5-1140G7**
- **Intel Core i3-1115G4**
- **Intel Core i3-1115G4**
- **Intel Core i3-1110G4**

- **Intel Core i3-1115GRE**
- **Intel Core i3-1115G4E**
- **Intel Core i3-1125G4**
- **Intel Core i3-1125G4**
- **Intel Core i3-1120G4**
- **Intel Pentium Gold 7505**
- **Intel Celeron 6305**
- **Intel Celeron 6305E**

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

(BZ#1882620)

11세대 코어 마이크로프로세서를 사용하는 Intel GPU 지원

이 릴리스에는 다음 CPU 모델에서 볼 수 있는 Xe gen 12 통합 그래픽이 포함된 11세대 코어 CPU 아키텍처(이전 명칭: Hadoop *Lake*)에 대한 지원이 추가되었습니다.

- **Intel Core i9-11900KF**
- **Intel Core i9-11900K**

- **Intel Core i9-11900**
- **Intel Core i9-11900F**
- **Intel Core i9-11900T**
- **Intel Core i7-11700K**
- **Intel Core i7-11700KF**
- **Intel Core i7-11700T**
- **Intel Core i7-11700**
- **Intel Core i7-11700F**
- **Intel Core i5-11500T**
- **Intel Core i5-11600**
- **Intel Core i5-11600K**
- **Intel Core i5-11600KF**
- **Intel Core i5-11500**
- **Intel Core i5-11600T**

- **Intel Core i5-11400**
- **Intel Core i5-11400F**
- **Intel Core i5-11400T**

(BZ#1784246, BZ#1784247, BZ#1937558)

NVIDIA Ampere가 지원

이번 릴리스에서는 **GA102** 또는 **GA104** 칩셋을 사용하는 **Nvidia Ampere GPU**에 대한 지원이 추가되었습니다. 여기에는 다음과 같은 **GPU** 모델이 포함됩니다.

- **redhat RTX 3060 Ti**
- 스키마 **RTX 3070**
- **GeForce RTX 3080**
- **GeForce RTX 3090**
- **RTX A4000**
- **RTX A5000**
- **RTX A6000**
- **NVIDIA A40**

노보 그래픽 드라이버는 아직 **Nvidia Ampere** 제품군으로 **3D** 가속화를 지원하지 않습니다.

(BZ#1916583)

다양한 업데이트된 그래픽 드라이버

다음 그래픽 드라이버가 최신 업스트림 버전으로 업데이트되었습니다.

- **Matrox mgag200** 드라이버
- **Aspeed ast** 드라이버

(JIRA:RHELPLAN-72994, BZ#1854354, BZ#1854367)

4.16. 웹 콘솔

필요한 재시작을 위해 Software Updates 페이지 검사

이번 업데이트를 통해 **RHEL** 웹 콘솔의 소프트웨어 업데이트 페이지에서 일부 서비스 또는 실행 중인 프로세스만 설치 후 효과적으로 업데이트할 수 있는지 확인합니다. 이 경우 시스템을 재부팅하지 않아도 됩니다.

(JIRA:RHELPLAN-59941)

웹 콘솔의 그래픽 성능 분석

이번 업데이트를 통해 시스템 그래프 페이지가 시스템의 성능을 분석하기 위한 새로운 전용 페이지로 교체되었습니다. 성능 지표를 보려면 **Overview** (개요) 페이지에서 **View Details**(세부 정보 및 기록 보기)를 클릭합니다. **Utilization Saturation(Utilization Saturation)** 및 **Errors(USE)** 방법을 기반으로 현재 지표 및 기록 이벤트를 표시합니다.

(JIRA:RHELPLAN-59938)

웹 콘솔의 SSH 키 설정 지원

이전에는 로그인하는 동안 **Reuse my password for remote connections**(원격 연결에 내 암호 재사

용)가 선택되었을 때 웹 콘솔에서 초기 로그인 암호를 사용하여 원격 호스트에 로그인할 수 있었습니다. 이 옵션은 제거되었으며 웹 콘솔 대신 원격 호스트에 자동으로 암호 없이 로그인할 사용자를 위해 SSH 키를 설정하는 데 도움이 됩니다.

자세한 내용은 웹 콘솔에서 원격 시스템 관리를 확인합니다.

(JIRA:RHELPLAN-59950)

4.17. RED HAT ENTERPRISE LINUX 시스템 역할

로깅 역할 구성에 추가된 RELP 보안 전송 지원

신뢰할 수 있는 이벤트 로깅 프로토콜인 RELP는 rsyslog 서버 간에 로그 메시지를 전달하고 받는 안전하고 안정적인 프로토콜입니다. 이 향상된 기능을 통해 rsyslog 서버가 RELP 프로토콜을 통해 로그 메시지를 전달하고 받을 수 있으므로, 관리자는 rsyslog 사용자의 높은 요구 사항을 갖춘 유용한 프로토콜인 RELP의 혜택을 누릴 수 있습니다.

(BZ#1889484)

SSH 클라이언트 RHEL 시스템 역할이 지원됨

이전에는 서버 및 클라이언트에 일관되고 안정적인 방식으로 RHEL SSH를 구성하는 벤더 지원 자동화 툴이 없었습니다. RHEL 시스템 역할을 사용하면 운영 체제 버전과 독립적으로 체계적이고 통합된 방식으로 SSH 클라이언트를 구성할 수 있습니다.

(BZ#1893712)

기존 RHEL 시스템 역할 형식에 대한 대안: Ansible 컬렉션

RHEL 8.4에서는 기존 RHEL 시스템 역할 형식에 대한 옵션으로 사용할 수 있는 컬렉션 형식으로 RHEL 시스템 역할이 도입되었습니다.

이번 업데이트에서는 네임스페이스와 컬렉션 이름으로 구성된 정규화된 컬렉션 이름(FCN)의 개념을 도입했습니다. 예를 들어 커널 역할의 정규화된 이름은 redhat.rhel_system_roles.kernel_settings입니다.

- 네임스페이스와 컬렉션 이름을 조합하면 오브젝트가 고유합니다.

- 네임스페이스와 컬렉션 이름을 결합하면 충돌 없이 컬렉션 및 네임스페이스 전반에서 오브젝트를 공유할 수 있습니다.

RPM 패키지를 사용하여 컬렉션을 설치합니다. python3-jmespath 가 플레이북을 실행하는 호스트에 설치되어 있는지 확인합니다.

```
# yum install rhel-system-roles
```

RPM 패키지에는 레거시 Ansible 역할 형식과 새 Ansible 컬렉션 형식의 역할이 모두 포함되어 있습니다. 예를 들어 네트워크 역할을 사용하려면 다음 단계를 수행합니다.

기존 형식:

```
---
- hosts: all
  roles:
rhel-system-roles.network
```

수집 형식:

```
---
- hosts: all
  roles:
redhat.rhel_system_roles.network
```

Automation Hub를 사용하고 Automation Hub에서 호스팅되는 System Roles Collection을 설치하려면 다음 명령을 입력합니다.

```
$ ansible-galaxy collection install redhat.rhel_system_roles
```

그런 다음 앞에서 설명한 대로 Collection 형식으로 역할을 사용할 수 있습니다. 이를 위해서는 Ansible Galaxy 대신 Automation Hub를 사용하도록 ansible-galaxy 명령으로 시스템을 구성해야 합니다. 자세한 내용은 Ansible Galaxy 대신 Automation Hub를 사용하도록 ansible-galaxy 클라이언트를 구성하는 방법을 참조하십시오.

(BZ#1893906)

메트릭 역할은 PCP를 통해 SQL 서버에 대한 메트릭 수집의 구성 및 활성화를 지원합니다.

메트릭 RHEL 시스템 역할은 이제 Performance Co-Pilot, pcp 를 사용하여 SQL Server, mssql 을 연결하는 기능을 제공합니다. SQL Server는 Microsoft의 범용 관계형 데이터베이스입니다. SQL Server는 실행 중에 있는 작업에 대한 내부 통계를 업데이트합니다. 이러한 통계는 SQL 쿼리를 사용하여 액세스할 수 있지만, 성능 분석 작업을 수행해야 하는 시스템 및 데이터베이스 관리자가 이러한 지표를 기록하고 보고할 수 있어야 합니다. 이 향상된 기능을 통해 사용자는 메트릭 RHEL 시스템 역할을 사용하여 mssql 메트릭에 대한 기록, 보고 및 시각화 기능을 제공하는 Performance Co-Pilot, pcp 로 SQL 서버, mssql 연결을 자동화할 수 있습니다.

(BZ#1893908)

Metrics RHEL 시스템 역할에서 사용할 수 있는 export-metric-data-to-elasticsearch 기능

Elasticsearch는 인기 있고 강력하며 확장 가능한 검색 엔진입니다. 이 향상된 기능을 통해 Metrics RHEL 시스템 역할에서 Elasticsearch로 지표 값을 내보내면 사용자가 그래픽 인터페이스, REST API를 포함한 Elasticsearch 인터페이스를 통해 지표에 액세스할 수 있습니다. 결과적으로 사용자는 이러한 Elasticsearch 인터페이스를 사용하여 성능 문제를 진단하고 용량 계획, 벤치마킹 등의 기타 성능 관련 작업을 지원할 수 있습니다.

(BZ#1895188)

SSHD RHEL 시스템 역할 지원

이전에는 서버 및 클라이언트에 일관되고 안정적인 방식으로 SSH RHEL 시스템 역할을 구성하는 벤더 지원 자동화 툴이 없었습니다. 이 향상된 기능을 통해 RHEL 시스템 역할을 사용하여 운영 체제 버전과 관계없이 체계적이고 통합된 방식으로 sshd 서버를 구성할 수 있습니다.

(BZ#1893696)

암호화 정책 RHEL 시스템 역할이 지원됨

이 향상된 기능을 통해 RHEL 8에는 시스템 전체 암호화 정책 관리를 위한 새로운 기능이 도입되었습니다. RHEL 시스템 역할을 사용하면 원하는 수의 RHEL 8 시스템에서 암호화 정책을 일관되고 쉽게 구성할 수 있습니다.

(BZ#1893699)

로깅 RHEL 시스템 역할에서 rsyslog 동작 지원

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

(BZ#1889893)

네트워킹 RHEL 시스템 역할이 ethtool 설정을 지원합니다.

이 향상된 기능을 통해 네트워킹 RHEL 시스템 역할을 사용하여 NetworkManager 연결의 ethtool 통합 설정을 구성할 수 있습니다. 인터럽트 결합 절차를 사용하는 경우 시스템은 네트워크 패킷을 수집하고 여러 패킷에 대한 단일 인터럽트를 생성합니다. 결과적으로 하나의 하드웨어 인터럽트가 있는 커널로 전송되는 데이터 양이 증가하여 인터럽트 로드가 줄어들고 처리량이 극대화됩니다.

(BZ#1893961)

4.18. 가상화

IBM Z 가상 머신은 최대 248개의 CPU를 실행할 수 있음

이전에는 DIAG318 이 활성화된 IBM Z(s390x) 가상 머신(VM)에서 사용할 수 있는 CPU 수는 240으로 제한되었습니다. 이제 Extended-Length SCCB를 사용하여 IBM Z VM은 최대 248개의 CPU를 실행할 수 있습니다.

(JIRA:RHELPLAN-44450)

HMAT가 RHEL KVM에서 지원

이번 업데이트를 통해 이제 RHEL KVM에서 ACPI 이기종 메모리 속성 테이블(HMAT)이 지원됩니다. ACPI HMAT는 메모리 측면 캐시 특성과 같은 메모리 속성과 SPA(System Physical Address) 메모리 범위와 관련된 대역폭 및 대기 시간 세부 정보에 대한 정보를 제공하여 메모리를 최적화합니다.

(JIRA:RHELPLAN-37817)

가상 머신에서 Intel Atom P5000 프로세서의 기능을 사용할 수 있음

이제 virtualridge CPU 모델 이름을 VM(가상 머신)에 사용할 수 있습니다. Intel Atom P5000 프로세서가 있는 호스트에서 Hardware ridge 를 VM의 XML 구성의 CPU 유형으로 사용하여 이러한 프로세서의 새로운 기능을 VM에 노출합니다.

(JIRA:RHELPLAN-37579)

virtio-gpu 장치가 Windows 10 이상 버전의 가상 머신에서 더 효율적으로 작동

이번 업데이트에서는 **virtio-win** 드라이버를 확장하여 선택한 **Windows** 플랫폼에서 **virtio-gpu** 장치에 사용자 정의 드라이버를 제공합니다. 그 결과 **virtio-gpu** 장치는 이제 **Windows 10** 이상을 게스트 시스템으로 사용하는 가상 머신의 성능이 향상되었습니다. 또한 장치도 향후 개선 사항에서 **virtio-win** 에 이르기까지 이점을 얻을 수 있습니다.

(BZ#1861229)

3세대 AMD EPYC 프로세서 가상화 지원

이번 업데이트에서는 **RHEL 8**의 가상화에 **EPYC**라고도 하는 **3**세대 **AMD EPYC** 프로세서가 지원됩니다. 결과적으로 **RHEL 8**에서 호스팅되는 가상 머신은 이제 **EPYC-Milan CPU** 모델을 사용할 수 있으며 프로세서에서 제공하는 새로운 기능을 사용할 수 있습니다.

(BZ#1790620)

4.19. 클라우드 환경의 RHEL

골드 이미지 자동 AWS 등록

이번 업데이트를 통해 **Amazon Web Services** 및 **Microsoft Azure**에 대한 **RHEL 8.4** 이상의 골드 이미지는 사용자가 **RHSM(Red Hat Subscription Management)** 및 **Red Hat Insights**에 자동으로 등록하도록 구성할 수 있습니다. 따라서 골드 이미지에서 생성된 다수의 가상 시스템을 더 빠르고 쉽게 구성할 수 있습니다.

그러나 **RHSM**에서 제공하는 리포지토리를 사용해야 하는 경우 **/etc/rhsm/rhsm.conf** 의 **manage_repos** 옵션이 **1** 로 설정되어 있는지 확인합니다. 자세한 내용은 Red Hat KnowledgeBase 를 참조하십시오.

(BZ#1905398, BZ#1932804)

Cloud-init 은 IBM Cloud의 Power Systems Virtual Server에서 지원

이번 업데이트를 통해 **cloud-init** 유틸리티를 사용하여 **IBM Power Systems** 호스트에서 호스팅되고 **IBM Cloud Virtual Server** 서비스에서 실행되는 **RHEL 8** 가상 시스템을 구성할 수 있습니다.

(BZ#1886430)

4.20. 지원 관련 기능

SOS 버전 4.0으로 업데이트

sos 패키지가 버전 4.0으로 업그레이드되었습니다. 이 주요 버전 릴리스에는 여러 가지 새로운 기능 및 변경 사항이 포함되어 있습니다.

주요 변경 사항은 다음과 같습니다.

- 새 sos 바이너리가 유틸리티의 기본 진입점으로 이전 sosreport 바이너리를 대체했습니다.
- 이제 SOS 보고서가 sosreport tarballs를 생성하는 데 사용됩니다. sosreport 바이너리는 리디렉션 지점으로 유지 관리되며 이제 sos 보고서를 호출합니다.
- /etc/sos.conf 파일이 /etc/sos/sos.conf 로 이동되었으며 레이아웃이 다음과 같이 변경되었습니다.
  - [general] 섹션의 이름이 [global]로 변경되었으며, 모든 sos 명령 및 하위 명령에 사용할 수 있는 옵션을 지정하는 데 사용할 수 있습니다.
  - [tunables] 섹션의 이름이 [plugin_options] 로 변경되었습니다.
  - 각 sos 구성 요소, 보고,수집 및 정리 에는 전용 섹션이 있습니다. 예를 들어, sos는 보고서에서 글로벌 및 보고서에서 옵션을 로드합니다.
- SOS는 이제 Python3 전용 유틸리티입니다. Python2는 더 이상 모든 용량에서 지원되지 않습니다.

SOS 수집

SOS는 공식적으로 sos-collector 유틸리티를 기본 sos 프로젝트에 제공하고 여러 노드에서 동시에 sosreport를 수집하는 데 사용됩니다. sos-collector 바이너리는 리디렉션 지점으로 유지 관리되며 sos collect 를 호출합니다. 독립 실행형 sos-collector 프로젝트는 더 이상 독립적으로 개발되지 않습니다. sos 수집에 대한 개선 사항은 다음과 같습니다.

- 정책이 *정의된* 모든 배포에서 보고서 를 지원하는 모든 배포에서 **SOS** 수집이 지원됩니다.

- **--insecure-sudo** 옵션의 이름이 **--nopasswd-sudo** 로 변경되었습니다.

- 노드 수에 동시에 연결하는 데 사용된 **--threads** 옵션의 이름이 **--jobs**로 변경되었습니다.

sos clean

SOS는 공식적으로 **sos cleaner** 유틸리티의 기능을 기본 **sos** 프로젝트에 제공합니다. 이 하위 명령은 **IP** 주소, 도메인 이름 및 사용자 제공 키워드 정리와 같은 보고서에서 추가 데이터 난독화를 수행합니다.

참고: **--clean** 옵션을 **sos report** 또는 **sos collect** 명령과 함께 사용하면 **sos clean** 이 생성 중인 보고서에 적용됩니다. 따라서 보고서를 생성할 필요가 없으며 이후에는 정리된 기능을 적용할 필요가 없습니다.

sos clean 의 주요 개선 사항은 다음과 같습니다.

- **IPv4** 주소 난독화 지원. 이렇게 하면 검색된 주소 간에 토폴로지 관계를 유지하려고 합니다.

- 호스트 이름 및 도메인 이름 난독화 지원.

- 사용자 제공 키워드 난독화 지원.

- **sos report** 명령에 사용된 **--clean** 또는 **--mask** 플래그는 생성되는 보고서를 어렵게 만듭니다. 또는 다음 명령은 기존 보고서를 난독화합니다.

```
[user@server1 ~]$ sudo sos (clean|mask) $archive
```

전자를 사용하면 난독화된 보고서 아카이브가 **1**개 생성되는 반면, 후자의 경우 두 개의 파일, 즉 난독화된 아카이브와 비공용되지 않은 원본이 생성됩니다.

이 릴리스에 포함된 변경 사항에 대한 전체 내용은 sos-4.0을 참조하십시오.

(BZ#1966838)

4.21. 컨테이너

Podman에서 Docker용으로 작성된 볼륨 플러그인 지원

Podman에서 Docker 볼륨 플러그인을 지원합니다. 공급업체 및 커뮤니티 구성원이 작성한 이러한 볼륨 플러그인 또는 드라이버는 Podman에서 컨테이너 볼륨을 생성하고 관리하는 데 사용할 수 있습니다.

podman volume create 명령은 이제 지정된 이름의 볼륨 플러그인을 사용하여 볼륨 생성을 지원합니다. 볼륨 플러그인은 container. conf 구성 파일의 [engine.volume_plugins] 섹션에 정의해야 합니다.

예제:

```
[engine.volume_plugins]
testvol = "/run/docker/plugins/testvol.sock"
```

여기서 testvol 은 플러그 인의 이름이고 /run/docker/plugins/testvol.sock 은 플러그인 소켓 경로입니다.

podman volume create --driver testvol을 사용하여 testvol 플러그인을 사용하여 볼륨을 만들 수 있습니다.

(BZ#1734854)

ubi-micro 컨테이너 이미지를 사용할 수 있습니다.

registry.redhat.io/ubi8/ubi-micro 컨테이너 이미지는 기본 호스트에서 패키지 관리자를 사용하여 일반적으로 Podman과 함께 Buildah 또는 다단계 빌드를 사용하여 패키지를 설치하는 최소 기본 이미지입니다. 패키지 관리자 및 모든 종속성을 제외하고 이미지의 보안 수준이 높아집니다.

(JIRA:RHELPLAN-56664)

컨테이너 이미지 자동 업데이트 지원을 사용할 수 있습니다.

이번 개선된 기능을 통해 사용자는 **podman auto-update** 명령을 사용하여 자동 업데이트 정책에 따라 컨테이너를 자동 업데이트할 수 있습니다. 이미지가 업데이트되었는지 확인하려면 컨테이너에 지정된 **"io.containers.autoupdate=image"** 레이블이 지정되어 있어야 합니다. **Podman**이 있으면 **Podman**이 새 이미지를 가져와서 컨테이너를 실행하는 **systemd** 장치를 다시 시작합니다. **podman auto-update** 명령은 **systemd**를 사용하며 컨테이너를 생성하려면 완전히 지정된 이미지 이름이 필요합니다.

(JIRA:RHELPLAN-56661)

Podman에서 보안 단축 이름 지원

이미지의 단축 이름 별칭은 이제 **[aliases]** 테이블의 **registries.conf** 파일에서 구성할 수 있습니다. 짧은 이름 모드는 다음과 같습니다.

- 강제: 이미지를 가져오는 동안 일치하는 별칭을 찾을 수 없는 경우 **Podman**은 사용자에게 정규화되지 않은 검색 레지스트리 중 하나를 선택하라는 메시지를 표시합니다. 선택한 이미지를 성공적으로 가져오면 **Podman**은 사용자에게 **$HOME/.config/containers/short-name-aliases.conf** 파일에 새 단축 이름 별칭을 자동으로 기록합니다. 사용자에게 메시지가 표시될 수 없는 경우(예: **stdin** 또는 **stdout**은 **TTY**가 아님) **Podman**이 실패합니다. 동일한 별칭을 지정하는 경우 **short-name-aliases .conf** 파일이 **registries.conf** 파일보다 우선합니다.
- 허용: 강제 모드와 유사하지만 사용자에게 메시지가 표시될 수 없는 경우 실패하지는 않습니다. 대신 **Podman**은 지정된 순서로 모든 정규화되지 않은 레지스트리를 검색합니다. 별칭은 기록되지 않습니다.

예제:

```
unqualified-search-registries=[“registry.fedoraproject.org”, “quay.io”]

[aliases]

"fedora"="registry.fedoraproject.org/fedora"
```

(JIRA:RHELPLAN-39843)

container-tools:3.0 stable 스트림을 사용할 수 있습니다

Podman, Buildah, Skopeo 및 **runc** 툴이 포함된 **container-tools:3.0 stable** 모듈 스트림을 사용할 수 있습니다. 이번 업데이트에서는 이전 버전에 대한 버그 수정 및 개선 사항을 제공합니다.

이전 스트림에서 업그레이드하는 방법은 이후 스트림으로 전환을 참조하십시오.

(JIRA:RHELPLAN-56782)

5장. 외부 커널 매개변수로 중요한 변경

이 장에서는 시스템 관리자에게 **Red Hat Enterprise Linux 8.4**와 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.

5.1. 새 커널 매개변수

bgrt_disable = [ACPI, X86]

이 매개 변수는 **OEM(Original Equipment Manufacturer)** 로고를 깜빡이는 것을 방지하기 위해 **BGRT(부팅 그래픽 리소스 테이블)**를 비활성화합니다.

radix_hcall_invalidate = on [PPC/PSERIES]

이 매개 변수는 **Radix GTSE** 기능을 비활성화하고 **TLB(Translation Lookaside Buffer)** 무효화를 위해 **hcall**을 사용합니다.

disable_tlbie = [PPC]

이 매개 변수는 **TLBIE(Translation Look-Aside Buffer Invalidate Entry)** 명령을 비활성화합니다. 현재 **MMU(Hash Memory Management Unit)** 또는 일관성 있는 액셀러레이터는 **KVM**에서 작동하지 않습니다.

fw_devlink = [KNL]

이 매개 변수는 펌웨어를 스캔하여 소비자 및 공급업체 관계를 유추하여 소비자 및 공급업체 장치 간의 장치 링크를 생성합니다. 이 기능은 다음과 같은 작업의 순서가 적절히 수행되도록 드라이버가 모듈로 로드될 때 유용합니다.

- 장치 조사 (첫 번째로 공급, 소비자)
- 공급업체 부팅 상태 정리 (모든 소비자가 조사한 경우에만)
- 일시 중지, 재개 및 런타임 전원 관리 (PM) (소유업체 우선, 공급업체)

  형식: { off | 허용 | on | rpm }
- 꺼짐 - 펌웨어 정보에서 장치 링크를 생성하지 마십시오.
-

허용 - 펌웨어 정보에서 장치 링크를 생성하지만 부팅 상태 정리(sync_state() 호출)를 주문하는 경우에만 사용하십시오.

- 에서 - 펌웨어 정보에서 장치 링크를 생성하고 이를 사용하여 프로브를 적용하고 순서를 일시 중단하거나 재개합니다.

- rpm - 와 유사하지만 런타임 PM을 주문하는 데에도 사용됩니다.

기본값은 허용 입니다. /proc/cmdline 파일에서 구성된 값을 확인할 수 있습니다.

init_on_alloc = [MM]

이 매개변수는 새로 할당된 페이지와 힙 오브젝트를 0으로 채웁니다.

형식: 0 | 1

기본적으로 kernel CONFIG_INIT_ON_ALLOC_DEFAULT_ON 구성으로 설정됩니다.

init_on_free = [MM]

이 매개변수는 사용 가능한 페이지와 힙 오브젝트를 0으로 채웁니다.

형식: 0 | 1

기본 설정 CONFIG_INIT_ON_FREE_DEFAULT_ON

nofsgsbase [X86]

이 매개변수는 FSGSBASE 지침을 비활성화합니다.

nosgx [X86-64,SGX]

이 매개 변수는 Intel SGX(Software Guard Extensions) 커널 지원을 비활성화합니다.

rcutree.rcu_min_cached_objs = [KNL]

하나의 CPU당 캐시 및 유지 관리되는 최소 오브젝트 수입니다. 오브젝트 크기는 PAGE_SIZE 와

동일합니다. 캐시를 사용하면 페이지 할당기로 인한 부담을 줄일 수 있습니다. 또한 전체 알고리즘이 메모리 부족 상태에서 더 잘 작동합니다.

rcuperf.kfree_rcu_test = [KNL]

이 매개변수는 **kfree_rcu()** 기능 플러딩의 성능을 측정하는 데 사용됩니다.

rcuperf.kfree_nthreads = [KNL]

kfree_rcu() 의 반복문을 실행하는 스레드 수입니다.

rcuperf.kfree_alloc_num = [KNL]

반복에서 수행된 할당 및 자유 수입니다.

rcuperf.kfree_loops = [KNL]

rcuperf.kfree_alloc_num 할당 및 자유를 수행하는 반복문 수.

rcupdate.rcu_cpu_stall_ftrace_dump = [KNL]

이 매개변수는 **RCU(Read-copy-update) CPU stall** 경고를 보고한 후 **ftrace** 버퍼를 덤프합니다.

nopvspin = [X86,KVM]

이 매개 변수는 **PV(**반가상화**)** 최적화를 사용하여 **qspinlock** 느린 경로를 비활성화합니다. 이렇게 하면 하이퍼바이저가 고정 경합 시 게스트를 '유동'할 수 있습니다.

5.2. 새로운 /PROC/SYS/USER 매개변수

max_time_namespaces

현재 사용자 네임스페이스의 모든 사용자가 생성할 수 있는 최대 시간 네임스페이스 수입니다.

5.3. 새로운 /PROC/SYS/VM 매개변수

compaction_proactiveness

이 매개 변수는 커널이 메모리를 백그라운드에서 축소하는 방법을 적극적으로 결정합니다. 매개 변수는 범위 **[0, 100]**에서 값을 사용하고 기본값은 **0**입니다. 기본적으로 이 매개 변수를 비활성화하려는 동기는 메모리를 이동하기 위해 **500msec**마다 **kthread**에 의해 시스템의 현재 설정 및 예상 동작을 중단하지 않도록 하는 것이었습니다.

여러 다른 프로세스에 속하는 페이지가 이동되므로 압축은 시스템 전체에 미치는 영향이 거의 발생하지 않습니다. 이로 인해 애플리케이션의 대기 시간이 급증할 수도 있습니다. 커널은 사전 압축이 효과적이지 않음을 감지하면 **CPU** 사이클을 낭비하지 않도록 다양한 복구 방법을 사용합니다.

이 매개변수를 100과 같은 극단 값으로 설정할 때는 주의하십시오. 이로 인해 과도한 백그라운드 압축 활동이 발생할 수 있습니다.

watermark_boost_factor

이 매개변수는 메모리가 조각화될 때 회수 수준을 제어합니다. 다양한 이동성의 페이지가 페이지 블록 내에서 혼합되는 경우 회수될 영역의 높은 워터마크 비율을 정의합니다. 의 의도는 압축은 나중에 수행할 작업이 줄어들고 SLUB 할당, THP 및 hugetlbfs 페이지와 같은 미래의 높은 순서 할당의 성공 속도를 높이는 것입니다.

seal _scale_factor 매개변수와 관련하여 단위는 10,000의 배수로 되어 있습니다. 조각화로 인해 페이지 블록을 혼합하는 경우 높은 워터마크의 최대 150%를 확보할 수 있음을 의미합니다. 회수 수준은 최근 과거에 발생한 조각화 이벤트 수에 따라 결정됩니다. 이 값이 페이지 블록보다 작으면 페이지 가치가 있는 페이지 블록이 회수됩니다(예: 64비트 x86의 2MB). 상향수인 0은 이 기능을 비활성화합니다.

6장. 장치 드라이버

6.1. 새 드라이버

네트워크 드라이버

- Realtek 802.11ac 무선 8822b 드라이버 (rtw88_8822b.ko.xz)
- Realtek 802.11ac 무선 8822be 드라이버 (rtw88_8822be.ko.xz)
- Realtek 802.11ac 무선 8822c 드라이버 (rtw88_8822c.ko.xz)
- Realtek 802.11ac 무선 8822ce 드라이버 (rtw88_8822ce.ko.xz)
- Realtek 802.11ac 무선 코어 모듈 (rtw88_core.ko.xz)
- Realtek 802.11ac 무선 PCI 드라이버 (rtw88_pci.ko.xz)
- UDP 캡슐화된 트래픽용 인터페이스 드라이버 (bareudp.ko.xz)

그래픽 드라이버 및 기타 드라이버

- RegmapPodWire 모듈 (regmap-sdw.ko.xz)
- Intel® QuickAssist Technology (qat_4xxx.ko.xz)
- Intel® Data Accelerator Driver (idxd.ko.xz)
- Oracle VM VirtualBox 그래픽 카드 (vboxvideo.ko.xz)
- 로봇 게임 키보드에서 게임 키용 HID 드라이버 (hid-lg-g15.ko.xz)

- HWMON 인터페이스를 통해 RAPL MSR에서 AMD Energy 보고 드라이버(amd_.ko.xz)
- EFA(Elastic Fabric Adapter) (efa.ko.xz)
- AMD® PCI-E Non-Transparent Bridge Driver (ntb_hw_amd.ko.xz)
- PCIe NTB 성능 측정 도구 (ntb_perf.ko.xz)
- PCIe NTB 간단한 Pingpong 클라이언트 (ntb_pingpong.ko.xz)
- PCIe NTB 디버깅 툴 (ntb_tool.ko.xz)
- NTB를 통한 소프트웨어 대기열 쌍 전송 (ntb_transport.ko.xz)
- Intel Elkhart Lake PCH pinctrl/GPIO 드라이버(pinctrl-elkhartlake.ko.xz)
- Dell 플랫폼 설정 제어 인터페이스 (dell-wmi-sysman.ko.xz)
- DesignWare PWM Controller (pwm-dwc.ko.xz)
- PodWire 버스 (soundwire-bus.ko.xz)
- cadence macwire Library (soundwire-cadence.ko.xz)
- 액티브와이어 일반 대역폭 할당 (soundwire-generic-allocation.ko.xz)
- Intel VoIP Init Library (soundwire-intel.ko.xz)

- Apple "MFi"장치에 대한 빠른 제어 (apple-mfi-fastcharge.ko.xz)
- TI HD3SS3220 DRP 포트 컨트롤러 드라이버 (hd3ss3220.ko.xz)
- STMicro appliances ST160x Type-C 컨트롤러 드라이버(stusb160x.ko.xz)
- Nitro Enclaves Driver (nitro_enclaves.ko.xz)

6.2. 업데이트된 드라이버

그래픽 및 기타 드라이버 업데이트

- VMware SVGA 장치(vmwgfx.ko.xz)용 독립형 drm 드라이버가 버전 2.18.0.0으로 업데이트되었습니다.
- Cisco FCoE HBA Driver(fnic.ko.xz)가 1.6.0.53 버전으로 업데이트되었습니다.
- HP Smart Array Controller 버전 3.4.20-200-RH1(hpsa.ko.xz)의 드라이버가 버전 3.4.20-200-RH1로 업데이트되었습니다.
- Emulex LightPulse Fibre Channel SCSI 드라이버 12.8.0.5(lpfc.ko.xz)가 버전 0:12.8.0.5로 업데이트되었습니다.
- LSI MPT Fusion SAS 3.0 장치 드라이버(mpt3sas.ko.xz)가 버전 35.101.00.00으로 업데이트되었습니다.
- Qlogic 파이버 채널 HBA 드라이버(qla2xxx.ko.xz)가 버전 10.02.00.104-k로 업데이트되었습니다.
- SCSI 디버그 어댑터 드라이버(scsi_debug.ko.xz)가 0190 버전으로 업데이트되었습니다.
- Microsemi Smart Family Controller 버전 1.2.16-012(smartpqi.ko.xz)용 드라이버가 1.2.16-012 버전으로 업데이트되었습니다.

- **HPE 워치독 드라이버(hpwdt.ko.xz)가 버전 2.0.4로 업데이트되었습니다.**

7장. 버그 수정

이 부분에서는 사용자에게 중요한 영향을 미치는 Red Hat Enterprise Linux 8.4에서 수정된 버그에 대해 설명합니다.

7.1. 설치 프로그램 및 이미지 생성

Anaconda는 텍스트 모드에서 ldl 또는 포맷되지 않은 DASD 디스크에 대한 대화 상자 표시

이전에는 텍스트 모드로 설치하는 동안 Anaconda가 Linux 디스크 레이아웃(ldl) 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 Anaconda는 텍스트 모드에서 ldl 및 포맷되지 않은 DASD 디스크를 인식하고 사용자가 설치의 향후 사용률에 맞게 올바르게 포맷할 수 있는 대화 상자를 표시합니다.

(BZ#1874394)

InfiniBand 네트워크 인터페이스가 설치 프로그램 부팅 옵션을 사용하여 구성되었을 때 RHEL 설치 프로그램을 시작하지 못했습니다.

이전에는 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 못했습니다.

이 문제는 RHEL NetworkManager가 InfiniBand 모드에서 네트워크 인터페이스를 인식하지 못하고 대신 인터페이스에 이더넷 연결을 구성했기 때문에 발생했습니다.

그 결과 연결 활성화에 실패하고 초기 단계에서 InfiniBand 인터페이스를 통한 연결이 필요한 경우 RHEL 설치 프로그램이 설치를 시작하지 못했습니다.

이번 릴리스에서는 설치 프로그램이 설치 프로그램 부팅 옵션을 사용하여 RHEL 설치 초기 단계에서 구성하는 InfiniBand 네트워크 인터페이스를 성공적으로 활성화하고 설치가 성공적으로 완료된 것입니다.

(BZ#1890009)

Anaconda에서 자동 파티셔닝을 예약할 수 있습니다.

이전에는 LVM 유형 디스크의 자동 파티셔닝 중에 설치 프로그램에서 선택한 각 디스크에서 LVM PV의 파티션을 생성하려고 했습니다. 이러한 디스크에 이미 파티션 레이아웃이 있는 경우 오류 메시지로 자동 파티션 일정이 실패했을 수 있습니다.

이번 업데이트를 통해 문제가 해결되었습니다. 이제 설치 프로그램에서 자동 파티션을 예약할 수 있습니다.

(BZ#1642391)

Anaconda GUI를 사용하여 무선 네트워크 구성은 수정되었습니다.

이전에는 Anaconda GUI(그래픽 사용자 인터페이스)를 사용하는 동안 무선 네트워크를 구성하면 설치가 중단되었습니다.

이번 업데이트를 통해 문제가 해결되었습니다. Anaconda GUI를 사용하는 동안 설치 중에 무선 네트워크를 구성할 수 있습니다.

(BZ#1847681)

7.2. 소프트웨어 관리

%autopatch rpm 매크로에 대해 새로운 -m 및 -M 매개변수가 지원됩니다.

이번 업데이트를 통해 지정된 매개 변수가 있는 패치 범위만 적용하기 위해 %autopatch 매크로에 -m (min) 및 -M (max) 매개 변수가 추가되었습니다.

(BZ#1834931)

1.18 버전으로 다시 기반 팝업

팝업 패키지가 업스트림 버전 1.18로 업그레이드되어 이전 버전에 다음과 같은 주요 변경 사항이 추가되었습니다.

- 전체 코드베이스 정리 및 현대화.

- 별칭 exec 명령에 대한 권한을 삭제하지 못했습니다.

- 리소스 누수를 포함한 다양한 버그가 수정되었습니다.

(BZ#1843787)

7.3. 쉘 및 명령행 툴

snmpbulkget 은 존재하지 않는 **PID**에 대해 유효한 출력을 제공합니다.

이전에는 **the snmpbulkget** 명령이 존재하지 않는 **PID**에 유효한 출력을 제공하지 않았습니다. 결과적으로 이 명령은 결과를 찾을 수 없으므로 출력에서 실패했습니다.

이번 업데이트를 통해**snmpbulkget** 은 존재하지 않는 **PID**에 유효한 출력을 제공합니다.

(BZ#1817190)

CRON 명령은 이제 트리거 조건에 따라 이메일을 전송합니다.

이전에는**ReaR(Relax-and- Recovery)** 유틸리티가 잘못 구성되면 **CRON** 명령에서 이메일을 통해 관리자에게 전송된 오류 메시지를 트리거했습니다. 결과적으로 **ReaR** 에 구성을 수행하지 않은 경우에도 관리자가 이메일을 수신합니다.

이번 업데이트를 통해 **CRON** 명령이 수정되어 트리거 조건에 따라 이메일을 전송합니다.

(BZ#1729499)

이제 **NetBackup** 버전 **8.2**를 **ReaR** 의 백업 메커니즘으로 사용할 수 있습니다.

이전에는 **NetBackup**을 백업 방법으로 사용할 때 **Relax-and- recovery (ReaR)** 유틸리티에서 복구 시스템에서 **vxpbx_exchanged** 서비스를 시작하지 않았습니다. 결과적으로 **NetBackup 8.2**를 사용하여 복구 시스템의 백업에서 데이터를 복원하는 데 실패하고 **NetBackup** 서버에 다음과 같은 오류 메시지가 기록되었습니다.

오류 **bpbrm (pid=...) client Info tar (pid=...에서 cmd)**를 실행할 수 없습니다.) **done.** 상태**: 25: socket Error bpbrm (pid=...)** 클라이언트 복원 **EXIT STATUS 25:** 소켓에 연결할 수 없음

이번 업데이트를 통해 ReaR 은 vxpbx_exchanged 서비스와 관련 필수 파일을 복구 시스템에 추가하고 복구 시스템이 시작될 때 서비스를 시작합니다.

(BZ#1898080)

libvpd 가 2.2.8 버전으로 업데이트.

주요 변경 사항은 다음과 같습니다.

- sqlite 작업을 비동기 화하여 vpdupdate 의 성능을 개선했습니다.

(BZ#1844429)

대체 유틸리티로 LUKS2 암호화된 파티션을 사용하여 시스템을 복원

이전에는 Relax-and- recover (Rear)유틸리티로 백업하기 위해 시스템에 하나의 LUKS2 암호화된 파티션이 존재할 때 ReaR이 LUKS2 암호화 파티션을 지원하지 않는다는 사실을 사용자에게 알리지 않았습니다. 결과적으로 ReaR 유틸리티는 복원 단계에서 시스템의 원래 상태를 재생성할 수 없었습니다.

이번 업데이트를 통해 기본 LUKS2 구성, 오류 검사 및 개선된 출력 지원이 ReaR 유틸리티에 추가되었습니다. 이제 ReaR 유틸리티가 기본 LUKS2 암호화된 파티션을 사용하여 시스템을 복원하거나 사용자를 반대로 알립니다.

(BZ#1832394)

Texlive 가 이제 Poppler에서 올바르게 작동합니다.

이전에는 Poppler 유틸리티가 API 변경에 대한 업데이트를 실행했습니다. 결과적으로 이러한 API 변경으로 인해 Texlive 빌드가 작동하지 않았습니다. 이번 업데이트를 통해 Texlive 빌드가 새 Poppler 유틸리티로 올바르게 작동합니다.

(BZ#1889802)

7.4. 인프라 서비스

RPZ는 와일드카드 문자로 작동합니다.

이전에는 lib/dns/ rpz.c 파일의 dns_rpz _find_name 함수에서 동일한 접미사의 레코드가 있는 경우 와일드카드 문자를 고려하지 않았습니다. 결과적으로 와일드카드 문자를 포함하는 일부 레코드가 무시되었습니다. 이번 업데이트를 통해 dns_rpz_find_name 함수가 수정되어 와일드카드 문자를 고려합니다.

(BZ#1876492)

7.5. 보안

pkcs11에 대한 개선된 패딩

이전에는 pkcs11 토큰 레이블에 일부 스마트 카드의 추가 패딩이 있었습니다. 결과적으로 잘못된 패딩으로 인해 레이블 특성에 따라 일치하는 카드가 발생할 수 있었습니다. 이번 업데이트를 통해 패딩은 모든 카드와 정의된 PKCS #11 URI에 대해 수정되어 애플리케이션에서 일치해야 합니다.

(BZ#1877973)

해결된 sealert 연결 문제 처리

이전에는 setroubleshoot 데몬이 충돌하면 sealert 프로세스가 응답하지 않을 수 있었습니다. 그 결과 GUI는 분석을 표시하지 않고 응답하지 않아 명령줄 툴에서 출력을 출력하지 않고 종료될 때까지 계속 실행되게 되었습니다. 이번 업데이트에서는 sealert 와 setroubleshootd 간의 연결 문제 처리가 개선되었습니다. 이제 sealert 에서 setroubleshoot 데몬이 충돌하는 경우 오류 메시지를 보고하고 종료합니다.

(BZ#1875290)

setroubleshoot를 통한 감사 레코드 분석 최적화

이전에는 setroubleshoot-3.3.23-1 에 도입된 새로운 기능이 성능에 부정적인 영향을 미쳐 AVC 분석이 이전보다 최대 8배 느렸습니다. 이번 업데이트에서는 AVC 분석 시간을 크게 줄이는 최적화를 제공합니다.

(BZ#1794807)

고정 SELinux 정책 인터페이스 구문 분석기

이전 버전에서는 정책 인터페이스 구문 분석기로 인해 인터페이스 파일에 ifndef 블록이 포함된 사용자 지정 정책을 설치할 때 구문 오류 메시지가 표시되었습니다. 이번 업데이트에서는 인터페이스 파일 구

문 분석이 개선되어 이 문제가 해결됩니다.

(BZ#1868717)

레이블 지정 오류 시 **setfiles** 가 중지되지 않음

이전에는 파일의 레이블을 다시 지정하지 않을 때마다 **setfiles** 유틸리티가 중지되었습니다. 그 결과 잘못 레이블된 파일이 대상 디렉토리에 남아 있었습니다. 이번 업데이트를 통해 **setfiles** 는 레이블을 다시 지정할 수 없는 파일을 건너뛰므로 **setfiles** 는 대상 디렉터리의 모든 파일을 처리합니다.

(BZ#1926386)

정전 시 **SELinux** 정책 저장소 재구축이 강화되었습니다.

이전에는 캐싱을 작성하여 **SELinux-policy** 재빌드가 전원 오류로 인해 문제가 발생하지 않았습니다. 결과적으로 정책을 다시 빌드하는 동안 정전 후 **SELinux** 정책 저장소가 손상될 수 있습니다. 이번 업데이트를 통해 **libsemanage** 라이브러리는 메타데이터에 보류 중인 모든 수정 사항을 사용하고 정책 저장소가 포함된 파일 시스템에 캐시된 파일 데이터를 사용하기 전에 씁니다. 결과적으로 정책 저장소가 전력 실패 및 기타 중단에 더 취약해졌습니다.

(BZ#1913224)

libselinux 에서 **SELinux** 사용자의 기본 컨텍스트를 올바르게 결정합니다.

이전에는 더 이상 사용되지 않는 **security_compute_user()** 함수를 사용하기 때문에 **libselinux** 라이브러리에서 일부 시스템에서 **SELinux** 사용자의 기본 컨텍스트를 확인하지 못했습니다. 결과적으로 복잡한 보안 정책이 있는 시스템에서 일부 시스템 서비스를 사용할 수 없었습니다. 이번 업데이트를 통해 **libselinux** 에서 더 이상 **security_compute_user()** 를 사용하지 않고 정책 복잡성과 관계없이 **SELinux** 사용자의 기본 컨텍스트를 적절하게 결정합니다.

(BZ#1879368)

rsync 모드의 **Geo-replication**이 **SELinux**로 인해 더 이상 실패하지 않음

이전에는 **SELinux** 정책에서 **rsync_t** 에서 실행되는 프로세스에서 **security.trusted** 확장 속성의 값을 설정하지 못했습니다. 그 결과 **RHGS(Red Hat Gluster Storage)**의 **geo-replication**이 실패했습니다. 이번 업데이트에는 **rsync_ t** 프로세스에서 **security.trusted** 를 설정할 수 있는 새로운 **SELinux** 부울 **rsync_ sys_admin** 이 포함되어 있습니다. 결과적으로 **rsync_sys_admin** 부울이 활성화된 경우 **rsync** 는 **security.trusted** 확장 속성을 설정할 수 있으며 **geo-replication**은 더 이상 실패하지 않습니다.

(BZ#1889673)

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

이전에는 RAM이 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 RAM이 부족한 시스템에서 더 이상 메모리가 부족하지 않습니다(예: GUI 및 Workstation 을 사용한 패키지 그룹 서버).

(BZ#1824152)

FAT가 있는 CIS에서 조정된 시스템은 더 이상 부팅 시 실패하지 않습니다

이전에는 SCAP 보안 가이드(SSG)의 CIS(Center for Internet Security Guide) 프로필에 FAT 파일 시스템 액세스를 담당하는 커널 모듈 로드를 비활성화하는 규칙이 포함되어 있었습니다. 결과적으로 SSG가 이 규칙을 수정하면 시스템이 ESP(EFI 시스템 파티션)를 포함하여 FAT12, FAT16 및 FAT32 파일 시스템으로 포맷된 파티션에 액세스할 수 없었습니다. 이로 인해 시스템이 부팅되지 않았습니다. 이번 업데이트를 통해 프로필에서 규칙이 제거되었습니다. 결과적으로 이러한 파일 시스템을 사용하는 시스템은 더 이상 부팅되지 않습니다.

(BZ#1927019)

OVAL 검사는 GPFS를 원격로 간주합니다.

이전에는 OpenSCAP 스캐너가 마운트된 GPG(일반 병렬 파일 시스템)를 원격 파일 시스템(FS)으로 식별하지 않았습니다. 그 결과 OpenSCAP은 로컬 시스템에만 적용된 OVAL 검사를 위해 GPFS를 스캔했습니다. 이로 인해 스캐너가 리소스가 부족하여 검사를 완료하지 못하는 경우가 있었습니다. 이번 업데이트를 통해 GPFS가 원격 FS 목록에 포함되었습니다. 결과적으로 OVAL 검사는 GPFS를 원격 FS로 올바르게 고려하고 검사가 더 빠릅니다.

(BZ#1840579)

fapolicyd-selinux SELinux 정책에서 모든 파일 유형을 지원합니다.

이전에는 fapolicyd-selinux SELinux 정책에서 모든 파일 유형을 다루지 않았습니다. 결과적으로 fapolicyd 서비스는 sysfs 와 같은 모니터링되지 않은 위치에 있는 파일에 액세스할 수 없었습니다. 이번 업데이트를 통해 fapolicyd 서비스는 모든 파일 시스템 유형을 대상으로 하며 분석합니다.

(BZ#1940289)

fapolicyd 가 더 이상 **RHEL** 업데이트를 금지하지 않음

업데이트가 실행 중인 애플리케이션의 바이너리를 교체하면 커널은 (삭제된) 접미사를 추가하여 메모리의 애플리케이션 바이너리 경로를 수정합니다. 이전에는 **fapolicyd** 파일 액세스 정책 데몬이 애플리케이션을 신뢰할 수 없는 것으로 처리했습니다. 결과적으로 **fapolicyd** 는 이러한 애플리케이션이 다른 파일을 열고 실행하는 것을 방지했습니다. 이번 업데이트를 통해 **fapolicyd** 는 바이너리 경로의 접미사를 무시하므로 바이너리 데이터베이스와 일치할 수 있습니다. 결과적으로 **fapolicyd** 는 규칙을 올바르게 적용하고 업데이트 프로세스를 완료할 수 있습니다.

(BZ#1896875)

1.0.0-1로 업데이트하는 **usbguard**

usbguard 패키지가 업스트림 버전 **1.0.0-1**로 업데이트되었습니다. 이번 업데이트에서는 개선 사항 및 버그 수정을 제공합니다. 특히 다음과 같습니다.

- 안정적인 공용 **API**는 이전 버전과의 호환성을 보장합니다.
- 이제 **rules.d** 디렉터리 내의 규칙 파일이 영숫자순으로 로드됩니다.
- 단일 규칙으로 여러 장치의 정책을 변경할 수 없는 일부 사용 사례.
- 레이블별로 규칙을 필터링해도 더 이상 오류가 발생하지 않습니다.

(BZ#1887448)

usbguard에서 감사 메시지를 보낼 수 있음

서비스 강화의 일환으로 **CAP_AUDIT_WRITE** 기능이 누락된 동안 **usbguard.service** 의 기능이 제한되었습니다. 결과적으로 시스템 서비스로 실행 중인 **usbguard** 는 감사 이벤트를 보낼 수 없었습니다. 이번 업데이트를 통해 서비스 구성이 업데이트되어 **USBGuard**에서 감사 메시지를 보낼 수 있습니다.

(BZ#1940060)

tangd 에서 잘못된 요청을 올바르게 처리

이전에는 **tangd** 데몬에서 일부 잘못된 요청에 대해 오류 종료 코드를 반환했습니다. 그 결과

tangd.socket@.service 가 실패했습니다. 이로 인해 실패한 유닛 수가 증가하면 문제가 발생할 수 있습니다. 이번 업데이트를 통해 **tangd** 서버 자체에 문제가 있을 때만 오류 코드로 종료됩니다. 결과적으로 **tangd** 는 잘못된 요청을 올바르게 처리합니다.

(BZ#1828558)

7.6. 네트워킹

ipset 조회와 관련된 규칙을 사용하여 **RHEL 7**에서 **RHEL 8**로 **iptables** 규칙 세트를 마이그레이션해도 더 이상 실패하지 않습니다.

이전에는 **iptables** 규칙 세트에서 활성화된 카운터를 사용하여 **ipset** 명령을 참조하는 동안 모든 추가 제약 조건이 일치하는 경우에만 **ipset** 카운터가 업데이트되었습니다. 결과적으로 **ipset** 조회와 관련된 규칙은 **--match-set xxx src --bytes-gt 100**과 같이 **-m set** 과 관련된 규칙은 일치하지 않습니다. **ipset** 의 카운터가 추가되지 않기 때문입니다. 이번 업데이트를 통해 **ipset** 조회와 관련된 규칙을 사용하여 **iptables** 규칙 세트를 마이그레이션하는 것이 예상대로 작동합니다.

(BZ#1806882)

iptraf-ng 는 더 이상 원시 메모리 콘텐츠를 노출하지 않습니다

이전에는 **iptraf-ng** 의 필터에서 **%p** 를 설정하면 애플리케이션이 상태 표시줄에 원시 메모리 콘텐츠를 표시했습니다. 그 결과 **inessential** 정보가 표시되었습니다. 이번 업데이트를 통해 **iptraf-ng** 프로세스는 하단의 상태 표시줄에 원시 메모리 콘텐츠를 표시하지 않습니다.

(BZ#1842690)

Anaconda ip 부트 옵션에서 **DHCP**를 사용할 때 네트워크 액세스를 사용할 수 있습니다.

초기 **RAM** 디스크(**initrd**)는 **NetworkManager**를 사용하여 네트워킹을 관리합니다. 이전에는 **RHEL 8.3 ISO** 파일에서 제공하는 **dracut NetworkManager** 모듈에서 **Anaconda** 부팅 옵션의 첫 번째 필드가 항상 설정되었다고 잘못 가정했습니다. 결과적으로 **DHCP**를 사용하고 **ip=::<host_name>::dhcp** 를 설정하면 **NetworkManager**에서 **IP** 주소를 검색하지 않고 **Anaconda**에서 네트워크를 사용할 수 없었습니다. 이 문제는 해결되었습니다. 결과적으로 **RHEL 8.4 ISO**를 사용하여 언급된 시나리오에 호스트를 설치할 때 **Anaconda ip** 부트 옵션이 예상대로 작동합니다.

(BZ#1900260)

XDP 프로그램을 언로드해도 **nfp** 드라이버를 사용하는 **Netronome** 네트워크 카드에서 더 이상 실패하지 않습니다

이전에는 **Netronome** 네트워크 카드의 **nfp** 드라이버에 버그가 포함되어 있었습니다. 그 결과 이러한 카드를 사용한 경우 **XDP(eXpress Data Path)** 프로그램을 로드하지 못하고 **XDP _XDP_EXPECTED_FD** 기능을 사용하여 **XDP** 프로그램을 로드하지 못했습니다. 예를 들어, 이는 **libxdp** 라이브러리를 사용하여 로드된 **XDP** 프로그램에 영향을 미쳤습니다. 이 버그가 수정되었습니다. 결과적으로 **Netronome** 네트워크 카드에서 **XDP** 프로그램을 언로드하는 것이 예상대로 작동합니다.

(BZ#1880268)

NetworkManager에서 **DHCP**를 사용하여 호스트 이름 검색 및 모든 인터페이스에서 역방향 **DNS** 조회를 시도합니다.

이전 버전에서는 **/etc/hostname** 파일에 호스트 이름이 설정되지 않은 경우 **NetworkManager**는 지표 값이 가장 낮은 기본 경로가 있는 인터페이스를 통해서만 **DHCP** 또는 역방향 **DNS** 조회를 사용하여 호스트 이름을 가져오려고 했습니다. 결과적으로 기본 경로가 없는 네트워크에서 호스트 이름을 자동으로 할당할 수 없었습니다. 이번 업데이트에서는 동작이 변경되고 **NetworkManager**는 먼저 기본 경로 인터페이스를 사용하여 호스트 이름 검색을 시도합니다. 이 프로세스가 실패하면 **NetworkManager**는 사용 가능한 다른 인터페이스를 시도합니다. 결과적으로 **NetworkManager**는 **/etc/hostname** 에 설정되지 않은 경우 모든 인터페이스에서 **DHCP** 및 역방향 **DNS** 조회를 사용하여 호스트 이름을 검색합니다.

NetworkManager가 이전 동작을 사용하도록 구성하려면 다음을 수행합니다.

1. 다음 콘텐츠를 사용하여 **/etc/NetworkManager/conf.d/10-hostname.conf** 파일을 만듭니다.

```
[connection-hostname-only-from-default]
hostname.only-from-default=1
```

2. **NetworkManager** 서비스를 다시 로드합니다.

```
# systemctl reload NetworkManager
```

(BZ#1766944)

7.7. 커널

커널이 **IBM Z** 시스템에서 더 이상 오탐 경고를 반환하지 않음

이전에는 **RHEL 8**의 **IBM Z** 시스템에는 사용자가 액세스할 수 있도록 **ZONE_DMA** 메모리 영역에 허용된 항목이 누락되었습니다. 그 결과 커널은 다음과 같은 오탐(**false positive**) 경고를 반환했습니다.

```
...
```

```
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 표시되었습니다. 예를 들어, **debuginfo.sh** 스크립트를 실행합니다.

이번 업데이트에서는 **DMA(**직접 메모리 액세스**)** 버퍼에 플래그가 추가되어 사용자 공간 애플리케이션이 버퍼에 액세스할 수 있습니다.

따라서 설명된 시나리오에는 경고 메시지가 표시되지 않습니다.

(BZ#1660290)

RHEL 시스템은 **tboot GRUB** 항목에서 예상대로 부팅

이전에는 버전 **1.9.12-2**의 **tboot** 유틸리티로 인해 신뢰할 수 있는 플랫폼 모듈**(TPM) 2.0**이 활성화된 일부 **RHEL** 시스템이 기존 모드에서 부팅되지 않았습니다. 그 결과 **tboot Grand Unified Bootloader (GRUB)** 항목에서 부팅하려고 할 때 시스템이 중지되었습니다. 새로운 버전의 **RHEL 8** 및 **tboot** 유틸리티를 업데이트하면 문제가 해결되었으며 **RHEL** 시스템이 예상대로 부팅됩니다.

(BZ#1947839)

커널이 과부하 컨테이너 시나리오에서 메모리를 성공적으로 회수

컨테이너 내의 **I/O** 및 메모리에 볼륨이 제한된 경우 데이터 경쟁 조건으로 인해 메모리를 회수하는 커널 코드에 소프트 잠금이 발생했습니다. 데이터 경쟁은 다음과 같은 경우 발생하는 현상입니다.

- 최소한 두 개의 **CPU** 스레드가 동일한 데이터 집합을 동시에 수정하려고 합니다.
- 이 **CPU** 스레드 중 하나 이상이 데이터 세트에서 쓰기 작업을 시도합니다.

데이터 세트를 수정하기 위한 각 스레드의 정확한 타이밍에 따라 결과는 **A, B** 또는 **AB(interminate)**가 될 수 있습니다.

컨테이너의 메모리 부족 상태가 발생하면 여러 OOM(메모리 부족)이 종료되어 컨테이너가 잠기고 응답하지 않습니다. 이번 릴리스에서는 잠금 및 최적화를 위한 RHEL 커널 코드가 업데이트되었습니다. 결과적으로 커널이 더 이상 응답하지 않으며 데이터는 경쟁 조건에 포함되지 않습니다.

(BZ#1860031)

오프라인 메모리가 있는 RHEL 8은 더 이상 커널 패닉을 유발하지 않습니다

이전 버전에서는 시작되었지만 오프라인으로 표시된 메모리로 RHEL 8을 실행하면 경우에 따라 커널이 초기화되지 않은 메모리 페이지에 액세스하려고 했습니다. 그 결과 커널 패닉이 발생했습니다. 이번 업데이트에서는 유휴 페이지 추적에 대한 커널 메커니즘이 수정되어 문제가 발생하지 않습니다.

(BZ#1867490)

NUMA 시스템에 더 이상 예기치 않은 메모리 레이아웃이 발생하지 않음

이전에는 ARM64 및 S390 아키텍처에서 CONFIG_NODES_SPAN_OTHER_NODES 옵션이 누락되어 NUMA 시스템에서 예기치 않은 메모리 레이아웃을 경험했습니다. 그 결과 교차된 여러 NUMA 노드의 메모리 영역과 낮은 NUMA 노드의 교차 메모리 리전이 높은 NUMA에 추가되었습니다.

이번 업데이트를 통해 NUMA 시스템에 더 이상 메모리 레이아웃 문제가 발생하지 않습니다.

(BZ#1844157)

rngd 서비스가 poll() 시스템 호출에서 더 이상 사용 중이지 않음

버전 4.18.0-193.10부터 커널에 FIPS 모드용 새 커널 엔트로피 소스가 추가되었습니다. 그 결과, the rngd 서비스가 /dev/random 장치의 poll() 시스템 호출에 대해 사용량 대기했습니다. 이 경우 시스템이 FIPS 모드에 있을 때 100%의 CPU 시간이 사용되었습니다. 이번 업데이트를 통해 FIPS 모드에서 /dev/random 장치의 poll() 핸들러가 특히 /dev/random 장치에 대해 개발된 핸들러로 변경되었습니다. 그 결과 설명된 시나리오에서 the rngd 서비스가 더 이상 poll() 를 대기하지 않습니다.

(BZ#1884857)

SCHED_DEADLINE 스케줄러에 대한 HRTICK 지원이 활성화되어 있습니다.

이전에는 SCHED_DEADLINE 정책으로 구성된 특정 작업에 대해 높은 해상도 시스템 타이머(HRTICK)의 기능이 강제 적용되지 않았습니다. 결과적으로 SCHED_DEADLINE 스케줄러를 사용하는

이러한 작업에 대한 제한 메커니즘은 해당 작업에 대해 구성된 모든 런타임을 사용합니다. 이로 인해 실시간 환경에서 예기치 않은 대기 시간이 급증했습니다.

이번 업데이트에서는 높은 해상도 선점을 제공하는 **HRTICK** 기능을 활성화합니다. **HRTICK** 은 높은 해상도 타이머를 사용하여 작업이 런타임을 완료할 때 제한 메커니즘을 적용합니다. 따라서 설명된 시나리오에서는 이 문제가 더 이상 발생하지 않습니다.

(BZ#1885850)

tpm2-abrmd가 버전 **2.3.3.2**로 업데이트

tpm2-abrmd 패키지가 여러 버그 수정을 제공하는 버전 **2.3.3.2**로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 일시적인 처리 사용을 수정했습니다.
- **TPM** 명령 전송 인터페이스 **(TCTI)**에서 부분 읽기 수정
- 액세스 브로커 리팩터링

(BZ#1855177)

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)

7.8. 파일 시스템 및 스토리지

SMB 대상에 액세스해도 더 이상 **EREMOTE** 오류가 발생하지 않습니다.

이전에는 **cifsacl** 마운트 옵션을 사용하여 **RHEL SMB** 클라이언트에 **DFS** 네임스페이스를 마운트할 수 없으며 목록에 액세스할 수 없었습니다. 이번 업데이트에서는 커널이 **EREMOTE** 를 담당하도록 수정되어 **SMB** 공유에 액세스할 수 있게 되었습니다.

(BZ#1871246)

NFS readdir 기능의 성능 향상

이전 버전에서는 디렉터리를 나열하는 **NFS** 클라이언트 프로세스가 목록을 완료하는 데 시간이 오래 걸릴 수 있었습니다. 이번 업데이트를 통해 다음 시나리오에서 성능을 나열하는 **NFS** 클라이언트 디렉터리가 향상되었습니다.

- **100,000**개 이상의 파일이 있는 대규모 디렉터리 나열.
- 수정 중인 디렉토리 목록.

(BZ#1893882)

7.9. 고가용성 및 클러스터

corosync.conf 파일의 기본 토큰 시간 초과 값이 **1**초에서 **3**초로 증가했습니다.

이전에는 **corosync.conf** 파일의 **TOTEM** 토큰 시간 제한 값이 **1**초로 설정되었습니다. 이 짧은 시간 초과로 클러스터가 신속하게 반응하지만 네트워크 지연의 경우 조기 장애 조치가 발생할 수 있습니다. 빠른 응답과 광범위한 적용 가능성 간에 더 나은 장단점을 제공하기 위해 이제 기본값을 **3**초로 설정합니다. 토큰 시간 제한 값 수정에 대한 자세한 내용은 **RHEL 5, 6, 7** 또는 **8 High Availability** 클러스터에서 **totem** 토큰 시간 초과 값을 변경하는 방법을 참조하십시오. https://access.redhat.com/solutions/221263

(BZ#1870449)

7.10. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

perl-Time-HiRes 를 설치할 때 인플레이스 업그레이드 가능

이전에는 **RHEL 8**에 배포된 **perl-Time-HiRes** 패키지에 **RHEL 7** 버전의 패키지에 포함된 **epoch** 번호가 누락되었습니다. 그 결과 **perl-Time-HiRes** 가 설치되면 **RHEL 7**에서 **RHEL 8**로 인플레이스 업그레이

드를 수행할 수 없었습니다. 누락된 **epoch** 번호가 추가되고 **perl-Time-HiRes** 가 설치되면 인플레이스 업그레이드가 더 이상 실패하지 않습니다.

(BZ#1895852)

7.11. 컴파일러 및 개발 도구

glibc DNS 스텁 확인자는 동일한 트랜잭션 **ID**를 사용하여 병렬 쿼리를 올바르게 처리합니다.

이번 업데이트 이전에는 **GNU C** 라이브러리 **glibc** 의 **DNS** 스텁 확인자가 동일한 트랜잭션 **ID**를 사용하는 병렬 쿼리에 대한 응답을 올바르게 처리하지 않았습니다. 결과적으로 트랜잭션 **ID**가 같을 때 두 번째 병렬 응답이 쿼리와 일치하지 않아 시간 초과 및 재시도가 발생했습니다.

이번 업데이트를 통해 두 번째 병렬 응답이 이제 유효한 것으로 인식됩니다. 그 결과 **glibc DNS** 스텁 확인자는 인식되지 않는 응답으로 인해 과도한 시간 초과를 방지합니다.

(BZ#1868106)

이제 **fgetsgent()** 및 **fgetsgent_r()** 을 사용하여 구성 파일을 읽습니다.

/etc/gshadow 파일에서 구체적으로 구조화된 항목 또는 읽기 중에 파일 크기를 변경하면 **fgetsgent()** 및 **fgetsgent _r()** 함수에서 잘못된 포인터를 반환하는 경우가 있었습니다. 결과적으로 이러한 함수를 사용하여 **/etc/gshadow** 또는 **/etc/** 에 있는 기타 구성 파일을 읽는 애플리케이션이 분할 오류 오류로 실패했습니다. 이번 업데이트에서는 **fgetsgent()** 및 **fgetsgent_r()** 을 수정하여 구성 파일을 보다 강력하게 읽습니다. 결과적으로 애플리케이션에서 구성 파일을 읽을 수 있습니다.

(BZ#1871397)

glibc 문자열 기능은 이제 **AMD64** 및 **Intel 64** 프로세서의 시스템 캐시에 부정적인 영향을 미치지 않도록 합니다.

이전에는 문자열의 **glibc** 구현이 **64**비트 **AMD** 및 **Intel** 프로세서의 스레드에 사용할 수 있는 마지막 수준 캐시의 양을 잘못 예상했습니다. 결과적으로 대규모 버퍼에서 **memcpy** 함수를 호출하면 시스템의 전체 캐시 성능에 부정적인 영향을 미치거나 **memcpy** 시스템 호출 속도가 느렸습니다.

이번 업데이트를 통해 마지막 수준 캐시 크기가 더 이상 시스템에서 보고된 하드웨어 스레드 수를 사용하여 확장되지 않습니다. 결과적으로 문자열 기능이 이제 대규모 버퍼의 캐시를 바이패스하여 나머지 시스템 캐시에 부정적인 영향을 주지 않습니다.

(BZ#1880670)

glibc 동적 로더는 이제 libc.so.6의 특정 오류를 방지합니다.

이전에는 libc.so.6 공유 오브젝트가 기본 프로그램으로 실행된 경우(예: glibc 버전 정보 표시) glibc 동적 로더에서 LD_PRELOAD 환경 변수를 사용하여 로드된 오브젝트와 관련하여 libc.so.6 의 재배치를 올바르게 주문하지 않았습니다. 결과적으로 LD_PRELOAD 가 설정된 경우 libc.so.6 호출로 인해 libc.so.6 을 예기치 않게 종료하는 경우가 있었습니다. 이번 업데이트에서는 버그가 수정되어 동적 로더가 이제 libc.so.6 의 재배치를 올바르게 처리합니다. 따라서 설명된 문제가 더 이상 발생하지 않습니다.

(BZ#1882466)

glibc 동적 링커는 정적 스레드-로컬 스토리지 공간의 일부를 정적 TLS 할당으로 제한합니다.

이전에는 glibc 동적 링커에서 동적 TLS에 사용 가능한 모든 정적 스레드-로컬 스토리지(TLS) 공간을 먼저 제공했습니다. 결과적으로 동적 TLS 할당에서 사용 가능한 모든 정적 TLS 공간을 이미 사용했기 때문에 dlopen 함수를 사용하여 런타임에 추가 공유 오브젝트를 로드하지 못한 경우가 있었습니다. 이 문제는 특히 64비트 ARM 아키텍처 및 IBM Power Systems에서 발생했습니다.

이제 동적 링커가 정적 TLS 영역의 일부를 정적 TLS 할당으로 제한하고 이 공간을 동적 TLS 최적화에 사용하지 않습니다. 결과적으로 기본 설정을 사용하는 경우 더 많은 경우 dlopen 호출이 성공합니다. 기본 설정보다 할당된 정적 TLS가 필요한 애플리케이션에서는 새로운 glibc.rtld.optional_static_tls 튜닝 가능 항목을 사용할 수 있습니다.

(BZ#1871396)

glibc 동적 링커는 64비트 ARM 변형 호출 규칙에 대한 지연 바인딩을 비활성화합니다.

이전에는 glibc 동적 링커에서 64비트 ARM (AArch64) 변형 호출 규칙을 사용하여 함수의 지연 바인딩을 비활성화하지 않았습니다. 그 결과 동적 링커가 이러한 함수 호출에서 인수를 손상시켜 잘못된 결과 또는 프로세스 실패가 발생했습니다. 이번 업데이트를 통해 동적 링커는 설명된 시나리오에서 지연 바인딩을 비활성화하고 함수 인수가 올바르게 전달됩니다.

(BZ#1893662)

GCC 가 버전 8.4로 업데이트

GCC(GNU 컴파일러 컬렉션)는 이전 버전에 비해 여러 버그 수정을 제공하는 업스트림 버전 8.4로 변경되었습니다.

(BZ#1868446)

7.12. IDM (IDENTITY MANAGEMENT)

Samba 전체 링크 기능이 VFS 모듈로 변환되었습니다

이전에는 **wide link** 매개변수 가 **smbd** 서비스의 핵심 기능의 일부였습니다. 이 기능은 안전하지 않으므로 이름이 **widelinks** 인 별도의 **VFS**(가상 파일 시스템) 모듈로 이동되었습니다. 이전 버전과의 호환성을 위해 **RHEL 8.4**의 **Samba**는 광범위한 링크 **= yes** 가 구성에 설정된 공유에 대해 이 모듈을 자동으로 로드합니다.

중요: **Red Hat**은 안전하지 않은 링크 기능을 사용하지 않는 것이 좋습니다. 대신 바인드 마운트 를 사용하여 파일 계층 구조의 일부를 **Samba**에서 공유한 디렉토리에 마운트합니다. 바인드 마운트 구성에 대한 자세한 내용은 **mount (8)** 도움말 페이지의 **Bind** 마운트 작업 섹션을 참조하십시오.

광범위한 링크를 사용하여 마운트를 바인딩 하는 구성에서 전환하려면 다음을 수행합니다.

1. 공유 외부에 연결되는 모든 심볼릭 링크에 대해 링크를 바인드 마운트 로 바꿉니다. 자세한 내용은 **mount (8)** 도움말 페이지의 **Bind** 마운트 작업 섹션을 참조하십시오.

2. **/etc/samba/smb.conf** 파일에서 전체 링크 **= yes** 항목을 제거합니다.

3. **Samba**를 다시 로드합니다.

```
# smbcontrol all reload-config
```

(BZ#1925192)

네트워크 연결 유휴 시간 초과가 더 이상 리소스 오류로 보고되지 않음

이전 버전에서는 **Directory Server**에서 유휴 네트워크 연결 시간이 초과될 때 리소스를 일시적으로 사용할 수 없다는 잘못된 오류를 보고했습니다. 이번 업데이트를 통해 네트워크 연결 유휴 시간 제한에 대한 오류 매크로가 **EAGAIN** 에서 **ETIMEDOUT** 으로 변경되었습니다. 시간 초과를 설명하는 정확한 오류 메시지가 **Directory Server** 액세스 로그에 기록되었습니다.

(BZ#1859301)

PKI CA에 연결된 **PKI ACME** 응답자가 발행한 인증서가 더 이상 **OCSP** 검증에 실패하지 않습니다.

이전에는 **PKI CA**에서 제공한 기본 **ACME** 인증서 프로필에 실제 **OCSP** 서비스를 가리키지 않는 샘플 **OCSP URL**이 포함되어 있었습니다. 결과적으로 **PKI ACME** 응답자가 **PKI CA** 발행자를 사용하도록 구성된 경우 응답자가 발급한 인증서가 **OCSP** 검증에 실패할 수 있습니다. 이번 업데이트에서는 **ACME** 인증서 프로필에서 하드 코딩된 **URL**을 제거하고 사용자 지정하지 않은 경우 프로필 구성 파일을 수정하는 업그레이드 스크립트를 추가합니다.

(BZ#1868233)

7.13. 그래픽 인프라

디스플레이 백라이트가 최근 **Intel** 노트북에서 안정적으로 작동합니다.

Intel CPU가 있는 특정 최신 랩탑에는 디스플레이 백라이트를 제어하기 위한 전용 인터페이스가 필요합니다. 이전에는 **RHEL**에서 독점 인터페이스를 지원하지 않았으며 노트북에서는 신뢰할 수 없는 **VESA** 인터페이스를 사용하려고 했습니다. 결과적으로 **RHEL**은 해당 랩탑에서 디스플레이 백라이트를 제어할 수 없었습니다.

이번 업데이트를 통해 **RHEL**은 독점 백라이트 인터페이스에 대한 지원을 추가함으로써 이제 디스플레이 제어가 예상대로 작동합니다.

(BZ#1885406)

7.14. RED HAT ENTERPRISE LINUX 시스템 역할

tests_luks.yml 로 인해 **NVME** 디스크에서 파티션 케이스가 실패하지 않습니다

이전에는 **NVME** 디스크에서 **virtio/scsi** 에서 사용한 것과 다른 파티션 명명 규칙을 사용했으며 스토리지 역할이 이를 반영하지 않았습니다. 결과적으로 **NVME** 디스크로 **Storage** 역할을 실행하면 충돌이 발생했습니다. 이번 수정으로 **Storage RHEL** 시스템 역할은 이제 **blivet** 모듈에서 파티션 이름을 가져옵니다.

(BZ#1865990)

selinux RHEL 시스템 역할은 더 이상 **present**라는 변수를 사용하지 않습니다

이전에는 **selinux RHEL** 시스템 역할의 일부 작업이 있는 문자열을 사용하는 대신 **present** 라는 변수를 잘못 사용했습니다 . 그 결과 **selinux RHEL** 시스템 역할은 라는 변수가 없음을 알리는 오류를 반환했습니다 . 이번 업데이트에서는 이 문제가 해결되어 **present** 문자열을 사용하도록 해당 작업을 변경합니다. 결과적으로 **selinux RHEL** 시스템 역할이 예상대로 작동하며 오류 메시지가 표시되지 않습니다.

(BZ#1926947)

rsyslog-gnutls 패키지가 누락되면 로깅 출력이 더 이상 실패하지 않습니다.

로깅 **RHEL** 시스템 역할이 보안 원격 입력 및 보안 전달 출력을 제공하도록 구성된 경우 글로벌 **tls** **rsyslog-gnutls** 패키지가 필요합니다. 이전에는 이전 버전에서 **thel tls rsyslog-gnutls** 패키지가 무조건 설치되도록 변경되었습니다. 결과적으로 관리 노드에서 **tls rsyslog-gnutls** 패키지를 사용할 수 없는 경우 보안 원격 입력 및 보안 전달 출력이 구성의 일부로 포함되지 않은 경우에도 로깅 역할 구성이 실패했습니다. 이번 업데이트에서는 보안 연결이 구성되어 있는지 확인하고 글로벌 **tls logging_pki_files** 변수를 확인하여 문제를 해결합니다. **rsyslog-gnutls** 패키지는 보안 연결이 구성된 경우에만 설치됩니다. 결과적으로 기록 출력이 누락된 **rsyslog-gnutls** 패키지와 함께 실패하지 않으므로 **elasticsearch** 를 통합하도록 **Red Hat Enterprise Virtualization Hypervisor**를 구성하는 작업을 수행합니다.

(BZ#1927943)

7.15. 가상화

Windows Server 2019 호스트에서 **RHEL 8** 게스트 콘솔에 연결하는 속도가 더 이상 느려지지 않습니다.

이전에는 **Windows Server 2019** 호스트에서 다중 사용자 모드에서 **RHEL 8**을 게스트 운영 체제로 사용할 때 현재 게스트의 콘솔 출력에 연결하는 데 예상보다 훨씬 오래 걸렸습니다. 이번 업데이트에서는 **Hyper-V** 하이퍼바이저의 **VRAM** 성능이 개선되어 문제를 해결합니다.

(BZ#1908893)

QXL을 사용하여 **Wayland**를 사용하는 가상 머신의 여러 모니터를 표시할 수 있습니다

이전 버전에서는 **remote-viewer** 유틸리티를 사용하여 **Wayland** 디스플레이 서버를 사용하는 **VM**(가상 시스템)의 모니터를 두 개 이상 *표시하면 VM이 응답하지 않고 표시* 상태 메시지가 무기한 표시되었습니다. 기본 코드가 수정되어 설명된 문제가 발생하지 않습니다.

(BZ#1642887)

7.16. 클라우드 환경의 RHEL

GPU에 최적화된 **Azure** 인스턴스가 이제 **hibernation** 후 올바르게 작동합니다.

NV6과 같이 **GPU** 최적화 가상 머신(VM) 크기가 있는 **Microsoft Azure** 인스턴스에서 **RHEL 8**을 게스트 운영 체제로 실행하는 경우 **VM**을 **hibernation**에서 다시 시작하면 **VM**의 **GPU**가 잘못 작동했습니다. 이 문제가 발생하면 커널은 다음 메시지를 기록했습니다.

```
hv_irq_unmask() failed: 0x5
```

이번 업데이트를 통해 **Microsoft Azure**의 영향을 받는 **VM**이 다시 시작한 후 **GPU**를 올바르게 처리하므로 문제가 발생하지 않습니다.

(BZ#1846838)

가상 머신이 최대 절전 상태에서 다시 시작한 후 의도한 TX/RX 패킷 카운터가 증가합니다.

이전에는 **CX4 VF NIC**를 사용하여 **RHEL 8** 가상 머신이 **Microsoft Azure**의 최대 절전에서 다시 시작될 때 **TX/RX** 패킷 카운터가 증가를 중지했습니다. 이번 업데이트에서는 문제가 해결되고 의도한 대로 패킷 카운터가 증가합니다.

(BZ#1876527)

RHEL 8 가상 머신이 Azure의 hibernation에서 더 이상 다시 시작하지 못했습니다

이전에는 **SR-IOV** 가 활성화된 **RHEL 8** 가상 머신(VM)이 활성화된 경우 **VF**(가상 기능) **vmbus** 장치의 **GUID**가 최대 절전으로 변경되어 **Microsoft Azure**에 할당되었습니다. 결과적으로 **VM**이 다시 시작되면 다시 시작하고 예기치 않게 종료되지 않았습니다. 이번 업데이트를 통해 **vmbus** 장치 **VF**가 더 이상 변경되지 않고 **VM**이 최대 절전 모드로 다시 시작됩니다.

(BZ#1876519)

Hyper-V 및 KVM 게스트에서 중복 오류 메시지 제거

이전 버전에서는 **RHEL 8** 게스트 운영 체제가 **KVM** 또는 **Hyper-V** 가상 머신에서 실행될 때 **/var/log/messages** 파일에 다음과 같은 오류 메시지가 보고되었습니다.

```
serial8250: too much work for irq4
```

이는 중복 오류 메시지로, 이제 제거되었습니다.

문제에 대한 자세한 내용은 **Red Hat** 지식베이스 솔루션을 참조하십시오.

(BZ#1919745)

7.17. 컨테이너

Podman 시스템 연결은 기본 연결을 자동으로 추가합니다.

이전에는 **podman system connection add** 명령에서 첫 번째 연결이 자동으로 기본 연결로 설정되지 않았습니다. 결과적으로 **podman system connection default <connection_name>** 명령을 수동으로 실행하여 기본 연결을 설정해야 합니다. 이번 업데이트를 통해 **podman system connection add** 명령이 예상대로 작동합니다.

(BZ#1881894)

podman run --pid=host 는 rootless 모드에서 작동합니다.

이전에는 **podman run --pid=host** 명령을 **rootless** 사용자로 실행할 수 없었습니다. 그 결과 **OCI** 권한 오류가 발생했습니다.

```
$ podman run --rm --pid=host quay.io/libpod/testimage:20200929 cat -v /proc/self/attr/current

Error: container_linux.go:370: starting container process caused: process_linux.go:459: container init caused: readonly path /proc/bus: operation not permitted: OCI permission denied
```

이번 업데이트를 통해 문제가 해결되었습니다.

(BZ#1940854)

8장. 기술 프리뷰

다음 부분에서는 **Red Hat Enterprise Linux 8.4**에서 사용할 수 있는 모든 기술 프리뷰 목록을 제공합니다.

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

8.1. 설치 프로그램 및 이미지 생성

Red Hat 커넥터를 기술 프리뷰로 이용 가능

이제 **Red Hat Insights**와 서브스크립션 콘텐츠를 사용하는 단일 명령으로 **RHEL** 시스템에 연결할 수 있습니다. **Red Hat Enterprise Linux 8.4**에서 기술 프리뷰로 사용 가능한**rhc(Red Hat** 커넥터**) CLI**는 등록 환경을 통합하고 **Red Hat**에 연결하기 위해 **subscription-manager** 및 **insights-client** 명령을 별도로 실행할 필요가 없습니다. **Red Hat** 커넥터 및 스마트 관리 서브스크립션을 통해 클라우드에서 직접 문제를 해결할 수도 있습니다.

자세한 내용은 **Red Hat** 커넥터 구성 가이드를 참조하십시오.

(BZ#1957316)

8.2. 네트워킹

UDP 터널을 통해 MPLS 트래픽을 기술 프리뷰로 캡슐화하기 위한 bareudp 장치 지원 소개

bareudp 장치에 대한 지원은 이제 **ip link** 명령을 기술 프리뷰로 사용하여 사용할 수 있습니다. **bareudp** 장치는 **UDP** 터널 내의 유니캐스트 및 멀티캐스트 멀티캐스트 레이블 스위칭**(MPLS)** 및 **IPv4/IPv6**와 같은 다양한 **L3** 프로토콜을 사용하여 트래픽을 라우팅하는 **L3** 캡슐화 터널링을 지원합니다. 추가 필터 및 작업을 통해 **UDP**에서 **MPLS** 패킷 라우팅을 시작할 수 있습니다.

예를 들어 새 **bareudp** 장치를 생성하려면 다음 명령을 사용합니다.

```
# ip link add dev bareudp0 type bareudp dstport 6635 ethertype mpls_uc
```

bareudp0 장치를 사용하여 **UDP** 터널에서 **MPLS** 수신 패킷을 라우팅하려면 다음 명령을 사용합니다.

```
# tc qdisc add dev enp1s0 ingress
# tc filter add dev enp1s0 ingress proto mpls_uc matchall  \
```

```
> action tunnel_key set src_ip 2001:db8::22 dst_ip 2001:db8::21 id 0   \
> action mirred egress redirect dev bareudp0
```

bareudp 장치를 만드는 동안 사용되는 옵션 및 매개 변수에 대한 자세한 내용은 **ip-link(8)** 도움말 페이지의 **Bareudp** 유형 지원 섹션을 참조하십시오.

(BZ#1849815)

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)

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 64**비트가 아닌 아키텍처에 **XDP** 프로그램 로드. **AMD** 및 **Intel 64**비트 이외의 아키텍처에는 **libxdp** 라이브러리를 사용할 수 없습니다.
- **XDP** 하드웨어 오프로딩.

(BZ#1889737)

TC용 멀티 프로토콜 레이블 전환을 기술 프리뷰로 사용 가능

MPLS(Multi-protocol Label Switching)는 엔터프라이즈 네트워크 전반에서 트래픽 흐름을 라우팅하는 커널 내 데이터 전달 메커니즘입니다. **MPLS** 네트워크에서 패킷을 수신하는 라우터는 패킷에 연결된 레이블을 기반으로 패킷의 추가 경로를 결정합니다. 레이블을 사용하면 **MPLS** 네트워크는 특정 특성을 가진 패킷을 처리할 수 있습니다. 예를 들어 특정 포트에서 수신된 패킷을 관리하거나 일관된 방식으로 특정 유형의 트래픽을 전달하기 위해 **add tc** 필터를 추가할 수 있습니다.

패킷이 엔터프라이즈 네트워크에 진입한 후 **MPLS** 라우터는 레이블 추가를 위한 내보내기, 레이블을 업데이트하는 스왑, 라벨을 제거하기 위한 **pop** 등의 패킷에서 여러 작업을 수행합니다. **MPLS**를 사용하면 **RHEL**에서 하나 이상의 레이블을 기반으로 작업을 로컬로 정의할 수 있습니다. 라우터를 구성하고 트래픽 제어(**tc**) 필터를 설정하여 레이블, 트래픽 클래스, 스택하단, 라이브 시간과 같은 **MPLS** 레이블 스택(**lse**)요소를 기반으로 패킷에 적절한 조치를 수행할 수 있습니다.

예를 들어 다음 명령은 첫 번째 레이블이 ***12323*** 이고 두 번째 레이블 ***45832*** 가 있는 수신 패킷과 일치하도록 필터를 ***enp0s1*** 네트워크 인터페이스에 추가합니다. 일치하는 패킷에서 다음 작업이 수행됩니다.

- 첫 번째 **MPLS TTL**이 감소합니다 (**TTL**이 **0**에 도달하면 패킷이 삭제됩니다)
- 첫 번째 **MPLS** 레이블이 ***549386***으로 변경되었습니다.
- 결과 패킷은 대상 **MAC** 주소 ***00:00:5E:53:01*** *및 소스* ***MAC*** *주소* ***00:00:5E:00:53:02*** 를 사용하여 ***enp0s2*** 를 통해 전송됩니다.

```
# tc filter add dev enp0s1 ingress protocol mpls_uc flower mpls lse depth 1 label 12323 lse
depth 2 label 45832 \
action mpls dec_ttl pipe \
action mpls modify label 549386 pipe \
action pedit ex munge eth dst set 00:00:5E:00:53:01 pipe \
action pedit ex munge eth src set 00:00:5E:00:53:02 pipe \
action mirred egress redirect dev enp0s2
```

(BZ#1814836, BZ#1856415)

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)

향상된 Multipath TCP 지원은 기술 프리뷰로 제공됩니다.

다중 경로 TCP(MPTCP)는 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.

RHEL 8.4는 다음과 같은 추가 기능을 제공합니다.

- 여러 동시 활성 서브스트림
- active-backup 지원
- 스트림 성능 개선
- 수신 및 전송 버퍼 자동 조정으로 메모리 사용량 개선
- SYN 쿠키 지원

서버에서 실행되는 애플리케이션은 기본적으로 MPTCP를 지원하거나 관리자가 eBPF 프로그램을 커널에 로드하여 IPPROTO_TCP를 IPPROTO_MPTCP 로 동적으로 변경해야 합니다.

자세한 내용은 Multipath TCP로 시작하기를 참조하십시오.

(JIRA:RHELPLAN-57712)

systemd-resolved 서비스를 기술 프리뷰로 사용 가능

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

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

(BZ#1906489)

nispor 패키지가 기술 프리뷰로 사용 가능

nispor 패키지는 이제 Linux 네트워크 상태 쿼리를 위한 통합 인터페이스인 기술 프리뷰로 사용할 수 있습니다. nispor는 python 및 C api를 통해 실행 중인 모든 네트워크 상태를 쿼리하는 통합 방법을 제공합니다. nispor 는 nmstate 도구에서 종속성으로 작동합니다.

nispor 패키지를 nmstate 종속성 또는 개별 패키지로 설치할 수 있습니다.

- nispor 를 개별 패키지로 설치하려면 다음을 입력합니다.

```
# yum install nispor
```

- nmstate 종속성으로 nispor 를 설치하려면 다음을 입력합니다.

```
# yum install nmstate
```

nispor 는 종속성으로 나열됩니다.

nispor 사용에 대한 자세한 내용은 /usr/share/doc/nispor/README.md 파일을 참조하십시오.

(BZ#1848817)

8.3. 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)

accel-config 패키지는 기술 프리뷰로 사용 가능

accel-config 패키지는 이제 기술 프리뷰로 RHEL 8.4용 Intel EM 64T 및 AMD64 아키텍처에서 사용할 수 있습니다. 이 패키지는 Linux 커널에서 DSA(Data-streaming 액셀러레이터) 하위 시스템을 제어하고 구성하는 데 도움이 됩니다. 또한 sysfs (pseudo-filesystem)를 통해 장치를 구성하고 json 형식으로 구성을 저장하고 로드합니다.

(BZ#1843266)

SGX를 기술 프리뷰로 이용 가능

SGX(Software Guard Extensions)는 소프트웨어 코드와 데이터를 공개 및 수정하지 못하도록 보호하는 Intel® 기술입니다. 이 릴리스에서는 SGX v1 및 v1.5에 대한 커널 지원이 시작됩니다. 버전 1을 사용하면 유연한 시작 제어 메커니즘을 사용하는 플랫폼이 SGX 기술을 사용할 수 있습니다.

(BZ#1660337)

eBPF를 기술 프리뷰로 이용 가능

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

가상 시스템에는 다양한 유형의 맵 생성을 지원하고 특수 어셈블리와 유사한 코드로 프로그램을 로드할 수 있는 새로운 시스템 호출 bpf() 가 포함되어 있습니다. 그런 다음 코드가 커널로 로드되고 즉시 컴파일을 사용하여 기본 머신 코드로 변환됩니다. bpf() syscall은 root 사용자와 같이 CAP_SYS_ADMIN 기능을 가진 사용자만 사용할 수 있습니다. 자세한 내용은 bpf(2) 매뉴얼 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 bpftrace.
- AF_XDP: 패킷 처리 성능 우선 순위를 지정하는 애플리케이션의 사용자 공간에 eXpress Data Path(XDP) 경로를 연결하는 소켓입니다.

(BZ#1559616)

커널용 액셀러레이터 드라이버를 스트리밍하는 데이터는 기술 프리뷰로 사용할 수 있습니다.

커널의 DSA(데이터 스트리밍 액셀러레이터) 드라이버는 현재 기술 프리뷰로 사용할 수 있습니다. DSA는 Intel CPU 통합 액셀러레이터로, 프로세스 주소 공간 ID(pasid) 제출 및 공유 가상 메모리(SVM)가 포함된 공유 작업 대기열을 지원합니다.

(BZ#1837187)

soft-RoCE를 기술 프리뷰로 이용 가능

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

(BZ#1605216)

8.4. 파일 시스템 및 스토리지

NVMe/TCP를 기술 프리뷰로 사용 가능

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

NVMe/TCP를 스토리지 클라이언트 또는 대상으로 사용하는 것은 nvme-cli 및 nvm etcli 패키지에서

제공하는 툴을 사용하여 관리할 수 있습니다.

NVMe/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**Volatile** 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 철저하게 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 씬 프로비저닝 관리
- 필요에 따라 파일 시스템 크기 자동 확장
- 파일 시스템 관리

Stratis 스토리지를 관리하려면 stratisd 백그라운드 서비스와 통신하는 stratis 유틸리티를 사용합니다.

Stratis는 기술 프리뷰로 제공됩니다.

자세한 내용은 Stratis 설명서를 참조하십시오. Stratis 파일 시스템 설정.

RHEL 8.3에서 Stratis를 버전 2.1.0으로 업데이트했습니다. 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 Samba별 Kerberos 서비스 주체를 IdM에 추가하고 IdM 클라이언트를 준비합니다. 예를 들어 유틸리티는 sss ID 매핑 백엔드에 대한 ID 매핑 구성을 사용하여 /etc/samba/smb.conf 를 만듭니다. 결과적으로 관리자가 IdM 도메인 멤버에 Samba를 설정할 수 있습니다.

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

자세한 내용은 IdM 도메인 멤버에서 Samba 설정을 참조하십시오.

(JIRA:RHELPLAN-13195)

8.5. 고가용성 및 클러스터

pcs cluster setup 명령의 로컬 모드 버전을 기술 프리뷰로 사용 가능

기본적으로 pcs cluster setup 명령은 모든 구성 파일을 클러스터 노드에 자동으로 동기화합니다. Red Hat Enterprise Linux 8.3 이후 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 번들이 기술 프리뷰로 사용 가능한 컨테이너 번들 기능과 함께 Podman에서 실행됩니다. 이 기능에는 기술 프리뷰가 한 가지 예외가 있습니다. Red Hat은 Red Hat Openstack을 위한 Pacemaker 번들 사용을 완전히 지원합니다.

(BZ#1619620)

corosync-qdevice 의 추론을 기술 프리뷰로 사용 가능

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

(BZ#1784200)

새로운 fence-agents-heuristics-ping 펜스 에이전트

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

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

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

(BZ#1775847)

8.6. IDM (IDENTITY MANAGEMENT)

ID 관리 JSON-RPC API를 기술 프리뷰로 사용 가능

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

이전에는 여러 버전의 API 명령을 활성화하도록 IdM API가 개선되었습니다. 이러한 개선 사항은 명령의 동작을 호환되지 않는 방식으로 변경할 수 있습니다. 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 사용할 수 있습니다.

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

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

(BZ#1664719)

IdM에서 DNSSEC 사용 가능

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

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

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

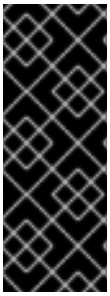
통합된 DNS가 있는 IdM 서버는 DNSSEC를 사용하여 다른 DNS 서버에서 얻은 DNS 응답을 확인합니다. 이는 권장 명명 방식에 따라 구성되지 않은 DNS 영역의 가용성에 영향을 줄 수 있습니다.

(BZ#1664718)

ACME를 기술 프리뷰로 이용 가능

이제 ACME(Automd Certificate Management Environment) 서비스를 기술 프리뷰로 IdM(Identity Management)에서 사용할 수 있습니다. ACME는 자동화된 식별자 검증 및 인증서 발급을 위한 프로토콜입니다. 이 목표는 인증서의 수명을 줄이고 인증서 라이프사이클 관리로부터 수동 프로세스를 방지하여 보안을 강화하는 것입니다.

RHEL에서 ACME 서비스는 RHCS(Red Hat Certificate System) PKI ACME 응답자를 사용합니다. RHCS ACME 하위 시스템은 IdM 배포의 모든 CA(인증 기관) 서버에 자동으로 배포되지만 관리자가 요청을 활성화할 때까지 서비스 요청은 서비스하지 않습니다. RHCS는 ACME 인증서를 발급할 때 acmeIPAServerCert 프로필을 사용합니다. 발급한 인증서의 유효 기간은 90일입니다. ACME 서비스를 활성화하거나 비활성화하면 전체 IdM 배포에 영향을 줍니다.



중요

모든 서버가 RHEL 8.4 이상을 실행하는 IdM 배포에서만 ACME를 활성화하는 것이 좋습니다. 이전 RHEL 버전에는 ACME 서비스가 포함되지 않으므로 혼합 버전 배포에서 문제가 발생할 수 있습니다. 예를 들어 ACME가 없는 CA 서버는 다른 SAN(DNS 주체 대체 이름)을 사용하므로 클라이언트 연결이 실패할 수 있습니다.

주의

현재 RHCS는 만료된 인증서를 제거하지 않습니다. ACME 인증서는 90일 후에 만료되므로 만료된 인증서가 누적되어 성능에 영향을 줄 수 있습니다.

- 전체 IdM 배포에서 ACME를 활성화하려면 ipa-acme-manage enable 명령을 사용합니다.

```
# ipa-acme-manage enable
The ipa-acme-manage command was successful
```

- 전체 IdM 배포에서 ACME를 비활성화하려면 ipa-acme-manage disable 명령을 사용합니다.

```
# ipa-acme-manage disable
The ipa-acme-manage command was successful
```

- ACME 서비스가 설치되어 있고 활성화 또는 비활성화되었는지 확인하려면 ipa-acme-manage status 명령을 사용합니다.

```
# ipa-acme-manage status
ACME is enabled
The ipa-acme-manage command was successful
```

(JIRA:RHELPLAN-58596)

8.7. 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)

8.8. 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)

8.9. RED HAT ENTERPRISE LINUX 시스템 역할

HA Cluster RHEL 시스템 역할을 기술 프리뷰로 사용 가능

HA(고가용성 클러스터) 역할은 이제 기술 프리뷰로 사용할 수 있습니다. 현재 다음과 같은 주요 설정을 사용할 수 있습니다.

- 펜싱이 실행되지 않고 리소스가 없는 클러스터 구성
- 다중 링크 클러스터 구성
- 사용자 정의 클러스터 이름 및 노드 이름 구성
- 부팅 시 클러스터가 자동으로 시작되도록 구성

(BZ#1893743)

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 문서를 참조하십시오.

(BZ#1812552)

8.10. 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-V에서 기본적으로 활성화되어 있지 않은 경우도 있습니다. 이를 활성화하려면 다음 Microsoft 문서를 참조하십시오.

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

(BZ#1519039)

KVM 가상 머신용 AMD SEV

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

단일 호스트에서 이 기능을 한 번에 사용할 수 있는 VM의 개수는 호스트 하드웨어에 의해 결정됩니다. 현재 AMD EPYC 프로세서는 SEV를 사용하여 최대 509개의 실행 중인 VM을 지원합니다.

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

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

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

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

Intel vGPU

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

선택한 Intel GPU만 vGPU 기능과 호환됩니다.

또한 Intel vGPU에서 작동하는 VNC 콘솔을 활성화할 수 있습니다. 사용자는 VM의 VNC 콘솔에 연결

하여 Intel vGPU에서 호스팅하는 VM의 데스크탑을 확인할 수 있습니다. 그러나 현재 이 기능은 RHEL 게스트 운영 체제에서만 작동합니다.

(BZ#1528684)

중첩된 가상 머신 생성

중첩된 KVM 가상화는 RHEL 8을 사용하여 Intel, AMD64 및 IBM Z 시스템 호스트에서 실행되는 KVM 가상 시스템(VM)을 위한 기술 프리뷰로 제공됩니다. 이 기능을 사용하면 물리적 RHEL 8 호스트에서 실행되는 RHEL 7 또는 RHEL 8 VM이 하이퍼바이저 역할을 하며 고유한 VM을 호스팅할 수 있습니다.

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

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

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

- NIC(네트워크 인터페이스 컨트롤러)에 SR-IOV 지원이 활성화됨
- 가상 NIC에 대해 SR-IOV 지원이 활성화됨
- 가상 스위치에 SR-IOV 지원이 활성화됨
- NIC의 VF(가상 기능)가 가상 머신에 연결되어 있습니다.

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

(BZ#1348508)

ESXi 하이퍼바이저 및 SEV-ES는 RHEL VM의 기술 프리뷰로 사용 가능

RHEL 8.4 이상에서는 기술 프리뷰로 AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES)를 활성화하여 VMware의 ESXi 하이퍼바이저 버전 7.0.2 이상에서 RHEL 가상 시스템(VM)을

보호할 수 있습니다.

(BZ#1904496)

8.11. 컨테이너

CNI 플러그인은 Podman에서 기술 프리뷰로 사용할 수 있습니다.

이제 **Podman rootless** 모드에서 기술 프리뷰로 **CNI** 플러그인을 사용할 수 있습니다. 이 기능을 활성화하려면 사용자가 자체 **rootless CNI** 인프라 컨테이너 이미지를 빌드해야 합니다.

(BZ#1932083)

crun 은 기술 프리뷰로 사용할 수 있습니다.

이제 **crun OCI** 런타임을 **container-tools:rhel8** 모듈에 기술 프리뷰로 사용할 수 있습니다. **crun** 컨테이너 런타임은 컨테이너가 **rootless** 사용자의 추가 그룹에 액세스할 수 있는 주석을 지원합니다. 이는 **setgid**가 설정된 디렉터리 또는 사용자가 그룹 액세스 권한만 가진 디렉터리에 볼륨 마운팅에 유용합니다. 현재 **crun** 또는 **runc** 런타임이 **cgroupsv2** 를 완전히 지원하지 않습니다.

(BZ#1841438)

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 및 컨테이너 그룹으로 구성된 포드를 관리하는 데 사용됩니다.

(JIRA:RHELPLAN-56659)

9장. 사용되지 않는 기능

이 부분에서는 **Red Hat Enterprise Linux 8**에서 *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 8**에서는 변경되지 않습니다. 지원 기간에 대한 자세한 내용은 **Red Hat Enterprise Linux** 라이프 사이클 및 **Red Hat Enterprise Linux Application Streams** 라이프 사이클을 참조하십시오.

사용되지 않는 하드웨어 구성 요소는 현재 또는 향후 주요 릴리스의 새로운 배포에 구현하는 것을 권장하지 않습니다. 하드웨어 드라이버 업데이트는 보안 및 중요 수정 사항으로만 제한됩니다. **Red Hat**은 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 존재하지만 **RHEL 8**에서 *제거된* 기능에 대한 자세한 내용은 **RHEL 8** 채택 시 고려 사항을 참조하십시오.

9.1. 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)

Kickstart autostep 명령이 더 이상 사용되지 않음

autostep 명령은 더 이상 사용되지 않습니다. 이 명령에 대한 관련 섹션은 RHEL 8 설명서에서 제거되었습니다.

(BZ#1904251)

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-composer에 대한 lorax-composer 를 제거하고 osbuild-composer 백엔드를 설치 제거하는 것이 좋습니다.

자세한 내용은 사용자 지정 RHEL 시스템 이미지 구성을 참조하십시오.

(BZ#1893767)

9.2. 소프트웨어 관리

rpmbuild --sign 이 더 이상 사용되지 않음

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

(BZ#1688849)

9.3. 쉘 및 명령행 툴

OpenEXR 구성 요소가 더 이상 사용되지 않음

OpenEXR 구성 요소는 더 이상 사용되지 않습니다. 따라서 EXR 이미지 형식에 대한 지원이 imagecodecs 모듈에서 삭제되었습니다.

(BZ#1886310)

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 컨텐츠 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)

9.4. 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 Portal의 약한 암호화 알고리즘 지식 베이스 문서 및 update-crypto-policies(8) 도움말 페이지를 참조하십시오.

(BZ#1660839)

RHEL 8에서 DSA 사용 중단

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

(BZ#1646541)

SSL2 Client Hello가 NSS에서 더 이상 사용되지 않음

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

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

(BZ#1645153)

TPM 1.2가 더 이상 사용되지 않음

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

(BZ#1657927)

/etc/selinux/config 를 사용하여 SELinux를 비활성화하는 런타임이 더 이상 사용되지 않음

/etc/selinux/config 파일에서 SELINUX=disabled 옵션을 사용하여 SELinux를 비활성화하는 런타임은 더 이상 사용되지 않습니다. RHEL 9에서 /etc/selinux/config 를 통해서만 SELinux를 비활성화하면 SELinux가 활성화된 상태로 시작되지만 정책이 로드되지 않습니다.

시나리오에서 SELinux를 완전히 비활성화해야 하는 경우 Red Hat은 SELinux 제목 사용의 부팅 시 SELinux 모드 변경 섹션에 설명된 대로 커널 명령줄에 selinux=0 매개 변수를 추가하여 SELinux 비활성화를 권장합니다.

(BZ#1932222)

selinux-policy에서 제거된 IPA SELinux 모듈

ipa SELinux 모듈은 더 이상 유지 관리되지 않으므로 selinux-policy 패키지에서 제거되었습니다. 이제 이 기능이 ipa-selinux 하위 패키지에 포함됩니다. 로컬 SELinux 정책의 ipa 모듈에서 유형 또는 인터페이스를 사용해야 하는 경우 ipa-selinux 패키지를 설치합니다.

(BZ#1461914)

9.5. 네트워킹

RHEL 8에서 네트워크 스크립트가 더 이상 사용되지 않음

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

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

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

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

ifup 및 **ifdown** 스크립트는 설치된 레거시 네트워크 스크립트에 연결됩니다.

레거시 네트워크 스크립트를 호출하면 사용 중단을 알리는 경고 메시지가 표시됩니다.

(BZ#1647725)

dropwatch 툴이 더 이상 사용되지 않음

dropwatch 툴이 더 이상 사용되지 않습니다. 이 도구는 향후 릴리스에서 지원되지 않습니다. 따라서 이 패키지는 새로운 배포에 권장되지 않으므로 **Red Hat**은 **perf** 명령행 도구를 사용하는 것이 좋습니다.

perf 명령줄 툴 사용에 대한 자세한 내용은 **Red Hat** 고객 포털의 **Perf**로 시작하기 섹션 또는 **perf** 도움말 페이지를 참조하십시오.

(BZ#1929173)

9.6. 커널

디스크리스 부팅을 사용하여 실시간 **8**용 **RHEL** 설치는 더 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 8**의 마이너 업데이트에서는 더 이상 디스크리스 부팅 기능이 지원되지 않습니다.

(BZ#1748980)

The rdma_rxe soft -RoCE 드라이버는 더 이상 사용되지 않습니다.

소프트웨어 **RXE(Remote Direct Memory Access over Converged Ethernet)**는 **RDMA(Remote Direct Memory Access)**를 에뮬레이션하는 기능입니다. **RHEL 8**에서는 **soft-RoCE** 기능은 지원되지 않

는 기술 프리뷰로 사용할 수 있습니다. 그러나 안정성 문제로 인해 이 기능은 더 이상 사용되지 않으며 RHEL 9에서 제거됩니다.

(BZ#1878207)

9.7. 플랫폼 지원

Linux firewire 하위 시스템 및 관련 사용자 공간 구성 요소는 RHEL 8에서 더 이상 사용되지 않음

firewire 하위 시스템은 IEEE 1394 버스의 모든 리소스를 사용하고 유지 관리할 수 있는 인터페이스를 제공합니다. RHEL 9에서 firewire 는 커널 패키지에서 더 이상 지원되지 않습니다.

firewire 에는 libavc1394,libdc1394,libraw1394 패키지에서 제공하는 여러 사용자 공간 구성 요소가 포함되어 있습니다. 이러한 패키지도 사용 중단의 영향을 받습니다.

(BZ#1871863)

9.8. 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 8에서 계속 사용할 수 있습니다.

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

자세한 내용은 디스크 스케줄러 설정을 참조하십시오.

(BZ#1665295)

LVM 미러 가 더 이상 사용되지 않음

LVM 미러 세그먼트 유형이 더 이상 사용되지 않습니다. 미러 지원은 향후 RHEL의 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 변환을 참조하십시오.

LVM 미러 에는 몇 가지 알려진 문제가 있습니다. 자세한 내용은 파일 시스템 및 스토리지의 알려진 문제를 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)

비동기 이외의 VDO 쓰기 모드는 더 이상 사용되지 않음

VDO는 RHEL 8에서 여러 쓰기 모드를 지원합니다.

- sync
- async
- async-unsafe

- auto

RHEL 8.4부터 다음 쓰기 모드가 더 이상 사용되지 않습니다.

sync

VDO 계층 위의 장치는 VDO가 동기 상태인지 인식할 수 없으므로 장치는 VDO 동기화 모드를 활용할 수 없습니다.

async-unsafe

VDO는 Atomicity, Consistency, Isolation, Durability(ACID)를 준수하는 비동기 모드의 성능을 줄이기 위한 해결 방법으로 이 쓰기 모드를 추가했습니다. Red Hat은 대부분의 사용 사례에 대해 async-unsafe 를 권장하지 않으며 이를 사용하는 사용자를 인식하지 못합니다.

auto

이 쓰기 모드에서는 다른 쓰기 모드 중 하나만 선택합니다. VDO가 단일 쓰기 모드만 지원하는 경우에는 더 이상 필요하지 않습니다.

이러한 쓰기 모드는 향후 주요 RHEL 릴리스에서 제거됩니다.

이제 권장 VDO 쓰기 모드가 async 가 됩니다.

VDO 쓰기 모드에 대한 자세한 내용은 Selecting a VDO write mode 를 참조하십시오.

(JIRA:RHELPLAN-70700)

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)

9.9. 고가용성 및 클러스터

clcockter 툴을 지원하는 **pcs** 명령이 더 이상 사용되지 않음

클러스터 구성 형식을 분석하기 위해 **cl cockter** 툴을 지원하는 **pcs** 명령이 더 이상 사용되지 않습니다. 이제 명령이 더 이상 사용되지 않으며 이러한 명령과 관련된 섹션이 **pcs help** 디스플레이 및 **pcs(8)** 도움말 페이지에서 제거된다는 경고를 출력합니다.

(BZ#1851335)

9.10. 컴파일러 및 개발 도구

gdb.i686 패키지는 더 이상 사용되지 않습니다.

RHEL 8.1에서는 다른 패키지의 종속성 문제로 인해 **32**비트 버전의 **GDB(GNU Debugger) gdb.i686** 이 제공되었습니다. **RHEL 8**에서는 **32**비트 하드웨어를 지원하지 않으므로 **RHEL 8.4** 이후 **gdb.i686** 패키지는 더 이상 사용되지 않습니다. **64**비트 버전의 **GDB gdb.x86_64** 는 **32**비트 애플리케이션을 디버깅할 수 있습니다.

gdb.i686 을 사용하는 경우 다음과 같은 중요한 문제를 유의하십시오.

- **gdb.i686** 패키지는 더 이상 업데이트되지 않습니다. 대신 **gdb.x86_64** 를 설치해야 합니다.
- **gdb.i686**이 설치되어 있으면 **gdb. x86_64**를 설치하면 **dnf** 가 패키지 **gdb -8.2-14.el8.x86_64**가 더 이상 사용되지 않습니다. **gdb-8.2-12.el8.i686**에서 제공하는 **gdb <8.2-14.el8.el8.el8.i686.** 이 동작은 다음과 같습니다. **gdb.i686** 을 제거하거나 **dnf** 를 **--allowerasing** 옵션을 전달하여 **gdb.i686** 을 제거하고 **gdb.x8_64** 를 설치합니다.
-

사용자는 더 이상 libc.so .6()(64비트) 패키지를 사용하는 64비트 시스템에 gdb. i686 패키지를 설치할 수 없습니다.

(BZ#1853140)

Libdwarf 가 더 이상 사용되지 않음

RHEL 8에서는 libdwarf 라이브러리가 더 이상 사용되지 않습니다. 라이브러리는 향후 주요 릴리스에서 지원되지 않을 가능성이 큽니다. 대신 ELF/DWARF 파일을 처리하려는 애플리케이션에 elfutils 및 libdw 라이브러리를 사용합니다.

libdwarf-tools dwarfdump 프로그램의 대안은 모두 --debug -dump 플래그를 전달하여 사용하는 binutils readelf 프로그램 또는 elfutils eu- readelf 프로그램입니다.

(BZ#1920624)

9.11. IDM (IDENTITY MANAGEMENT)

OpenSSH-ldap 이 더 이상 사용되지 않음

openssh-ldap 하위 패키지는 Red Hat Enterprise Linux 8에서 더 이상 사용되지 않으며 RHEL 9에서 제거됩니다. openssh-ldap 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 ldap 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 SSSD에서 키를 가져올 수 있도록 하려면 sssd.conf 파일의 services 옵션에 ssh를 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 8**에서 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. **KDC**가 **krb5check** 오픈소스 **Python** 스크립트와 함께 **DES** 또는 **3DES** 암호화를 사용하는지 확인하십시오. **GitHub**의 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 **3DES**에서 독립성을 테스트합니다.
   a. **KDC**의 **/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 _enctypes,default_tgs_enctypes** 및 **default_tkt_enctypes** 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)

ctdb 서비스의 독립 실행형 사용이 더 이상 사용되지 않음

RHEL 8.4부터 고객은 다음 두 조건이 모두 적용되는 경우에만 **ctdb** 클러스터형 **Samba** 서비스를 사용하는 것이 좋습니다.

- **ctdb** 서비스는 **resource-agent ctdb** 를 사용하여 **pacemaker** 리소스로 관리됩니다.
- **ctdb** 서비스는 **Red Hat Gluster Storage** 제품 또는 **GFS2** 파일 시스템에서 제공하는 **GlusterFS** 파일 시스템을 포함하는 스토리지 볼륨을 사용합니다.

ctdb 서비스의 독립형 사용 사례는 더 이상 사용되지 않으며 차후 **Red Hat Enterprise Linux** 주요 릴리스에는 포함되지 않습니다. **Samba** 지원 정책에 대한 자세한 내용은 기술 자료 문서 **RHEL** 복구 스토리지 지원 정책 **- ctdb** 일반 정책을 참조하십시오.

(BZ#1916296)

PDC 또는 **BDC**로 **Samba** 실행이 더 이상 사용되지 않음

관리자가 **Samba**를 **PDC**(기본 도메인 컨트롤러)로 실행하고 백업 도메인 컨트롤러(**BDC**)로 **Samba**를 실행할 수 있도록 하는 전통적인 도메인 컨트롤러 모드는 더 이상 사용되지 않습니다. 이러한 모드를 구성하는 코드 및 설정은 향후 **Samba** 릴리스에서 제거됩니다.

RHEL 8의 **Samba** 버전이 **PDC** 및 **BDC** 모드를 제공하는 한, **Red Hat**은 **NT4** 도메인을 지원하는 **Windows** 버전을 사용하는 기존 설치에서만 이러한 모드를 지원합니다. **Red Hat**은 새로운 **Samba NT4**

도메인을 설정하지 않는 것이 좋습니다. Microsoft 운영 체제는 Windows 7 및 Windows Server 2008 R2 이후의 경우 NT4 도메인을 지원하지 않기 때문입니다.

PDC를 사용하여 Linux 사용자만 인증하는 경우 RHEL 서브스크립션에 포함된 Red Hat IdM(Identity Management) 으로 마이그레이션하는 것이 좋습니다. 그러나 Windows 시스템을 IdM 도메인에 연결할 수는 없습니다. Red Hat은 백그라운드에서 사용하는 PDC 기능인 IdM을 계속 지원합니다.

Red Hat은 DB(AD 도메인 컨트롤러)로 Samba 실행을 지원하지 않습니다.

(BZ#1926114)

libwbclient의 SSSD 버전이 더 이상 사용되지 않음

libwbclient 패키지의 SSSD 구현이 추가되어 Samba smbd 서비스가 winbind 서비스를 실행할 필요 없이 AD에서 사용자 및 그룹 정보를 검색할 수 있습니다. 이제 Samba에서 winbind 서비스가 실행 중이고 AD와의 통신을 처리해야 하므로 보안상의 이유로 관련 코드가 smdb 에서 제거되었습니다. 이러한 추가 필수 기능은 SSSD에 속하지 않고 libwbclient 의 SSSD 구현은 최신 버전의 Samba에서 사용할 수 없으므로 libwbclient 의 SSSD 구현은 더 이상 사용되지 않습니다.

(BZ#1881992)

9.12. 데스크탑

libgnome-keyring 라이브러리가 더 이상 사용되지 않음

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

(BZ#1607766)

9.13. 그래픽 인프라

AGP 그래픽 카드는 더 이상 지원되지 않습니다.

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

(BZ#1569610)

9.14. 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)

9.15. 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)

9.16. 가상화

virt-manager가 더 이상 사용되지 않음

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

(JIRA:RHELPLAN-10304)

RHEL 8에서 가상 머신 스냅샷이 올바르게 지원되지 않음

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

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

니다.

(BZ#1686057)

Cirrus VGA 가상 GPU 유형이 더 이상 사용되지 않음

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

(BZ#1651994)

IBM POWER의 **KVM**이 더 이상 사용되지 않음

IBM POWER 하드웨어에서 **KVM** 가상화를 사용하는 것이 더 이상 사용되지 않습니다. 결과적으로 **IBM POWER**의 **KVM**은 **RHEL 8**에서 계속 지원되지만 향후 **RHEL**의 주요 릴리스에서는 지원되지 않습니다.

(JIRA:RHELPLAN-71200)

SHA1- 기반 서명을 사용한 **SecureBoot** 이미지 확인이 더 이상 사용되지 않음

UEFI (PE/COFF) 실행 파일에서 **SHA1-** 기반 서명을 사용하여 **SecureBoot** 이미지 확인을 수행하는 것이 더 이상 사용되지 않습니다.

대신 **Red Hat**은 **SHA2** 알고리즘을 기반으로 하는 서명을 사용하는 것이 좋습니다.

(BZ#1935497)

SPICE가 더 이상 사용되지 않음

SPICE 원격 디스플레이 프로토콜은 더 이상 사용되지 않습니다. **SPICE**는 **RHEL 8**에서 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)

9.17. 컨테이너

Podman varlink 기반 **API v1.0**이 제거되었습니다.

Podman varlink 기반 **API v1.0**은 이전 **RHEL 8** 릴리스에서 더 이상 사용되지 않습니다. **Podman v2.0**에서 새 **Podman v2.0 RESTful API**를 도입했습니다. **Podman v3.0**이 릴리스되면서 **varlink** 기반 **API v1.0**이 완전히 제거되었습니다.

(JIRA:RHELPLAN-45858)

container-tools:1.0 이 더 이상 사용되지 않음

container-tools:1.0 모듈은 더 이상 사용되지 않으며 더 이상 보안 업데이트를 받지 않습니다. **container -tools:2.0** 또는 **container-tools: 3.0** 과 같이 지원되는 최신 모듈 스트림을 사용하는 것이 좋습니다.

(JIRA:RHELPLAN-59825)

9.18. 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**
- **firewire**

- **geoipupdate**
- 호스트 이름
- **ISL**
- **ISL-devel**
- **libavc1394**
- **libdc1394**
- **libdwarf**
- **libdwarf-devel**
- **libdwarf-static**
- **libdwarf-tools**
- **libidn**
- **libpng12**
- **libraw1394**
- **lorax-composer**

- **mailman**
- **mailx - s-nail로 대체**
- **Mercurial**
- **ncompress**
- **net-tools**
- **netcf**
- **netcf-libs**
- **network-scripts**
- **nss_nis**
- **nss-pam-ldapd**
- **openssh-ldap**
- **parfait**
- **peripety**
- **perl-prefork**

- **perl-Sys-Virt**
- **python3-nose**
- **python3-pymongo**
- **python3-pytoml - python3-to ml로 교체**
- **python3-virtualenv - Python 3에서 venv 모듈을 대신 사용합니다.**
- **redhat-support-lib-python**
- **redhat-support-tool**
- **scala**
- **sendmail**
- **jp-tools**
- **ypbind**
- **ypserv**
- **xdelta**
- **xinetd**

9.19. 사용되지 않는 장치

이 섹션에는 **RHEL 8**의 라이프사이클이 끝날 때까지 계속 지원되지만 이 제품의 향후 주요 릴리스에서는 지원되지 않을 수 있으며 새로운 배포에 권장되지 않는 장치(드라이버, 어댑터)가 나열되어 있습니다. 나열된 장치 이외의 장치에 대한 지원은 변경되지 않았습니다.

PCI ID는 ***vendor:device:subvendor:subdevice*** 형식입니다. ***subdevice*** 또는 ***subvendor:subdevice*** 항목이 나열되지 않은 경우 이러한 누락된 항목의 값이 있는 장치는 더 이상 사용되지 않습니다. 시스템에서 하드웨어의 **PCI ID**를 확인하려면 **lspci -nn** 명령을 실행합니다.

장치 유형	드라이버	장치	장치 ID
PCI	bnx2		
PCI	hpsa		0x103C:0x3239:0x103C:0x21C4
PCI	hpsa		0x103C:0x3239:0x103C:0x21C9
PCI	hpsa		0x103C:0x3239:0x103C:0x21CC
PCI	hpsa		0x103C:0x3239:0x103C:0x21CD
PCI	hpsa		0x103C:0x3239:0x103C:0x21CE
PCI	hpsa		0x103C:0x323a:0x103C:0x3233
PCI	hpsa		0x103C:0x323a:0x103C:0x3241
PCI	hpsa		0x103C:0x323a:0x103C:0x3243
PCI	hpsa		0x103C:0x323a:0x103C:0x3245
PCI	hpsa		0x103C:0x323a:0x103C:0x3247
PCI	hpsa		0x103C:0x323a:0x103C:0x3249
PCI	hpsa		0x103C:0x323a:0x103C:0x324A
PCI	hpsa		0x103C:0x323a:0x103C:0x324B
PCI	hpsa		0x103C:0x323b:0x103C:0x3350
PCI	hpsa		0x103C:0x323b:0x103C:0x3351
PCI	hpsa		0x103C:0x323b:0x103C:0x3352

장치 유형	드라이버	장치	장치 ID
PCI	hpsa		0x103C:0x323b:0x103C:0x3353
PCI	hpsa		0x103C:0x323b:0x103C:0x3354
PCI	hpsa		0x103C:0x323b:0x103C:0x3355
PCI	hpsa		0x103C:0x323b:0x103C:0x3356
PCI	hpsa		0x103C:0x333f:0x103c:0x333f
PCI	hpsa		0x9005:0x0290:0x9005:0x0580
PCI	hpsa		0x9005:0x0290:0x9005:0x0581
PCI	hpsa		0x9005:0x0290:0x9005:0x0582
PCI	hpsa		0x9005:0x0290:0x9005:0x0583
PCI	hpsa		0x9005:0x0290:0x9005:0x0584
PCI	hpsa		0x9005:0x0290:0x9005:0x0585
PCI	lpfc		0x10df:0x0724
PCI	lpfc		0x10df:0xe200
PCI	lpfc		0x10df:0xe220
PCI	lpfc		0x10df:0xf011
PCI	lpfc		0x10df:0xf015
PCI	lpfc		0x10df:0xf100
PCI	lpfc		0x10df:0xfc40
PCI	megaraid_sas		0x1000:0x005b
PCI	mpt3sas		0x1000:0x006E
PCI	mpt3sas		0x1000:0x0080
PCI	mpt3sas		0x1000:0x0081
PCI	mpt3sas		0x1000:0x0082

장치 유형	드라이버	장치	장치 ID
PCI	mpt3sas		0x1000:0x0083
PCI	mpt3sas		0x1000:0x0084
PCI	mpt3sas		0x1000:0x0085
PCI	mpt3sas		0x1000:0x0086
PCI	mpt3sas		0x1000:0x0087
PCI	myri10ge		
PCI	netxen_nic		
PCI	sfc		0x1924:0x0803
PCI	sfc		0x1924:0x0813
PCI	qla2xxx		0x1077:0x2031
PCI	qla2xxx		0x1077:0x2532
PCI	qla2xxx		0x1077:0x8031

10장. 확인된 문제

이 부분에서는 Red Hat Enterprise Linux 8.4에서 알려진 문제에 대해 설명합니다.

10.1. 설치 프로그램 및 이미지 생성

auth 및 authconfig Kickstart 명령에는 AppStream 리포지토리가 필요

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

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

(BZ#1640697)

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

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

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

(BZ#1697896)

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 전달하면 문제가 해결됩니다. 결과적으로 네트워크 기반 설치 기능을 사용할 수 있습니다.

(BZ#1757877)

USB CD-ROM 드라이브는 Anaconda에서 설치 소스로 사용할 수 없습니다.

USB CD-ROM 드라이브가 소스인 경우 설치에 실패하고 Kickstart ignoredisk --only-use= 명령이 지정됩니다. 이 경우 Anaconda는 이 소스 디스크를 찾아서 사용할 수 없습니다.

이 문제를 해결하려면 harddrive --partition=sdX --dir=/ 명령을 사용하여 USB CD-ROM 드라이브에서 설치합니다. 결과적으로 설치에 실패하지 않습니다.

(BZ#1914955)

Anaconda는 사용자 정의 파티션의 암호화를 표시하지 않습니다

시스템 설치 중에 사용자 지정 파티션을 선택하면 Encrypt my data 라디오 버튼을 사용할 수 없습니다. 따라서 설치가 완료되면 데이터가 암호화되지 않습니다.

이 문제를 해결하려면 암호화하려는 각 장치에 대한 사용자 정의 파티션 화면에서 암호화를 설정합니다. 대화 상자를 종료할 때 Anaconda에서 암호를 요청합니다.

(BZ#1903786)

Kickstart 파일에 파티션 스키마가 지정되지 않은 경우 설치 프로그램에서 자동 파티셔닝 시도

Kickstart 파일을 사용하여 자동 설치를 수행할 때 설치 프로그램은 Kickstart 파일에 파티션 명령을 지정하지 않아도 자동 파티셔닝을 시도합니다. 설치 프로그램은 autopart 명령이 Kickstart 파일에 사용된 것처럼 작동하여 예기치 않은 파티션이 생성됩니다. 이 문제를 해결하려면 대화식으로 수동 파티션을 구성할 수 있도록 Kickstart 파일에서 reqpart 명령을 사용합니다.

(BZ#1954408)

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)

블루프린트 및 **Kickstart** 파일에 동일한 사용자 이름을 추가하면 **Edge** 이미지 설치가 실패합니다.

에지용 **RHEL** 이미지를 설치하려면 사용자가 **rhel-edge-container** 이미지를 빌드하는 청사진을 만들고 **Kickstart** 파일도 만들어 에지용 **RHEL**을 설치해야 합니다. 사용자가 청사진 및 **Kickstart** 파일에 동일한 사용자 이름, 암호 및 **SSH** 키를 추가하면 에지 이미지 설치용 **RHEL**이 실패합니다. 현재는 해결방법이 없습니다.

(BZ#1951964)

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 **1**분 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)

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 Insights에 등록할 수 있습니다.

```
# insights-client --register
```

(BZ#1931069)

autopart 유틸리티를 사용하여 설치에 일치하지 않는 디스크 섹터 크기

일치하지 않는 디스크 섹터 크기가 여러 개 있는 autopart 를 사용하여 RHEL을 설치하는 데 실패합니다. 이 문제를 해결하려면 일반 파티션 구성(예: autopart --type=plain)을 기본 LVM 스키마 대신 사용합니다. 또 다른 옵션은 섹터 크기를 재구성하는 것입니다. 예를 들어 --set-sector-size=<SIZE> <DEVICE> 를 실행합니다.

킥스타트 설치의 해결 방법으로 다음을 수행합니다.

- ignoredisk --drives=.을 지정하여 파티션 설정에 사용되는 디스크를 제한합니다. OR --only-use=...
- 생성된 각 LVM 물리 볼륨에 사용할 디스크를 지정합니다. 파티션 pv.1 --ondisk=...

수동 설치를 위한 해결 방법으로 다음을 수행합니다.

- 그래픽 또는 텍스트 모드에서 수동 설치 중에 동일한 섹터 크기의 디스크만 선택합니다.
- 설치에 일관되지 않은 섹터 크기가 있는 디스크를 선택하면 각 LVM 볼륨 그룹이 동일한 섹터

크기의 물리 볼륨을 사용하도록 제한합니다. 이 작업은 사용자 지정 파티션 대화 상자의 그래픽 모드에서만 수행할 수 있습니다.

(BZ#1935722)

부팅 중에 초기 오류가 발생한 후 GRUB가 디스크에 액세스하도록 재시도합니다

SAN(Storage Area Networks)이 디스크 호출 열기 및 읽기 를 인식하지 못하는 경우가 있습니다. 이전에는 GRUB 도구를 사용하여 grub_rescue 프롬프트에 들어가 부팅에 실패했습니다. 이번 업데이트를 통해 GRUB는 초기 호출을 통해 디스크를 열고 읽은 후 최대 20회까지 디스크에 액세스하려고 시도합니다. 이러한 시도 후에도 GRUB 도구를 열거나 디스크를 읽을 수 없는 경우 grub_rescue 모드로 들어갑니다.

(BZ#1987087)

HASH MMU 모드가 있는 IBM Power 시스템은 메모리 할당 실패로 부팅되지 않음

HASH 메모리 할당 단위(MMU) 모드를 사용하는 IBM Power Systems는 최대 192개 코어까지 kdump 를 지원합니다. 그 결과 192개 이상의 코어에서 kdump 가 활성화된 경우 메모리 할당 실패로 시스템이 부팅되지 않았습니다. 이러한 제한은 HASH MMU 모드 초기 부팅 중에 RMA 메모리 할당으로 인해 발생합니다. 이 문제를 해결하려면 kdump 를 사용하는 대신 fadump 가 활성화된 Radix MMU 모드를 사용하십시오.

(BZ#2028361)

10.2. 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)

10.3. 인프라 서비스

FIPS 모드에서 Postfix TLS 지문 알고리즘은 SHA-256으로 변경해야 합니다.

기본적으로 RHEL 8에서 postfix 는 이전 버전과의 호환성을 위해 TLS와 MD5 지문을 사용합니다. 그러나 FIPS 모드에서 MD5 해싱 기능을 사용할 수 없으므로 기본 postfix 구성에서 TLS가 잘못 작동할 수 있습니다. 이 문제를 해결하려면 postfix 구성 파일에서 해시 기능을 SHA-256으로 변경해야 합니다.

자세한 내용은 MD5 대신 SHA-256으로 전환하여 FIPS 모드에서 관련 Knowledgebase 문서 Fix postfix TLS 를 참조하십시오.

(BZ#1711885)

10.4. 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 쉘의 적절한 설정과 함께 새로 구현된 runas_check_shell 옵션을 활성화하십시오. 이렇게 하면 공격자가 시스템 계정(예: bin)에서 명령을 실행하지 못합니다.

(BZ#1786990)

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** 컨테이너를처리합니다.

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

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

(BZ#1763210)

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 **1.0.0**과 일치하지 않습니다.

CIS 벤치마크의 문제로 인해 **/etc/passwd-** 백업 파일에 대한 권한을 보장하는 **SCAP** 규칙의 수정으로 인해 권한을 **0644** 로 구성합니다. 그러나 **CIS Red Hat Enterprise Linux 8** 벤치마크 **1.0.0** 에는 해당 파일에 대한 파일 권한 **0600** 이 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 **SELinux**를 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)

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)

SHA-1 서명이 있는 서버에 대한 연결이 GnuTLS에서 작동하지 않음

인증서의 SHA-1 서명은 GnuTLS 보안 통신 라이브러리에서 안전하지 않은 것으로 거부됩니다. 결과적으로 GnuTLS를 TLS 백엔드로 사용하는 애플리케이션은 이러한 인증서를 제공하는 피어에 TLS 연결을 설정할 수 없습니다. 이 동작은 다른 시스템 암호화 라이브러리와 일치하지 않습니다.

이 문제를 해결하려면 SHA-256 또는 더 강력한 해시로 서명된 인증서를 사용하거나 LEGACY 정책으로 전환하도록 서버를 업그레이드합니다.

(BZ#1628553)

Libreswan은 leftikeport 및 rightikeport 옵션을 무시합니다.

Libreswan은 호스트 간 Libreswan 연결에서 left ikeport 및 rightikeport 옵션을 무시합니다. 결과적으로 Libreswan은 leftikeport 및 rightikeport 설정에 관계없이 기본 포트를 사용합니다. 현재 해결방법은 없습니다.

(BZ#1934058)

IKEv2 와 함께 라벨이 지정된 여러 IPsec 연결을 사용할 수 없습니다.

Libreswan에서 IKEv2 프로토콜을 사용하는 경우 둘 이상의 연결에 대해 IPsec의 보안 레이블이 올바르게 작동하지 않습니다. 그 결과, 레이블이 지정된 IPsec을 사용하여 Libreswan은 첫 번째 연결만 설정할 수 있지만 후속 연결을 올바르게 설정할 수는 없습니다. 둘 이상의 연결을 사용하려면 IKEv1 프로토콜을 사용합니다.

(BZ#1934859)

FIPS 모드에서 OpenSSL은 특정 D-H 매개변수만 허용

FIPS 모드에서 OpenSSL을 사용하는 TLS 클라이언트는 잘못된 dh 값 오류를 반환하고 수동으로 생성된 매개 변수를 사용하는 서버에 대한 TLS 연결을 중단합니다. 이는 FIPS 140-2를 준수하도록 구성된 경우 OpenSSL이 NIST SP 800-56A rev3 부록 D (그룹 14, 15, 16, 17, 18 및 18 및 RFC 7919)에 정의된 그룹을 준수하는 Diffie-Hellman 매개변수에서만 작동하기 때문입니다. 또한 OpenSSL을 사용하는 서버는 다른 모든 매개 변수를 무시하고 대신 유사한 크기의 알려진 매개 변수를 선택합니다. 이 문제를 해결하려면 규정 준수 그룹만 사용하십시오.

(BZ#1810911)

OpenSC pkcs15-init 를 통한 스마트 카드 프로비저닝 프로세스가 제대로 작동하지 않음

file_caching 옵션은 기본 OpenSC 구성에서 활성화되며 파일 캐싱 기능이 pkcs15-init 도구의 일부 명령을 올바르게 처리하지 않습니다. 결과적으로 OpenSC를 통한 스마트 카드 프로비저닝 프로세스가 실패합니다.

이 문제를 해결하려면 /etc/opensc.conf 파일에 다음 코드 조각을 추가합니다.

```
app pkcs15-init {
        framework pkcs15 {
                use_file_caching = false;
        }
}
```

pkcs15-init 를 통한 스마트 카드 프로비저닝은 이전에 설명한 해결 방법을 적용한 경우에만 작동합니다.

(BZ#1947025)

systemd 는 임의의 경로에서 명령을 실행할 수 없습니다.

systemd 서비스는 SELinux 정책 패키지에 이러한 규칙을 포함하지 않기 때문에 /home/user/bin 임의 경로에서 명령을 실행할 수 없습니다. 결과적으로 비 시스템 경로에서 실행되는 사용자 지정 서비스가 실패하고 SELinux가 액세스를 거부하면 AVC(액세스 벡터 캐시) 거부 감사 메시지를 기록합니다. 이 문제를 해결하려면 다음 중 하나를 수행하십시오.

- 쉘 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)

selinux-policy 는 IPsec이 TCP를 통해 작동하지 않도록 방지합니다.

RHEL 8.4 의 libreswan 패키지는 TCP 캡슐화를 사용하는 IPsec 기반 VPN을 지원합니다. 그러나 selinux-policy 패키지에는 이 업데이트가 반영되지 않습니다. 결과적으로 Libreswan이 TCP를 사용하도록 설정하면 ipsec 서비스가 지정된 TCP 포트에 바인딩되지 않습니다.

이 문제를 해결하려면 사용자 지정 SELinux 정책을 사용하십시오.

1. 텍스트 편집기에서 new .cil 파일을 엽니다. 예를 들면 다음과 같습니다.

```
# vim local_ipsec_tcp_listen.cil
```

2. 다음 규칙을 삽입합니다.

```
(allow ipsec_t ipsecnat_port_t (tcp_socket (name_bind name_connect)))
```

3. 파일을 저장하고 종료합니다.

4. **policy** 모듈을 설치합니다.

```
# semodule -i local_ipsec_tcp_listen.cil
```

5. **ipsec** 서비스를 다시 시작하십시오.

```
# systemctl restart ipsec
```

결과적으로 **Libreswan**은 일반적으로 사용되는 **4500/tcp** 포트를 바인딩하고 연결할 수 있습니다.

(**BZ#1931848**)

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**)

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)** 프로필은 일부 파일 권한을 기본값보다 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)

킥스타트에서는 RHEL 8에서 com _redhat_oscap 대신 org_fedora _oscap 을 사용합니다.

Kickstart는 OSCAP(Open Security Content Automation Protocol) Anaconda 애드온을 com_redhat _oscap 대신 org_fedora _oscap 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 프로그램

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

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

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

(BZ#1674001)

OSCAP Anaconda 애드온 이 사용자 지정 프로파일을 올바르게 처리하지 않음

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

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

(BZ#1691305)

킥스타트 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 OpenSCAP은 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)

SELinux 감사 규칙 및 SELinux 부울 구성에서 충돌

감사 규칙 목록에 **subj_*** 또는 **obj_*** 필드가 포함된 감사 규칙과 **SELinux** 부울 구성이 변경되면 **SELinux** 부울 설정으로 인해 교착 상태가 발생합니다. 그 결과 시스템이 응답을 중지하고 복구를 위해 재부팅이 필요합니다. 이 문제를 해결하려면 **subj_*** 또는 **obj_*** 필드를 포함하는 모든 감사 규칙을 비활성화하거나 **SELinux** 부울을 변경하기 전에 이러한 규칙을 일시적으로 비활성화합니다.

RHSA-2021:2168 권고가 릴리스되면서 커널은 이 상황을 올바르게 처리하고 더 이상 교착 상태가 아닙니다.

(BZ#1924230)

10.5. 네트워킹

GRO를 비활성화할 때 IPsec 오프로딩 중에 IPsec 네트워크 트래픽이 실패합니다

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

이 문제를 해결하려면 장치에서 **GRO**를 사용하도록 유지합니다.

(BZ#1649647)

10.6. 커널

특정 BCC 유틸리티는 무해한 경고를 표시합니다.

일부 컴파일러 특정 커널 헤더의 매크로 재정의로 인해. 일부 BCC(BPF Compiler Collection) 유틸리티는 다음 경고를 표시합니다.

```
warning: __no_sanitize_address' macro redefined [-Wmacro-redefined]
```

경고는 무해하며 무시해도 됩니다.

(BZ#1907271)

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 8을 실행하는 IBM Power System의 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)

Kdump는 SSH 또는 NFS 덤프 대상에서 vmcore 덤프에 실패했습니다.

새 버전의 dracut-network 는 ipcalc 가 필요한 dhcp-client 에 종속 항목을 삭제합니다. 결과적으로 NIC 포트가 고정 IP로 구성되고 SSH 또는 NFS 덤프 대상에서 덤프하도록 kdump 가 구성되면 다음 오류

메시지가 표시되고 **kdump** 가 실패합니다.

```
ipcalc: command not found
```

이 문제를 해결하려면 다음을 수행합니다.

1. **ipcalc** 패키지를 수동으로 설치합니다.

```
dnf install ipcalc
```

2. **kdump** 에 사용할 **initramfs** 를 다시 빌드합니다.

```
kdumpctrl rebuild
```

3. **kdump** 서비스를 다시 시작합니다.

```
systemctl restart kdump
```

따라서 설명된 시나리오에서 **kdump** 가 성공합니다.

(BZ#1931266)

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)

부팅 시 크래시 커널의 메모리 할당이 실패합니다

일부 **Ampere Altra** 시스템에서 **BIOS** 설정에서 **32**비트 지역이 비활성화되면 메모리 할당이 실패합니다. 결과적으로 기존 메모리는 메모리 할당을 예약할 만큼 크지 않으므로 **kdump** 서비스가 시작되지 않습니다.

이 문제를 해결하려면 다음과 같이 **BIOS**에서 **32**비트 **CPU**를 활성화합니다.

1. 시스템에서 **BIOS** 설정을 엽니다.
2. 설정 메뉴 를 엽니다.
3. **Memory Configuration(**메모리 구성**)** 에서 **Slave 32**비트 옵션을 활성화합니다.

결과적으로 크래시 커널이 **32**비트 지역 내의 메모리를 할당하고 **kdump** 서비스가 예상대로 작동합니다.

(BZ#1940674)

특정 커널 드라이버가 버전을 표시하지 않음

RHEL 8.4에서는 많은 네트워킹 커널 드라이버의 모듈 버전 지정에 대한 동작이 변경되었습니다. 결과적으로 이러한 드라이버는 이제 버전을 표시하지 않습니다. 또는 **ethtool -i** 명령을 실행한 후 드라이버는 드라이버 버전 대신 커널 버전을 표시합니다. 이 문제를 해결하기 위해 사용자는 다음 명령을 실행할 수 있습니다.

```
# modinfo <AFFECTED_DRIVER> | grep rhelversion
```

결과적으로 사용자는 필요한 시나리오에서 영향을 받는 커널 드라이버 버전을 확인할 수 있습니다.

드라이버 버전 문자열의 변경 양은 드라이버 자체의 변화량에 대한 실제 고려 사항이 없다는 점에 유의하십시오.

(BZ#1944639)

irqpoll을 사용하면 **vmcore** 생성에 실패합니다.

AWS(Amazon Web Services) 클라우드 플랫폼에서 실행되는 **64**비트 **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 파일에 irqpoll 을 KDUMP_COMMANDLINE_REMOVE 에 추가합니다.

```
KDUMP_COMMANDLINE_REMOVE="hugepages hugepagesz slub_debug quiet
log_buf_len swiotlb"
```

2. /etc/sysconfig/kdump 파일의 KDUMP_COMMANDLINE_APPEND 에서 irqpoll 을 제거합니다.

```
KDUMP_COMMANDLINE_APPEND="irqpoll nr_cpus=1 reset_devices
cgroup_disable=memory udev.children-max=2 panic=10 swiotlb=noforce novmcoredd"
```

3. 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)

HP NMI 워치독이 항상 크래시 덤프를 생성하지는 않음

경우에 따라 HP NMI 워치독의 hpwdt 드라이버는 perfmon 드라이버에서 NMI(maskable interrupt)를 사용했기 때문에 HPE 워치독 타이머에서 생성한 NMI(NMI)를 요청할 수 없습니다.

누락된 NMI는 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 NMI를 보냅니다.

두 시퀀스 모두 시스템이 응답하지 않는 경우 일반적으로 발생합니다. 정상적인 상황에서 이러한 두 상

황에 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 않은 경우 그대로 유지됩니다. 이 시나리오를 수행하려면 **virtual Power**(가상 전원) 버튼을 사용하여 서버를 재설정하거나 전원을 켭니다.

두 번째 경우(**2.**) 누락된 **NMI**는 **AAS(Automated System Recovery)**에서 **9**초 후에 재설정됩니다.

HPE Gen9 Server 라인은 이 문제를 한 자리 숫자 비율로 경험합니다. **Gen10**은 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 2**소켓 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)

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 0x30000000-0x31ffffff] not
reserved in ACPI namespace
[    2.827911] acpi PNP0A08:00: ECAM at [mem 0x30000000-0x31ffffff] for [bus 00-1f]
```

그러나 커널이 **0x30000000-0x31ffff** 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 0x30000000-0x31ffffffffff ff in ACPI namespace"**는 시스템 부팅 솔루션 중에 표시됩니다.

(BZ#1868526)

기본 설정의 **hwloc** 명령은 단일 **CPU Power9** 및 **Power10 LPAR**에서 작동하지 않습니다.

버전 **2.2.0**의 **hwloc** 패키지를 사용하면 **Power9 / Power10 CPU**를 실행하는 단일 노드 **NUMA(Non-Uniform Memory Access)** 시스템은 **"비허용"**으로 간주됩니다. 결과적으로 모든 **hwloc** 명령이 작동하지 않고 다음 오류 메시지가 표시됩니다.

```
Topology does not contain any NUMA node, aborting!
```

이 두 가지 옵션 중 하나를 사용하여 이 문제를 해결할 수 있습니다.

- 환경 변수 **HWLOC_ALLOW=all**설정
- 다양한 **hwloc** 명령과 함께 비활성화된 플래그 사용

결과적으로 **hwloc** 명령은 설명된 시나리오에 오류를 반환하지 않습니다.

(BZ#1917560)

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, UCX는 여전히 MPI 단면 작업에 openib BTL을 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.

- **m ca btl openib 매개 변수는 openib BTL을 비활성화합니다.**
- **m ca pml ucx 매개 변수는 OPEN MPI를 구성하여 PM L을 사용합니다.**
- **x UCX_NET_DEVICES= 매개변수는 지정된 장치를 사용하도록 UCX를 제한합니다.**

OPEN MPI는 이기종 클러스터(다양한 하드웨어 및 소프트웨어 구성)를 통해 실행할 때 UCX를 기본 PML으로 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 매개변수를 사용하여 mpirun 명령을 실행합니다.**

```
-mca pml_ucx_priority 5
```

결과적으로 OPEN MPI 라이브러리는 UCX를 통해 사용 가능한 대체 전송 계층을 선택할 수 있습니다.

(BZ#1866402)

가상 머신에 가상 기능을 연결할 때 연결이 실패합니다

an ionic 장치 드라이버를 사용하는 Pensando 네트워크 카드는 VLAN 태그 구성 요청을 자동으로 수락하고VF(네트워크 가상 기능)를VM(가상 시스템)에 연결하는 동안 네트워크 연결을 구성합니다. 이 기능은 카드 펌웨어에서 아직 지원하지 않으므로 이러한 네트워크 연결이 실패합니다.

(BZ#1930576)

10.7. 하드웨어 활성화

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.

(JIRA:RHELPLAN-28940)

10.8. 파일 시스템 및 스토리지

/boot 파일 시스템을 LVM에 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 8에서는 시스템 *부팅 항목에 부트 로더 사양* (BLS)을 사용합니다. 이 사양을 사용하려면 플랫폼 펌웨어에서 /boot 파일 시스템을 읽을 수 있어야 합니다. EFI 시스템에서 플랫폼 펌웨어는 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 BLS와 같은 표준으로 인해 감소하기 때문에 Red Hat은 지원을 개선하지 않을 계획입니다.

Red Hat은 LVM에서 /boot 를 지원할 계획도 없습니다. 대신 Red Hat은 /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. LVM은 다른 블록 크기의 PV로 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_embeded_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.
- 씬 풀 또는 VDO와 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 변환을 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)

여러 할당량 유형이 지정된 경우 xfs_quota 상태가 모든 유에 시간을 출력하지 않습니다.

현재 xfs_quota state 명령은 여러 할당량 유형을 지정하는 옵션으로 예상되는 할당량의 유예 시간을 출력하지 않습니다. 이 문제를 해결하려면 명령에 필요한 할당량 유형을 개별적으로 지정합니다(예: xfs_quota state -g,xfs_quota state -p 또는 xfs_quota state -u).

(BZ#1949743)

10.9. 고가용성 및 클러스터

ocf: Heartbeat:pgsql 리소스 에이전트 및 중지 작업에서 crm_mon 출력을 구문 분석하는 타사 에이전트는 RHEL 8.4의 종료 프로세스 중에 중지되지 않을 수 있습니다.

RHEL 8.4 GA 릴리스에서 Pacemaker의 crm_mon 명령줄 툴은 Pacemaker가 종료되기 시작할 때 일반적인 클러스터 정보가 아니라 "종료" 메시지를 표시하도록 수정되었습니다. 결과적으로 리소스 중지와 같은 종료 진행 상황을 모니터링할 수 없으며 중지 작업(예 : resource-agents 패키지 또는 일부 사용자

지정 또는 타사 에이전트 와 같이) 중지 작업에서 **crm_mon** 출력을 구문 분석하는 리소스 에이전트가 중지되지 않아 클러스터 문제가 발생할 수 있었습니다.

z-stream을 사용할 수 있을 때까지 **ocf:eurbeat:pgsql** 리소스 에이전트를 사용하는 클러스터가 **RHEL 8.4**로 업그레이드되지 않는 것이 좋습니다.

(BZ#1948620)

10.10. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

getpwnam() 은 **32**비트 애플리케이션에 의해 호출될 때 실패할 수 있습니다.

NIS 사용자가 **getpwnam()** 함수를 호출하는 **32**비트 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.

RHEL 8.3이 **Apache APR(Apache Portable Runtime)** 라이브러리로 업데이트되므로 **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)

OQGraph 플러그인이 활성화된 경우 **MariaDB 10.5** 는 존재하지 않는 테이블을 삭제할 것을 경고하지 않습니다.

OQGraph 스토리지 엔진 플러그인이 **MariaDB 10.5** 서버에 로드되면 **MariaDB** 에서 존재하지 않는 테이블을 삭제할 것을 경고하지 않습니다. 특히 사용자가 **DROP TABLE** 또는 **DROP TABLE IF EXISTS SQL** 명령을 사용하여 존재하지 않는 테이블을 삭제하려고 하면 **MariaDB** 에서 오류 메시지를 반환하거나 경고를 기록하지 않습니다.

OQGraph 플러그인은 기본적으로 설치되지 않는 mariadb-oqgraph-engine 패키지에서 제공합니다.

(BZ#1944653)

PAM 플러그인 버전 1.0이 MariaDB에서 작동하지 않음

MariaDB 10.3 은 PAM(Pluggable Authentication Modules) 플러그인 버전 1.0을 제공합니다. MariaDB 10.5 는 플러그인 버전 1.0 및 2.0을 제공하며 버전 2.0은 기본값입니다.

MariaDB PAM 플러그인 버전 1.0은 RHEL 8에서 작동하지 않습니다. 이 문제를 해결하려면 mariadb:10.5 모듈 스트림에서 제공하는 PAM 플러그인 버전 2.0을 사용합니다.

MariaDB 10.5 는 PAM 플러그인 버전 2.0을 제공합니다. 참조하십시오.

(BZ#1942330)

Pyodbc 는 MariaDB 10.3에서 작동하지 않습니다.

pyodbc 모듈은 현재 RHEL 8.4 릴리스에 포함된 MariaDB 10.3 서버에서 작동하지 않습니다. 이전 버전의 MariaDB 10.3 서버와 MariaDB 10.5 서버는 이 문제의 영향을 받지 않습니다.

근본 원인은 mariadb-connector-odbc 패키지에 있으며 영향을 받는 패키지 버전은 다음과 같습니다.

- pyodbc-4.0.30
- mariadb-server-10.3.27
- mariadb-connector-odbc-3.0.7

(BZ#1944692)

10.11. 컴파일러 및 개발 도구

GCC 툴 세트 10: Valgrind, IBM z15 아키텍처 지원 오류 보고

Valgrind에서는 아직 특정 **IBM z15** 프로세서 기능을 지원하지 않지만 **GCC Toolset 10 Valgrind**의 버그로 인해 **z15** 지원 시스템에서 **z15** 지원이 보고됩니다. 그 결과 사용 가능한 경우 **z15** 기능을 사용하려는 소프트웨어는 **Valgrind**에서 실행할 수 없습니다. 이 문제를 해결하려면 **z15** 프로세서에서 실행할 때 **/usr/bin/valgrind**를 통해 액세스할 수 있는 **Valgrind**의 시스템 버전을 사용하십시오. 이 빌드는 **z15** 지원을 보고하지 않습니다.

(BZ#1937340)

PCP의 **pmproxy** 의 메모리 누수

pmproxy 서비스에는 **5.3.0** 이전의 **PCP(Performance Co-Pilot)** 버전에서 메모리 누수가 발생합니다. **RHEL 8.4**에서는 **PCP** 버전 **5.3.0**을 사용할 수 없으며 **RHEL 8**의 이전 마이너 버전은 사용할 수 없습니다. 결과적으로 **RHEL 8** 사용자는 예상보다 많은 메모리 사용량이 발생할 수 있습니다.

이 문제를 해결하려면 **pmproxy** 의 메모리 사용량을 제한합니다.

1. 다음 명령을 실행하여 **/etc/systemd/system/pmproxy.service.d/override.conf** 파일을 생성합니다.

```
# systemctl edit pmproxy
```

2. 다음 내용을 추가하여 **.conf**를 재정의 하고 변경 사항을 저장합니다.

```
[Service]
MemoryMax=10G
```

요구 사항에 따라 ***10G*** 값을 바꿉니다.

3. **pmproxy** 서비스를 다시 시작합니다.

```
# systemctl restart pmproxy
```

결과적으로 **pmproxy** 의 메모리 사용량이 지정된 제한에 도달하면 **pmproxy** 서비스가 다시 시작됩니다.

(BZ#1991659)

10.12. 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)

IdM 호스트의 /var/log/lastlog 스파스 파일에서 성능 문제가 발생할 수 있습니다.

IdM 설치 중에 총 10,000개의 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 줄어듭니다.

그러나 UID가 높으면 /var/log/lastlog 파일에 문제가 발생할 수 있습니다. 예를 들어 UID가 1280000008인 사용자가 IdM 클라이언트에 로그인하면 로컬 /var/log/lastlog 파일 크기가 거의 400GB로 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 400GB인 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)

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)

FIPS 모드는 공유 시크릿을 사용하여 **Pod** 간 신뢰성을 설정하는 것을 지원하지 않습니다.

NTLMSSP 인증은 **FIPS**와 호환되지 않기 때문에 공유 보안을 사용하여 포드 간 트러스트를 설정하는 것은 **FIPS** 모드에서 실패합니다. 이 문제를 해결하려면 **FIPS** 모드와 **AD** 도메인이 활성화된 **IdM** 도메인 간에 신뢰를 설정할 때 **AD(Active Directory)** 관리 계정으로 인증합니다.

(BZ#1924707)

버전 **1.2.2**로 업데이트한 후 **authselect** 를 다운그레이드하면 시스템 인증이 중단됩니다.

authselect 패키지가 최신 업스트림 버전 **1.2.2** 로 다시 기반되었습니다. **authselect** 를 다운그레이드하는 것은 지원되지 않으며 **root** 를 포함한 모든 사용자의 시스템 인증이 중단됩니다.

authselect 패키지를 **1.2.1** 이하로 다운 그레이드한 경우 다음 단계를 수행하여 이 문제를 해결하십시오.

1. **GRUB** 부팅 화면에서 부팅하려는 커널 버전이 있는 **Red Hat Enterprise Linux** 를 선택하고 **e** 키를 눌러 항목을 편집합니다.

2.

linux 로 시작하는 행의 끝에 **single**을 별도의 단어로 입력하고 **Ctrl+x** 를 눌러 부팅 프로세스를 시작합니다.

3. 단일 사용자 모드에서 부팅할 때 루트 암호를 입력합니다.

4. 다음 명령을 사용하여 **authselect** 구성을 복원합니다.

```
# authselect select sssd --force
```

(BZ#1892761)

pki-ca 패키지 버전이 **10.10.5** 이전인 경우 **RHEL 8.3**에서 **RHEL 8.4**로 **IdM** 서버를 업그레이드할 수 없습니다.

pki -ca 패키지 버전이 **10.10.5** 이전인 경우 **IdM** 서버 업그레이드 프로그램인 **ipa- server-upgrade** 가 실패합니다. 필수 파일이 이러한 버전에 존재하지 않기 때문에 패키지 설치 시 및 **ipa-server-upgrade** 또는 **ipa ctl** 이 실행될 때 **IdM** 서버 업그레이드가 성공적으로 완료되지 않습니다.

이 문제를 해결하려면 **pki-*** 패키지를 버전 **10.10.5** 이상으로 업그레이드하고 **ipa-server-upgrade** 명령을 다시 실행합니다.

(BZ#1957768)

10.13. 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 8을 게스트 운영 체제로 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)

10.14. 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 rpming 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 Z에서 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 Vul¢ API를 지원하지 않습니다.

하드웨어 가속 또는 ARM을 사용하려면 독점형 Nvidia 드라이버를 설치합니다.

(JIRA:RHELPLAN-57914)

ESXi의 GUI가 낮은 비디오 메모리로 인해 충돌할 수 있습니다.

vCenter Server 7.0.1을 사용하는 VMware ESXi 7.0.1 하이퍼바이저의 RHEL 가상 시스템(VM)의 GUI(그래픽 사용자 인터페이스)에는 특정 양의 비디오 메모리가 필요합니다. VM에 여러 콘솔 또는 고해상도 모니터를 연결하는 경우 GUI에는 최소 16MB의 비디오 메모리가 필요합니다. 더 적은 비디오 메모리로 GUI를 시작하면 GUI가 예기치 않게 종료될 수 있습니다.

문제를 해결하려면 하이퍼바이저를 구성하여 VM에 최소 16MB 이상의 비디오 메모리를 할당하도록 구성합니다. 결과적으로 VM의 GUI가 더 이상 충돌하지 않습니다.

(BZ#1910358)

10.15. 가상화

virsh iface-* 명령이 일관되게 작동하지 않음

현재 virsh iface- start 및 virsh iface- destroy와 같은 virsh iface- * 명령은 구성 종속성으로 인해 실패하는 경우가 많습니다. 따라서 호스트 네트워크 연결을 구성하고 관리하는 데 virsh iface-* 명령을 사용하지 않는 것이 좋습니다. 대신 NetworkManager 프로그램과 관련 관리 애플리케이션을 사용합니다.

(BZ#1664592)

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 1.0에서 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)

IBM POWER Systems에서 **perf kvm** 레코드 를 사용하면 **VM**이 충돌할 수 있습니다.

little-endian 변형 **IBM POWER** 하드웨어에서 **RHEL 8** 호스트를 사용하는 경우 **perf kvm record** 명령을 사용하여 **KVM** 가상 시스템(**VM**)에 대한 추적 이벤트 샘플을 수집하면 **VM**이 응답하지 않습니다. 이러한 상황은 다음과 같은 경우 발생합니다.

- **perf** 유틸리티는 권한이 없는 사용자가 사용하며 **-p** 옵션은 **VM**(예: **perf kvm record -e trace_cycles -p 12345**)을 식별하는 데 사용됩니다.
- **VM**은 **virsh** 쉘을 사용하기 시작했습니다.

이 문제를 해결하려면 **perf kvm** 유틸리티를 **-i** 옵션과 함께 사용하여 **virsh** 쉘을 사용하여 생성된 **VM**을 모니터링합니다. 예를 들면 다음과 같습니다.

```
# perf kvm record -e trace_imc/trace_cycles/  -p <guest pid> -i
```

i 옵션을 사용하면 하위 작업은 카운터를 상속하지 않으므로 스레드를 모니터링하지 않습니다.

(BZ#1924016)

RHEL 7-ALT 호스트에서 RHEL 8로 POWER9 게스트 마이그레이션에 실패

현재 POWER9 가상 시스템을 RHEL 7-ALT 호스트 시스템에서 RHEL 8로 마이그레이션하는 것은 마이그레이션 상태: active 상태로 응답하지 않습니다.

이 문제를 해결하려면 RHEL 7-ALT 호스트에서 THP(투명한 대규모 페이지)를 비활성화하여 마이그레이션을 성공적으로 완료할 수 있습니다.

(BZ#1741436)

virt-customize 를 사용하면 guestfs-firstboot 가 실패하는 경우가 있습니다.

virt-customize 유틸리티를 사용하여 VM(가상 시스템) 디스크 이미지를 수정한 후 잘못된 SELinux 권한으로 인해 guestfs-firstboot 서비스가 실패합니다. 이로 인해 VM을 시작하는 동안 사용자 생성 실패 또는 시스템 등록 실패와 같은 다양한 문제가 발생합니다.

이 문제를 방지하려면 virt -customize로 디스크 이미지를 수정한 후 VM의 커널 명령줄에 --selinux-relabel 을 추가합니다.

(BZ#1554735)

IBM POWER에서 시작하지 않는 가상 머신 with iommu_platform=on

RHEL 8에서는 현재 IBM POWER 시스템의 VM(가상 머신)에 대한 iommu_platform=on 매개 변수를 지원하지 않습니다. 결과적으로 IBM POWER 하드웨어에서 이 매개 변수로 VM을 시작하면 부팅 프로세스 중에 VM이 응답하지 않습니다.

(BZ#1910848)

AMD EPYC에서 호스트 패스스루 모드를 사용할 때 VM에서 SMT CPU 토폴로지를 감지하지 않습니다.

AMD EPYC 호스트에서 CPU 호스트 패스스루 모드로 부팅되는 VM(가상 머신)이 부팅되면 CPU O EXT CPU 기능 플래그가 표시되지 않습니다. 결과적으로 VM은 코어당 여러 스레드가 있는 가상 CPU 토

폴로지를 탐지할 수 없습니다. 이 문제를 해결하려면 호스트 통과 대신 EPYC CPU 모델로 VM을 부팅합니다.

(BZ#1740002)

Hyper-V가 활성화된 Windows Server 2016 가상 머신이 특정 CPU 모델을 사용할 때 부팅되지 않음

현재 Windows Server 2016을 게스트 운영 체제로 사용하고 Hyper-V 역할이 활성화되어 다음 CPU 모델 중 하나를 사용하는 VM(가상 머신)을 부팅할 수 없습니다.

- EPYC-IBPB
- EPYC

이 문제를 해결하려면 EPYC-v3 CPU 모델을 사용하거나 VM에 대해 xsaves CPU 플래그를 수동으로 활성화합니다.

(BZ#1942888)

가상 머신에서 macvtap 인터페이스를 삭제하면 모든 macvtap 연결이 재설정됩니다.

현재 여러 macvtap 장치가 있는 실행 중인 VM(가상 시스템)에서 macvtap 인터페이스를 삭제하면 다른 macvtap 인터페이스의 연결 설정도 재설정됩니다. 결과적으로 VM에 네트워크 문제가 발생할 수 있습니다.

(BZ#1332758)

PowerVM에서 IBMVFC 장치 핫플러그에 실패

PowerVM 하이퍼바이저에서 RHEL 8 게스트 운영 체제와 함께 VM(가상 머신)을 사용하는 경우 현재 실행 중인 VM에서 IBM Power Virtual Fibre Channel(IBMVFC) 장치를 제거하려고 합니다. 대신 탁월한 번역 오류가 표시됩니다.

이 문제를 해결하려면 VM이 종료되면 IBMVFC 장치를 제거합니다.

(BZ#1959020)

ibmvfc 드라이버를 사용할 때 **IBM POWER** 호스트가 충돌할 수 있습니다.

LPAR(PowerVM 논리 파티션)에서 **RHEL 8**을 실행할 때 현재 **ibmvfc** 드라이버에 문제가 있어 다양한 오류가 발생할 수 있습니다. 결과적으로 호스트의 커널은 다음과 같은 특정 상황에서 패닉될 수 있습니다.

- **LPM(Live Partition Mobility)** 기능 사용
- 호스트 어댑터 재설정
- **SCSI** 오류 처리 **(SCSI EH)** 기능 사용

(BZ#1961722)

RHEL 8 게스트의 특정 상황에서 **virtiofs** 디렉토리 마운트 실패

현재 **virtiofs** 기능을 사용하여 **VM(**가상 머신)에 호스트 디렉터리를 제공할 때 **VM**에서 디렉터리를 마운트할 때 **VM**에서 **RHEL 8.4 (**또는 이전) 커널을 사용 중이지만 **RHEL 8.5 (**이상) **selinux-policy** 패키지를 사용하는 경우 **"Operation not supported"** 오류와 함께 실패합니다.

이 문제를 해결하려면 게스트를 재부팅하고 게스트의 사용 가능한 최신 커널로 부팅합니다.

(BZ#1995558)

10.16. 클라우드 환경의 RHEL

Kdump가 **Azure** 및 **Hyper-V**에서 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 DHCP로 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)

nm-cloud-setup 유틸리티는 Microsoft Azure에 잘못된 기본 경로를 설정합니다.

Microsoft Azure에서 nm-cloud-setup 유틸리티는 클라우드 환경의 올바른 게이트웨이를 감지하지 못합니다. 결과적으로 유틸리티는 잘못된 기본 경로를 설정하고 연결을 끊습니다. 현재 해결방법은 없습니다.

(BZ#1912236)

여러 게스트 디스크로 Hyper-V VM을 부팅할 때 SCSI 호스트 주소가 변경될 수 있습니다.

현재 Hyper-V 하이퍼바이저에서 RHEL 8 가상 머신(VM)을 부팅할 때 일부 경우 호스트 , *버스*, *대상*, *LBTL(Lun) SCSI 주소의 호스트* 부분이 변경됩니다. 결과적으로 VM의 HBTL SCSI 식별 또는 장치 노드로 설정된 자동화된 작업이 일관적으로 작동하지 않습니다. VM에 디스크가 두 개 이상 있거나 디스크에 크기가 다른 경우 발생합니다.

문제를 해결하려면 다음 방법 중 하나를 사용하여 킥스타트 파일을 수정하십시오.

방법 1: SCSI 장치에 대한 영구 식별자를 사용합니다.

예를 들어 다음 powershell 스크립트를 사용하여 특정 장치 식별자를 확인할 수 있습니다.

```
# Output what the /dev/disk/by-id/<value> for the specified hyper-v virtual disk.
# Takes a single parameter which is the virtual disk file.
# Note: kickstart syntax works with and without the /dev/ prefix.
param (
    [Parameter(Mandatory=$true)][string]$virtualdisk
)

$what = Get-VHD -Path $virtualdisk
$part = $what.DiskIdentifier.ToLower().split('-')

$p = $part[0]
$s0 = $p[6] + $p[7] + $p[4] + $p[5] + $p[2] + $p[3] + $p[0] + $p[1]

$p = $part[1]
$s1 =  $p[2] + $p[3] + $p[0] + $p[1]

[string]::format("/dev/disk/by-id/wwn-0x60022480{0}{1}{2}", $s0, $s1, $part[4])
```

다음과 같이 hyper-v 호스트에서 이 스크립트를 사용할 수 있습니다.

```
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_8.vhdx
/dev/disk/by-id/wwn-0x60022480e00bc367d7fd902e8bf0d3b4
PS C:\Users\Public\Documents\Hyper-V\Virtual hard disks> .\by-id.ps1 .\Testing_8\disk_3_9.vhdx
/dev/disk/by-id/wwn-0x600224807270e09717645b1890f8a9a2
```

나중에 디스크 값은 다음과 같이 kickstart 파일에서 사용할 수 있습니다.

```
part / --fstype=xfs --grow --asprimary --size=8192 --ondisk=/dev/disk/by-id/wwn-
0x600224807270e09717645b1890f8a9a2
part /home --fstype="xfs" --grow --ondisk=/dev/disk/by-id/wwn-
0x60022480e00bc367d7fd902e8bf0d3b4
```

이러한 값은 각 가상 디스크에 고유하므로 각 VM 인스턴스에 대해 구성을 수행해야 합니다. 따라서 %include 구문을 사용하여 디스크 정보를 별도의 파일에 배치하는 것이 유용할 수 있습니다.

방법 2: 장치 선택을 크기별로 설정합니다.

크기를 기반으로 디스크 선택을 구성하는 킥스타트 파일에 다음과 유사한 행이 포함되어야 합니다.

```
...

# Disk partitioning information is supplied in a file to kick start
%include /tmp/disks

...

# Partition information is created during install using the %pre section
%pre --interpreter /bin/bash --log /tmp/ks_pre.log

 # Dump whole SCSI/IDE disks out sorted from smallest to largest ouputting
 # just the name
 disks=(`lsblk -n -o NAME -l -b -x SIZE -d -I 8,3`) || exit 1

 # We are assuming we have 3 disks which will be used
 # and we will create some variables to represent
 d0=${disks[0]}
 d1=${disks[1]}
 d2=${disks[2]}

 echo "part /home --fstype="xfs" --ondisk=$d2 --grow" >> /tmp/disks
 echo "part swap --fstype="swap" --ondisk=$d0 --size=4096" >> /tmp/disks
 echo "part / --fstype="xfs" --ondisk=$d1 --grow" >> /tmp/disks
 echo "part /boot --fstype="xfs" --ondisk=$d1 --size=1024" >> /tmp/disks

%end
```

(BZ#1906870)

RHEL 8 가상 머신은 **AWS ARM64** 인스턴스에서 네트워크 성능이 낮습니다.

AWS(Amazon Web Services) ARM64 인스턴스에서 실행되는 **VM**(가상 머신)에서 **RHEL 8**을 게스트 운영 체제로 사용하는 경우, **iommu.strict=1** 커널 매개 변수를 사용하거나 **no iommu.strict** 매개 변수를 정의할 때 **VM**은 예상 네트워크 성능보다 낮습니다.

이 문제를 해결하려면 매개 변수를 **to iommu.strict=0** 으로 변경합니다. 그러나 **VM**의 보안도 줄일 수 있습니다.

(BZ#1836058)

FIPS 모드가 활성화된 경우 **RHEL 8** 게스트 최대 절전 실패

현재 **VM**이 **FIPS** 모드를 사용하는 경우 **RHEL 8**을 게스트 운영 체제로 사용하는 **VM**(가상 머신)을 최대 절전 모드로 설정할 수 없습니다.

(BZ#1934033, BZ#1944636)

백업 AMI에서 생성된 EC2 인스턴스에서 SSH 키가 올바르게 생성되지 않습니다.

현재 백업 AMI(Amazon Machine Image)에서 RHEL 8의 새 Amazon EC2 인스턴스를 만들 때 cloud-init 는 VM에서 기존 SSH 키를 삭제하지만 새 SSH 키를 생성하지 않습니다. 따라서 경우에 따라 VM을 호스트에 연결할 수 없습니다.

이 문제를 해결하려면 cloud.cgf 파일을 편집하고 "ssh_genkeytypes: ~" 행을 ssh_genkeytypes: ['rsa', 'ecdsa', 'ed25519'] 로 변경합니다.

이렇게 하면 설명된 환경에서 RHEL 8 VM을 프로비저닝할 때 SSH 키를 올바르게 삭제하고 생성할 수 있습니다.

(BZ#1957532)

백업 AMI에서 생성된 EC2 인스턴스에서 SSH 키가 올바르게 생성되지 않습니다.

현재 백업 AMI(Amazon Machine Image)에서 RHEL 8의 새 Amazon EC2 인스턴스를 만들 때 cloud-init 는 VM에서 기존 SSH 키를 삭제하지만 새 SSH 키를 생성하지 않습니다. 따라서 경우에 따라 VM을 호스트에 연결할 수 없습니다.

이 문제를 해결하려면 cloud.cgf 파일을 편집하고 "ssh_genkeytypes: ~" 행을 ssh_genkeytypes: ['rsa', 'ecdsa', 'ed25519'] 로 변경합니다.

이렇게 하면 설명된 환경에서 RHEL 8 VM을 프로비저닝할 때 SSH 키를 올바르게 삭제하고 생성할 수 있습니다.

(BZ#1963981)

10.17. 지원 관련 기능

redhat-support-tool 이 FUTURE 암호화 정책에서 작동하지 않음

고객 포털 API의 인증서에서 사용하는 암호화 키가 FUTURE 시스템 전체 암호화 정책의 요구 사항을 충족하지 않으므로 redhat-support-tool 유틸리티는 현재 이 정책 수준에서 작동하지 않습니다.

이 문제를 해결하려면 고객 포털 API에 연결하는 동안 DEFAULT 암호화 정책을 사용하십시오.

(BZ#1802026)

11장. 국제화

11.1. 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

11.2. RHEL 8 국제화의 주요 변경 사항

RHEL 8에서는 RHEL 7에 비해 국제화에 다음과 같은 변경 사항이 추가되었습니다.

- 유니코드 11 컴퓨팅 업계 표준에 대한 지원이 추가되었습니다.
- 국제화는 여러 패키지로 배포되므로 설치 공간을 더 적게 설치할 수 있습니다. 자세한 내용은 langpacks 사용을 참조하십시오.
- 다수의 glibc 로케일이 Unicode Common Locale Data Repository(CLDR)와 동기화되었습니다.

부록 A. 구성 요소별 티켓 목록

Bugzilla 및 JIRA ID는 참조를 위해 이 문서에 나열되어 있습니다. 공개적으로 액세스할 수 있는 Bugzilla 버그에는 티켓 링크가 포함되어 있습니다.

구성 요소	티켓
389-ds-base	BZ#1859301, BZ#1862529, BZ#1859218, BZ#1850275, BZ#1851975
KVM 하이퍼바이저	JIRA:RHELPLAN-44450
NetworkManager	BZ#1900260, BZ#1878783, BZ#1766944, BZ#1912236
OpenIPMI	BZ#1796588
SLOF	BZ#1910848
accel-config	BZ#1843266
anaconda	BZ#1890009, BZ#1874394, BZ#1642391, BZ#1609325, BZ#1854307, BZ#1821192, BZ#1822880,BZ#1914955, BZ#1847681, BZ#1903786,BZ#1931069, BZ#1954408, BZ#1897657
apr	BZ#1819607
authselect	BZ#1892761
bcc	BZ#1879411
bind	BZ#1876492, BZ#1882040, BZ#1854148
bpftrace	BZ#1879413
clevis	BZ#1887836, BZ#1853651
cloud-init	BZ#1886430, BZ#1750862, BZ#1957532, BZ#1963981
cmake	BZ#1816874
cockpit	BZ#1666722
corosync-qdevice	BZ#1784200
Corosync	BZ#1870449
createrepo_c	BZ#1795936, BZ#1894361

구성 요소	티켓
crun	BZ#1841438
crypto-policies	BZ#1919155, BZ#1660839
dhcp	BZ#1883999
distribution	BZ#1877430, BZ#1855776, BZ#1855781, BZ#1657927
dnf	BZ#1865803, BZ#1807446, BZ#1698145
문제 해결	BZ#1903566
dyninst	BZ#1892001, BZ#1892007
edk2	BZ#1935497
elfutils	BZ#1875318, BZ#1879758
fapolicyd	BZ#1940289, BZ#1896875, BZ#1887451
fence-agents	BZ#1775847
freeipmi	BZ#1861627
freeradius	BZ#1723362
gcc	BZ#1868446, BZ#1821994, BZ#1850498, BZ#1656139, BZ#1891998
gdb	BZ#1853140
Ghostscript	BZ#1874523
glibc	BZ#1868106,BZ#1871397,BZ#1880670, BZ#1882466, BZ#1871396,BZ#1893662, BZ#1817513, BZ#1871385,BZ#1871387,BZ#1871395
gnome-shell-extensions	BZ#1717947
gnome-software	BZ#1668760
gnutls	BZ#1628553
go-toolset	BZ#1870531

구성 요소	티켓
grafana-container	BZ#1916154
grafana-pcp	BZ#1845592, BZ#1854093
grafana	BZ#1850471
grub2	BZ#1583445
httpd	BZ#1869576, BZ#1883648
hwloc	BZ#1841354, BZ#1917560
ima-evm-utils	BZ#1868683
ipa	BZ#1891056,BZ#1340463,BZ#1816784,BZ#1924707,BZ#1664719,BZ#1664718
iproute	BZ#1849815
iptraf-ng	BZ#1842690, BZ#1906097
jmc	BZ#1919283
kernel-rt	BZ#1858099
kernel	BZ#1806882, BZ#1846838, BZ#1884857, BZ#1876527, BZ#1660290, BZ#1885850, BZ#1649647, BZ#1838876, BZ#1871246, BZ#1893882, BZ#1876519, BZ#1860031, BZ#1844416, BZ#1780258, BZ#1851933, BZ#1885406, BZ#1867490, BZ#1908893, BZ#1919745, BZ#1867910, BZ#1887940, BZ#1874005, BZ#1871214, BZ#1622041, BZ#1533270, BZ#1900674, BZ#1869758, BZ#1861261, BZ#1848427, BZ#1847567, BZ#1844157, BZ#1844111, BZ#1811839, BZ#1877019, BZ#1548297, BZ#1844086, BZ#1839055, BZ#1905088, BZ#1882620, BZ#1784246, BZ#1916583, BZ#1924230, BZ#1793389, BZ#1944639, BZ#1694705, BZ#1748451, BZ#1654962, BZ#1708456, BZ#1812577, BZ#1666538, BZ#1602962, BZ#1609288, BZ#1730502, BZ#1865745, BZ#1868526, BZ#1910358, BZ#1924016, BZ#1906870, BZ#1940674, BZ#1930576, BZ#1907271, BZ#1942888, BZ#1836058, BZ#1934033, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1570255, BZ#1814836, BZ#1696451, BZ#1348508, BZ#1839311, BZ#1783396, JIRA:RHELPLAN-57712, BZ#1837187, BZ#1904496, BZ#1660337, BZ#1665295, BZ#1569610
kexec-tools	BZ#1844941, BZ#1931266, BZ#1854037
kmod-redhat-oracleasm	BZ#1827015

구성 요소	티켓
kpatch	BZ#1798711
krb5	BZ#1877991
libbpf	BZ#1919345
libgnome-keyring	BZ#1607766
libguestfs	BZ#1554735
libmpc	BZ#1835193
libpcap	BZ#1743650
libpwquality	BZ#1537240
libreswan	BZ#1891128, BZ#1372050, BZ#1025061, BZ#1934058, BZ#1934859
libselinux-python-2.8-module	BZ#1666328
libselinux	BZ#1879368
libsemanage	BZ#1913224
libvirt	BZ#1664592, BZ#1332758, BZ#1528684
libvpd	BZ#1844429
llvm-toolset	BZ#1892716
lvm2	BZ#1496229, BZ#1768536
mariadb-connector-odbc	BZ#1944692
mariadb	BZ#1936842, BZ#1944653, BZ#1942330
Mesa	BZ#1886147
micropipenv	BZ#1849096
mod_fcgid	BZ#1876525
mod_security	BZ#1824859

구성 요소	티켓
mutter	BZ#1886034
mysql-selinux	BZ#1895021
net-snmp	BZ#1817190
nfs-utils	BZ#1592011
nispor	BZ#1848817
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1817533, BZ#1645153
opal-prd	BZ#1844427
opencryptoki	BZ#1847433
opencv	BZ#1886310
openmpi	BZ#1866402
opensc	BZ#1877973, BZ#1947025
openscap	BZ#1824152, BZ#1887794, BZ#1840579
openssl	BZ#1810911
osbuild-composer	BZ#1951964
oscap-anaconda-addon	BZ#1843932, BZ#1665082, BZ#1674001, BZ#1691305, BZ#1834716
p11-kit	BZ#1887853
pacemaker	BZ#1371576, BZ#1948620
pcp-container	BZ#1916155
pcp	BZ#1854035, BZ#1847808

구성 요소	티켓
pcs	BZ#1869399, BZ#1741056,BZ#1667066,BZ#1667061,BZ#1457314,BZ#1839637, BZ#1619620, BZ#1851335
perl-IO-String	BZ#1890998
perl-Time-HiRes	BZ#1895852
pki-core	BZ#1868233, BZ#1729215
podman	BZ#1734854, BZ#1881894, BZ#1932083
policycoreutils	BZ#1868717, BZ#1926386
popt	BZ#1843787
postfix	BZ#1688389, BZ#1711885
powerpc-utils	BZ#1853297
py3c	BZ#1841060
pyOpenSSL	BZ#1629914
pykickstart	BZ#1637872
pyodbc	BZ#1881490
python-PyMySQL	BZ#1820628
python-blivet	BZ#1656485
qemu-kvm	BZ#1790620, BZ#1719687, BZ#1860743, BZ#1740002, BZ#1651994
할당량	BZ#1868671
교체	BZ#1729499, BZ#1898080, BZ#1832394
redhat-support-tool	BZ#1802026
Redis	BZ#1862063
resource-agents	BZ#1471182

구성 요소	티켓
rhel-system-roles	BZ#1865990,BZ#1926947,BZ#1889484,BZ#1927943,BZ#1893712,BZ#1893743,BZ#1893906,BZ#1893908,BZ#1895188,BZ#1893696,BZ#1893699,BZ#1889893,BZ#1893961
rpm	BZ#1834931, BZ#1923167, BZ#1688849
rshim	BZ#1744737
rsyslog	BZ#1869874, JIRA:RHELPLAN-10431, BZ#1679512
rust-toolset	BZ#1896712
samba	BZ#1878109, JIRA:RHELPLAN-13195
scap-security-guide	BZ#1889344,BZ#1927019,BZ#1918742,BZ#1778188,BZ#1843913,BZ#1858866,BZ#1750755
scap-workbench	BZ#1877522
selinux-policy	BZ#1889673, BZ#1860443, BZ#1931848, BZ#1461914
sendmail	BZ#1868041
setroubleshoot	BZ#1875290, BZ#1794807
skopeo	BZ#1940854
sos	BZ#1966838
spamassassin	BZ#1822388
spice	BZ#1849563
sssd	BZ#1819012,BZ#1884196,BZ#1884213,BZ#1784459,BZ#1893698,BZ#1881992
stalld	BZ#1875037
stratisd	BZ#1798244, BZ#1868100
subscription-manager	BZ#1905398
subversion	BZ#1844947

구성 요소	티켓
sudo	BZ#1786990
swig	BZ#1853639
systemd	BZ#1827462
systemtap	BZ#1875341
tang-container	BZ#1913310
Tang	BZ#1828558
texlive	BZ#1889802
tpm2-abrmd	BZ#1855177
tuned	BZ#1874052
udica	BZ#1763210
unbound	BZ#1850460
usbguard	BZ#1887448, BZ#1940060
valgrind	BZ#1504123, BZ#1937340
virtio-win	BZ#1861229
Wayland	BZ#1673073
xdp-tools	BZ#1880268
xfsprogs	BZ#1949743
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1698565

구성 요소	티켓
기타	BZ#1839151,BZ#1780124, JIRA:RHELPLAN-59941, JIRA:RHELPLAN-59938, JIRA:RHELPLAN-59950, BZ#1952421, JIRA:RHELPLAN-37817, BZ#1918055, JIRA:RHELPLAN-56664, JIRA:RHELPLAN-56661, JIRA:RHELPLAN-39843, BZ#1925192, JIRA:RHELPLAN-73418, JIRA:RHELPLAN-63081, BZ#1935686, BZ#1634655, JIRA:RHELPLAN-56782, JIRA:RHELPLAN-72660, JIRA:RHELPLAN-72994, JIRA:RHELPLAN-37579, BZ#1952161, BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, JIRA:RHELPLAN-59111, BZ#1757877, BZ#1777138, JIRA:RHELPLAN-27987, JIRA:RHELPLAN-28940, JIRA:RHELPLAN-34199, JIRA:RHELPLAN-57914, BZ#1897383, BZ#1741436, BZ#1971061, JIRA:RHELPLAN-58629, BZ#1960412, BZ#1959020, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1889737,BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, JIRA:RHELPLAN-27737, JIRA:RHELPLAN-56659, BZ#1906489,BZ#1957316,BZ#1960043, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1932222,BZ#1686057,BZ#1748980, JIRA:RHELPLAN-71200, BZ#1827628, JIRA:RHELPLAN-45858, BZ#1871025,BZ#1871953, BZ#1874892, BZ#1893767, BZ#1916296, BZ#1926114, BZ#1904251, JIRA:RHELPLAN-59825, BZ#1920624, JIRA:RHELPLAN-70700, BZ#1929173

부록 B. 개정 내역

0.2-4

Thu Jun 09, Lucie Vanowkové (lmanasko@redhat.com)

- 새 기능 BZ#1996076 (Identity Management)이 추가되었습니다.

0.2-3

4월 29일, LRKKKKKKKK (lspackova@redhat.com)

- 더 이상 사용되지 않는 기능 소개가 업데이트되었습니다.
- BZ#1605216 의 고정 오타.
- 손상된 링크가 수정되었습니다.

0.2-2

Thu Mar 24 2022, Jaroslav Klech (jklech@redhat.com)

- 버그 수정 BZ#1947839 (Kernel)가 추가되었습니다.

0.2-1

Mon Mar 21 2022, Jaroslav Klech (jklech@redhat.com)

- 알려진 문제(커널)를 삭제했습니다.

0.2-0

2022년 2월 04일 Jaroslav Klech (jklech@redhat.commailto:jklech@redhat.com)

- 더 이상 사용되지 않는 기능 BZ#1871863 (Hardware Support)을 추가했습니다.

- 더 이상 사용되지 않는 패키지가 업데이트되었습니다.

- 더 이상 사용되지 않는 기능 BZ#1794513 (Filesystems 및 스토리지)이 추가되었습니다.

0.1-9

Thu January 20 2022, Lucie MaskovECDHE(lmanasko@redhat.com)

- 알려진 문제 BZ#2028361 (Installer 및 image creation)이 추가되었습니다.

0.1-8

2021년 12월 23일 목요일, 기니카 -파파산라(lspackova@redhat.com)

- soft-RoCE 드라이버인 rdma_rxe 에 대한 정보가 기술 프리뷰 BZ#1605216 및 더 이상 사용되지 않는 기능 BZ#1878207 (커널)에 추가되었습니다.

0.1-7

2021년 12월 22일 - 2021년 12월 22일, Valka -pa¢á(lspackova@redhat.com)

- 개선된 BZ#2005431 (보안)이 추가되었습니다.

- 더 이상 사용되지 않는 패키지가 업데이트되었습니다.

0.1-6

2021년 10월 29일, Jaroslav Klech(jklech@redhat.com)

- fw_devlink 매개 변수를 업데이트했습니다(외부 커널 매개 변수의 중요한 변경 사항).

0.1-5

2021년 10월 07일, 룰카 -파파산라(lspackova@redhat.com)

- 알려진 문제 BZ#1942330 (동적 프로그래밍 언어, 웹 및 데이터베이스 서버) 업데이트.

0.1-4

2021년 10월 5일 화요일, Lucie Maás¢(lmanasko@redhat.com)

- 더 이상 사용되지 않는 기능 BZ#1999620 (Shells 및 명령줄 툴)이 추가되었습니다.

0.1-3

2021년 9월 17일 금요일, Lucie Maásá(lmanasko@redhat.com)

- 알려진 문제 BZ#1987087 (설치자)이 추가되었습니다.

0.1-2

2021년 9월 07일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- 알려진 문제 BZ#1961722 (가상화) 업데이트.

0.1-1

2021년 9월 3일 금요일, 기니카 -파파산라(lspackova@redhat.com)

- 알려진 문제 BZ#1995558 (가상화) 업데이트.

0.1-0

2021년 8월 30일, 종료될 예정인 카메라 파파사라(lspackova@redhat.com)

- 알려진 문제 BZ#1995558 (가상화) 추가.
- 버그 수정 BZ#1940854 (컨테이너)가 추가되었습니다.

0.0-9

2021년 8월 20일 금요일, Lucie Maásá(lmanasko@redhat.com)

- YUM/DNF를 사용한 패키지 관리가 배포 장에 추가되었습니다.
- BZ#1708456 (커널)의 텍스트를 업데이트합니다.
- 새로운 기능 BZ#1888214 (파일 시스템 및 스토리지) 추가.
- 알려진 문제 BZ#1991659 (Compilers 및 개발 툴) 추가.
- 기술 프리뷰 기능 JIRA:RHELPLAN-58596 (ID 관리) 추가.

0.0-8

2021년 8월 10일 화요일, Lucie Manásá(lmanasko@redhat.com)

- 업데이트된 새 기능 BZ#1905398 (클라우드 환경의 RHEL).

0.0-7

2021년 8월 3일 화요일, Lucie Maásá(lmanasko@redhat.com)

- BZ#1935722 (설치 프로그램 및 이미지 생성)에 알려진 문제가 추가되었습니다.
- 알려진 문제 BZ#1961722 (가상화).

0.0-6

2021년 7월 23일 금요일, Lucie Maásá(lmanasko@redhat.com)

- 알려진 문제 BZ#1924230 (보안).

- 알려진 문제 BZ#1957768 (ID 관리).

0.0-5

2021년 7월 16일 금요일, Lucie Maásá(lmanasko@redhat.com)

- 알려진 문제 BZ#1959020 (가상화) 추가.
- 알려진 문제 BZ#1963981 (클라우드 환경의 RHEL)이 추가되었습니다.
- 새로운 기능 BZ#1340463 (ID 관리).
- 유효하지 않은 릴리스 노트 및 버전 이력 항목을 제거했습니다.

0.0-4

2021년 6월 23일 수요일, Lucie Maásá(lmanasko@redhat.com)

- 새로운 기능 BZ#1966838 (지원 가능).
- sfc를 사용하여 더 이상 사용되지 않는 장치가 업데이트되었습니다.
- 기타 작은 개선 사항.

0.0-3

2021년 6월 16일, Lucie Maásá(lmanasko@redhat.com)

- 더 이상 사용되지 않는 기능 BZ#1929173 (네트워킹)이 추가되었습니다.
- 더 이상 사용되지 않는 기능 BZ#1920624 (Compilers 및 개발 툴) 추가.

- 새로운 기능 JIRA:RHELPLAN-63081 (ID 관리).
- 알려진 문제 BZ#1949743 (파일 시스템 및 스토리지) 추가.
- BZ#1332758 (가상화)에 대한 정보가 추가되었습니다.
- 알려진 문제 BZ#1957532 (클라우드 환경의 RHEL)가 추가되었습니다.
- 기타 작은 개선 사항.

0.0-2

2021년 6월 4일 금요일, 메카 -파파산라(lspackova@redhat.com)

- BZ#1849815 참고 사항을 수정했습니다.
- 다양한 포맷 개선 사항.

0.0-1

2021년 5월 18일, Lucie Maásá(lmanasko@redhat.com)

- Red Hat Enterprise Linux 8.4 릴리스 노트.

0.0-0

2021년 3월 31일 수요일, Lucie Maásá(lmanasko@redhat.com)

- Red Hat Enterprise Linux 8.4 베타 릴리스 정보.