Red Hat Enterprise Linux 8

8.2 릴리스 노트

Red Hat Enterprise Linux 8.2 릴리스 정보

Last Updated: 2022-07-03

Red Hat Enterprise Linux 8 8.2 릴리스 노트

Red Hat Enterprise Linux 8.2 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 8.2에서 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

RED HAT 문서에 관한 피드백 제공

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

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

1장. 개요

설치 프로그램 및 이미지 생성

RHEL 8.2에서는 패키지 설치 전에 시스템을 등록하고 RHEL 서브스크립션을 연결한 다음 Red Hat CDN(콘텐츠 전달 네트워크)에서 설치할 수 있습니다. 설치 중에 시스템을 Red Hat Insights에 등록할 수도 있습니다. 대화형 GUI 설치와 자동화된 Kickstart 설치는 이러한 새로운 기능을 지원합니다.

자세한 내용은 5.1.1절. "설치 프로그램 및 이미지 생성" 의 내용을 참조하십시오.

인프라 서비스

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

자세한 내용은 5.1.4절. "인프라 서비스"의 내용을 참조하십시오.

보안

이제 **시스템 전체 암호화 정책에서 사용자 지정** 을 지원합니다. 이제 관리자는 전체 정책을 정의하거나 특정 값만 수정할 수 있습니다.

RHEL 8.2에는 SELinux **-policy 분석 및 데이터 흐름 검사를 위한 툴을 제공하는 setools-gui 및 setools-console-analyses** 패키지가 포함되어 있습니다.

SCAP 보안 가이드는 이제 호주 사이버 보안 센터(ACSC) **필수 Eight** Maturity Model과 호환되는 프로파일을 제공합니다.

자세한 내용은 5.1.5절. "보안"를 참조하십시오.

동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

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

- **Python 3.8**
- **Maven 3.6**

자세한 내용은 5.1.10절. "동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버" 을 참조하십시오.

컴파일러 툴 세트

RHEL 8.2에서는 다음 컴파일러 툴 세트가 업데이트되었습니다.

- **GCC 툴 세트 9**
- **clang 및 LLVM Toolset 9.0.1**
- **히스토리 툴 세트 1.41**
- **Go Toolset 1.13**

자세한 내용은 5.1.11절. "컴파일러 및 개발 도구"를 참조하십시오.

IdM (Identity Management)

Identity Management에는 새로운 명령줄 도구가 도입되었습니다. **상태 점검**. **Healthcheck** 는 사용자가 IdM 환경에 영향을 줄 수 있는 문제를 찾는 데 도움이 됩니다.

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

자세한 내용은 5.1.12절. “IdM (Identity Management)” 를 참조하십시오.

웹 콘솔

PatternFly 4 사용자 인터페이스 시스템 설계를 사용하도록 웹 콘솔이 다시 설계되었습니다.

보안 향상을 위해 세션 시간 초과가 웹 콘솔에 추가되었습니다.

자세한 내용은 5.1.15절. “웹 콘솔”를 참조하십시오.

데스크탑

GNOME Classic 환경의 작업 공간 전환기가 수정되었습니다. 스위터는 이제 아래쪽 막대의 오른쪽 부분에 위치하며 수평면 패널로 설계되었습니다. 필요한 축소판 이미지를 클릭하면 작업 영역 간 전환이 가능합니다.

DRM (**Direct Rendering Manager**) 커널 그래픽 하위 시스템은 업스트림 Linux 커널 버전 5.3으로 업데이트되었습니다. 이 버전은 새 GPU 및 APU에 대한 지원과 다양한 드라이버 업데이트를 포함하여 이전 버전에 비해 여러 가지 개선 사항을 제공합니다.

즉각적 업그레이드

RHEL 7에서 RHEL 8으로의 즉각적 업그레이드

지원되는 즉각적 업그레이드 경로는 다음과 같습니다.

- 64비트 Intel, IBM POWER 8(little endian) 및 IBM Z 아키텍처의 RHEL 7.9에서 RHEL 8.2로
- 커널 버전 4.14가 필요한 아키텍처의 RHEL 7.6에서 RHEL 8.2로: 64비트 ARM, IBM POWER 9(Lttle endian), IBM Z(Structure A). 이러한 아키텍처는 RHEL 7에서 완전히 지원되지만 RHEL 7.7 이후의 마이너 릴리스 업데이트는 제공되지 않습니다.

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

주요 개선 사항은 다음과 같습니다.

- RHEL 7에서 RHEL 8로의 즉각적 업그레이드에 추가 사용자 지정 리포지토리를 사용할 수 있습니다. Red Hat 서브스크립션 관리자 없이도 업그레이드할 수 있습니다.
- Leapp 유틸리티를 사용하여 사용자 지정 또는 타사 애플리케이션을 마이그레이션할 고유한 행위자를 만들 수 있습니다.

자세한 내용은 Red Hat Enterprise Linux 즉각적 업그레이드 사용자 지정을 참조하십시오.

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

RHEL 6에서 RHEL 8로 즉각적 업그레이드

RHEL 6.10에서 RHEL 8.2로 업그레이드하려면 RHEL 6에서 RHEL 8로 업그레이드하는 방법에 대한 지침을 따르십시오.

CentOS Linux 6 또는 Oracle Linux 6을 사용하는 경우 RHEL 8로 업그레이드하기 전에 지원되지 않는 **convert2rhel** 유틸리티를 사용하여 운영 체제를 RHEL 6로 변환할 수 있습니다. 자세한 내용은 CentOS Linux 또는 Oracle Linux에서 RHEL로 변환하는 방법을 참조하십시오.

추가 리소스

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

Red Hat Customer Portal 랩

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

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

2장. 아키텍처

Red Hat Enterprise Linux 8.2는 다음 아키텍처를 지원하는 커널 버전 4.18.0-193과 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. RHEL 8.2.1 릴리스

Red Hat은 마이너 릴리스 (8.Y)마다 분기별로 Red Hat Enterprise Linux 8 컨텐츠를 제공합니다. 분기 별 릴리스는 세 번째 숫자 (8.Y.1)로 번호가 매겨집니다. RHEL 8.2.1 릴리스의 새로운 기능은 다음과 같습니다.

4.1. 새로운 기능

JDK Mission Control을 버전 7.1.1로 업데이트

jmc:rhel8 모듈 스트림에서 제공하는 HotSpot JVM에 대한 JDK Mission Control(JMC) 프로파일러는 RHEL 8.2.1 릴리스와 함께 버전 7.1.1으로 업그레이드되었습니다.

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

- 다중 규칙 최적화
- SWT(Standard Widget Toolkit)를 기반으로 하는 새로운 JOverflow 보기
- 새 글꼴 그래프 보기
- HDR(High Dynamic Range) 히스토그램을 사용하는 새로운 대기 시간 시각화 방법

jmc:rhel8 모듈 스트림에는 두 개의 프로필이 있습니다.

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

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

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

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

(BZ#1792519)

jboss Toolset을 버전 1.43으로 다시 설정

capsule Toolset이 1.43 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 이제 유용한 줄 번호는 **Option(옵션) 및 Result panic message** (피정 결과) 메시지에 포함되어 있습니다.
- 하위 슬라이스 패턴에 맞는 확장된 지원.
- **matches!** 매크로는 부울 값을 반환하는 패턴 일치를 제공합니다.
- **항목** 조각은 특성, impls 및 extern 블록으로 나눌 수 있습니다.
- 기본 사항에 대한 유형 유추 개선.
- 유동 및 정수에 관련된 상수입니다.

pvc Toolset 모듈을 설치하려면 **root** 로 다음 명령을 실행하십시오.

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

사용 정보는 사용 설명서를 참조하십시오.

(BZ#1811997)

컨테이너 레지스트리에서 skopeo sync 명령을 지원

이번 개선된 기능을 통해 사용자는 **skopeo sync** 명령을 사용하여 컨테이너 레지스트리와 로컬 레지스트리를 동기화할 수 있습니다. **skopeo sync** 명령은 로컬 컨테이너 레지스트리 미러를 동기화하고 가동 가능한 환경 내에서 실행되는 레지스트리를 채우는 데 유용합니다.

skopeo sync 명령에는 소스(**--src**) 및 대상(**--dst**) 전송이 모두 별도로 지정해야 합니다. 사용 가능한 소스 및 대상 전송은 **docker** (컨테이너 레지스트리에서 호스팅되는 리포지토리) 및 **dir** (로컬 디렉터리 경로의 디렉터리)입니다. 소스 전송에는 **yaml** (로컬 YAML 파일 경로)도 포함됩니다. **skopeo 동기화 사용에 대한 자세한 내용은 skopeo -sync** 도움말 페이지를 참조하십시오.

(BZ#1811779)

설정 파일 container.conf 사용 가능

이 향상된 기능을 통해 사용자와 관리자는 컨테이너 엔진에 대한 기본 구성 옵션 및 명령줄 플래그를 지정할 수 있습니다. 컨테이너 엔진은 **/usr/share/containers/containers.conf** 및 **/etc/containers/containers.conf** 파일을 읽습니다. rootless 모드에서 컨테이너 엔진은 **$HOME/.config/containers/containers.conf** 파일을 읽습니다.

containers.conf 파일에 지정된 필드는 기본 옵션과 이전에 **containers.conf** 파일의 옵션을 재정의합니다. **container.conf** 파일은 Podman과 Buildah 간에 공유되며 **libpod.conf** 파일을 대체합니다.

(BZ#11826486)

이제 레지스트리 서버에서 로그인 및 로그아웃할 수 있습니다.

이번 개선된 기능을 통해 skopeo **login 및 skopeo logout** 명령을 사용하여 지정된 레지스트리 서버에서 로그인하고 로그아웃할 수 있습니다. **skopeo login** 명령은 표준 입력에서 사용자 이름 및 암호를 읽습니다. 사용자 이름 및 암호는 **--username(또는 -u) 및 -- password (또는 - p**) 옵션을 사용하여 설정할 수도 있습니다.

auth **file** 플래그를 설정하여 인증 파일의 경로를 지정할 수 있습니다. 기본 경로는 **${XDG_RUNTIME_DIR}/containers/auth.json** 입니다. **skopeo login 및 skopeo logout** 사용에 대한 자세한 내용은 **skopeo-login** 및 **skopeo-logout** 도움말 페이지를 참조하십시오.

(JIRA:RHELPLAN-47311)

podman 스토리지를 재설정할 수 있습니다.

이 향상된 기능을 통해 사용자는 **podman system reset 명령을 사용하여 podman storage** 를 초기 상태로 재설정할 수 있습니다. **podman system reset** 명령은 모든 포드, 컨테이너, 이미지 및 볼륨을 제거합니다. 자세한 내용은 **podman-system-reset** 도움말 페이지를 참조하십시오.

(JIRA:RHELPLAN-48941)

5장. RHEL 8.2.0 릴리스

5.1. 새로운 기능

이 부분에서는 Red Hat Enterprise Linux 8.2에 도입된 새로운 기능 및 주요 개선 사항에 대해 설명합니다.

5.1.1. 설치 프로그램 및 이미지 생성

시스템을 등록하고 RHEL 서브스크립션을 연결하며 Red Hat CDN에서 설치할 수 있는 기능

RHEL 8.2에서는 패키지 설치 전에 시스템을 등록하고 RHEL 서브스크립션을 연결한 다음 Red Hat CDN(콘텐츠 전달 네트워크)에서 설치할 수 있습니다. 대화형 GUI 설치와 자동화된 Kickstart 설치는 이 기능을 지원합니다. 이점은 다음과 같습니다.

- 작은 부트 ISO 이미지 파일을 사용하면 더 큰 바이너리 DVD ISO 이미지 파일을 다운로드할 필요가 없습니다.
- CDN은 최신 패키지를 사용하므로 설치 직후에 완전히 서브스크립션되고 최신 시스템이 생성됩니다. 설치 후 패키지 업데이트를 설치할 필요가 없습니다.
- 등록은 패키지 설치 전에 수행되므로 설치 프로세스가 더 짧고 간소화됩니다.
- Red Hat Insights에 대한 통합 지원이 제공됩니다.

(BZ#1748281)

설치 중에 시스템을 Red Hat Insights에 등록하는 기능

RHEL 8.2에서는 설치 중에 시스템을 Red Hat Insights에 등록할 수 있습니다. 대화형 GUI 설치와 자동화된 Kickstart 설치는 이 기능을 지원합니다.

이점은 다음과 같습니다.

- 비즈니스 운영에 영향을 미치기 전에 문제를 쉽게 식별, 우선 순위 지정 및 해결할 수 있습니다.
- 예측 분석을 통해 보안, 성능, 가용성 및 안정성에 대한 위협을 사전에 식별하고 해결합니다.
- 귀사의 환경에서 문제와 계획되지 않은 다운타임을 방지할 수 있습니다.

(BZ#1746391)

Image Builder에서 Azure 이미지 생성을 위한 cloud-init 지원 제공

이번 개선된 기능을 통해 Image Builder에서 만든 Azure 이미지에 cloud-init 지원이 제공됩니다. 따라서 신속한 프로비저닝을 통해 온프레미스 이미지를 생성하고 사용자 지정 데이터를 추가하는 기능을 고객에게 사용할 수 있습니다.

(BZ#1754711)

새로운 킥스타트 명령 추가: rhsm 및 zipl

이번 릴리스에서는 다음 킥스타트 명령이 추가되었습니다.

- **rhsm**: 설치 중에 Red Hat에 시스템을 등록하려면 **rhsm** 명령을 사용합니다. 자세한 내용은 고급 설치 가이드의 예제 **섹션** 을 참조하십시오.

- **zipl**: **zipl** 명령을 사용하여 IBM Z 시스템에 **zipl** 구성을 지정합니다. 자세한 내용은 고급 설치 가이드의 **모듈** 섹션을 참조하십시오.

(BZ#1972214)

5.1.2. 소프트웨어 관리

user-Agent 헤더 문자열에 /etc/os-release 파일에서 읽은 정보가 포함됩니다.

이번 개선된 기능을 통해 DNF에서 만든 HTTP 요청에 일반적으로 포함된 **User-Agent** 헤더 문자열이 **/etc/os-release** 파일에서 읽은 정보를 사용하여 확장되었습니다.

자세한 내용은 **dnf.conf(5)** 도움말 페이지에서 **user_agent** 를 참조하십시오.

(BZ#1676891)

모든 dnf-automatic.timer 타이머 장치는 기본적으로 실시간 시계를 사용합니다.

이전에는 **dnf-automatic.timer** 타이머 장치가 monotonic 클록을 사용했기 때문에 시스템 부팅 후 예기치 않은 활성화 시간이 발생했습니다. 이번 업데이트를 통해 타이머 장치는 오전 6시에서 오전 7시 사이에 실행됩니다. 이 시간 동안 시스템이 꺼진 경우 시스템을 부팅한 후 1시간 이내에 타이머 장치가 활성화됩니다.

(BZ#1754609)

createrepo_c 유틸리티는 이제 메타데이터에 허용하지 않는 제어 문자가 포함된 패키지를 건너뜁니다.

유효한 XML을 확인하려면 패키지 메타데이터에 다음을 제외하고 제어 문자가 없어야 합니다.

- 수평 탭
- 줄 바꿈 문자
- 캐리지 반환 문자

이번 업데이트를 통해 **createrepo_c** 유틸리티에는 새로 생성된 리포지토리에 허용하지 않는 제어 문자가 포함된 메타데이터가 포함된 패키지가 포함되어 있지 않으며 다음과 같은 오류 메시지를 반환합니다.

> C_CREATEREPOLIB: Critical: Cannot dump XML for PACKAGE_NAME (PACKAGE_SUM): Forbidden control chars found (ASCII values <32 except 9, 10 and 13)

(BZ#1743186)

5.1.3. 쉘 및 명령행 툴

Open CV가 3.4.6 버전으로 업데이트

opencv 패키지가 업스트림 버전 3.4.6로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- OPENCV_OPENCL_ **BUILD_EXTRA_OPTIONS** 및 **OPENCV_OPENCL_DEVICE_MAX_WORK_GROUP_SIZE** 와 같은 새로운 Open CL 매개변수 지원.
- 이제 **objdetect** 모듈에서 IC 코드 탐지 알고리즘을 지원합니다.
- **MatSize::dims** 또는 **VideoCapture:: getBackendName** 과 같은 여러 새 메서드.

- **drawframeAxes** 또는 **getVersionMajor** 와 같은 여러 새 함수.
- SSSE3 명령을 사용할 때 GaussianBlur 함수, **v_load_deinterleave** 및 **v_store_interleave** 내장 기능 개선 등 다양한 성능 향상.

(BZ#1694647)

5.1.4. 인프라 서비스

Graphviz-python3 이 CRB 리포지토리에 배포

이번 업데이트에서는 **graphviz-python3** 패키지가 RHEL 8에 추가됩니다. 패키지는 Python의 Graphviz 그래프 시각화 소프트웨어를 사용하는 데 필요한 바인딩을 제공합니다.

graphviz-python3 패키지는 지원되지 않는 CRB(CodeReady Linux Builder 리포지토리) 에 배포됩니다.

(BZ#1704875)

버전 2.13.0으로 조정

tuned 패키지가 업스트림 버전 2.13.0으로 업그레이드되었습니다. 주요 개선 사항은 다음과 같습니다.

- 아키텍처에 따라 튜닝 프레임워크가 추가되었습니다.
- 여러 include 지시문에 대한 지원이 추가되었습니다.
- **sap-hana**,**latency-performance** 및 **realtime** 프로필의 튜닝이 업데이트되었습니다.

(BZ#1738250)

PowerTOP 버전 2.11로 업데이트

powertop 패키지가 다음과 같은 주요 변경 사항을 제공하는 버전 2.11로 업그레이드되었습니다.

- EHL, TGL, ICL/ICX 플랫폼 지원

(BZ#1716721)

BIND에서 GeoLite Legacy GeoIP 대신 .GeoIP2 지원

GeoLite Legacy GeoIP 라이브러리는 더 이상 BIND에서 지원되지 않습니다. 이번 업데이트를 통해 GeoLite Legacy GeoP가 **libmaxminddb** 데이터 형식으로 제공되는 GeoIP2로 교체되었습니다.

새 형식에는 일부 구성을 변경해야 할 수 있으며 형식은 레거시 GeoIP ACL(액세스 제어 목록) 설정을 지원하지 않습니다.

- GeoIP netspeed
- GeoIP 조직
- ISO 3166 Alpha-3 국가 코드

(BZ#1564443)

이제 stale-answer 에서RHEL 공격의 경우 오래된 캐시된 레코드를 제공합니다.

이전에는 DDoS(Distributed Denial of Service) 공격으로 인해 신뢰할 수 있는 서버가 SERVFAIL 오류로 실패했습니다. 이번 업데이트를 통해 새로운 응답을 받을 때까지 **오래된 응답이 만료된 레코드를 제공합니다**.

serve-stale 기능을 활성화하거나 비활성화하려면 다음 중 하나를 사용합니다.

- 설정 파일
- 원격 제어 채널(rndc)

(BZ#1664863)

BIND를 버전 9.11.13으로 업데이트

bind 패키지가 버전 9.11.13으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- **tcp-highwater** 통계 변수가 추가되었습니다. 이 변수는 실행 중에 기록된 최대 동시 TCP 클라이언트를 표시합니다.
- **SipHash-2-4**기반 DNS 표시(RFC7873) 알고리즘이 추가되었습니다.
- **최소 응답 구성 옵션을 설정하는 방법에 관계없이 루트 설정 쿼리에** 대한 라벨 주소가 반환됩니다.
- **named-checkconf** 명령은 이제 **DNS64** 네트워크 접두사의 유효성을 확인합니다.
- **trusted-keys 및 managed-keys** 문이 모두 동일한 이름에 대해 구성된 경우 RFC 5011당 자동 롤오버가 더 이상 실패하지 않습니다. 대신 경고 메시지가 기록됩니다.
- 이제 **dig** 및 **nslookup** 유틸리티의 국제화된 도메인 이름(IDN) 처리가 터미널에서 실행되지 않을 때 기본적으로 비활성화됩니다(예: 스크립트의). **dig** 에서 IDN 처리는 **+idnin 및 +id nout** 옵션을 사용하여 에서 전환할 수 있습니다.

(BZ#1704328)

5.1.5. 보안

RHEL 8에는 DISA STIG 프로필이 포함되어 있습니다.

STIG(Security Technical Implementation Guides)는 DSA(Defense Information Systems Agency)가 게시한 정보 시스템 및 소프트웨어의 보안을 강화하기 위해 게시한 기본 권장 사항 집합입니다. 이 릴리스에는 이 보안 정책에 대한 프로필 및 Kickstart 파일이 포함되어 있습니다. 이 향상된 기능을 통해 사용자는 Red Hat Enterprise Linux 8용 DISA STIG 호환 시스템을 준수하는 시스템을 규정 준수 여부를 확인하고 시스템을 수정할 수 있습니다.

(BZ#1755447)

crypto-policies 를 이제 사용자 정의 가능

이번 업데이트를 통해 모든 정책 수준의 특정 알고리즘 또는 프로토콜을 조정하거나 새 전체 정책 파일을 현재 시스템 전체 암호화 정책으로 설정할 수 있습니다. 이를 통해 관리자는 다양한 시나리오에서 필요에 따라 시스템 전체 암호화 정책을 사용자 지정할 수 있습니다.

RPM 패키지는 해당 정책이 제공하는 정책을 **/usr/share/crypto-policies/policies** 디렉토리에 저장해야 합니다. **/etc/crypto-policies/policies** 디렉터리에는 로컬 사용자 지정 정책이 포함되어 있습니다.

자세한 내용은 update **-crypto-policies(8) 도움말 페이지 및 update- crypto-policies(8)** 도움말 페이지의 **Custom Policies 섹션을** 참조하십시오.

(BZ#1690565)

SCAP Security Guide가 ACSC Essential Eight 지원

scap-security-guide 패키지는 이제 호주 사이버 보안 센터(ACSC) 필수 Eight 규정 준수 프로필과 해당 Kickstart 파일을 제공합니다. 이 향상된 기능을 통해 사용자는 이 보안 기준을 준수하는 시스템을 설치할 수 있습니다. 또한 **OpenSCAP** 제품군을 사용하여 ACSC에서 정의한 최소 보안 제어 사양으로 보안 준수 및 해결을 확인할 수 있습니다.

(BZ#1755194)

컨테이너 보안 및 규정 준수 검사를 위한 oscap-podman 사용 가능

이번 **openscap** 패키지 업데이트에서는 컨테이너의 보안 및 규정 준수 검사를 위한 새로운 유틸리티가 도입되었습니다. **oscap-podman** 툴은 RHEL 7에서 컨테이너 및 컨테이너 이미지 스캔을 위해 서비스를 제공하는 **oscap-docker** 유틸리티와 동등합니다.

(BZ#1642373)

setroubleshoot 에서 execmem 액세스 거부를 분석하고 대응할 수 있음

이번 업데이트에서는 새 **setroubleshoot** 플러그인이 도입되었습니다. 플러그인은 **execmem** 액세스 거부(AVC)를 분석하고 관련 조언을 제공할 수 있습니다. 결과적으로 **setroubleshoot** 는 액세스를 허용하는 경우 부울을 전환하거나 부울이 액세스를 허용하지 않을 때 문제를 보고할 수 있습니다.

(BZ#1649842)

새 패키지: setools-gui 및 setools-console-analyses

이제 RHEL 7에 포함된 **setools-gui** 패키지가 RHEL 8에 도입되었습니다. 그래픽 도구를 사용하면 특히 고도의 전문 SELinux 정책이 있는 다단계 시스템에서 관계 및 데이터 흐름을 검사할 수 있습니다. **setools-gui** 패키지의 **apol** 그래픽 도구를 사용하면 SELinux 정책의 측면을 검사하고 분석할 수 있습니다. **setools-console-analyses 패키지의** 툴을 사용하면 도메인 전환 및 SELinux 정책 정보 흐름을 분석할 수 있습니다.

(BZ#1731519)

SELinux에서 제한된 사용자가 사용자 세션 서비스를 관리할 수 있음

이전에는 제한된 사용자가 사용자 세션 서비스를 관리할 수 없었습니다. 결과적으로 **systemctl --user 또는 busctl --user** 명령을 실행하거나 RHEL 웹 콘솔에서 작업할 수 없었습니다. 이번 업데이트를 통해 제한된 사용자는 사용자 세션을 관리할 수 있습니다.

(BZ#1727887)

lvmdbusd 서비스가 SELinux에 의해 제한됨

lvmdbusd 서비스는 LVM(논리 볼륨 관리자)에 D-Bus API를 제공합니다. 이전에는 **lvm_t에 대한 SELinux 정책이 정의된 경우에도 lvmdbusd 데몬이 lvm_t** 컨텍스트로 전환할 수 **없었습니다**. 결과적으로 **lvmdbusd** 데몬은 **unconfined_service_t** 도메인에서 실행되었으며 SELinux는 제한되지 않은 것으로 레이블이 **지정되었습니다**. 이번 업데이트를 통해 **lvmdbusd** 실행 파일에 **lvm_exec_t** 컨텍스트가 정의되어 있으며 **lvmdbusd** 를 강제 모드에서 SELinux에서 올바르게 사용할 수 있습니다.

(BZ#1726166)

semanage 는 SCTP 및 DCCP 포트 목록화 및 수정을 지원합니다.

이전에는 **semanage 포트**를 통해 TCP 및 UDP 포트만 나열하고 수정할 수 있었습니다. 이번 업데이트에서는 **semanage 포트에** SCTP 및 DCCP 프로토콜 지원이 추가되었습니다. 결과적으로 관리자는 두 개의

시스템이 SCTP를 통해 통신할 수 있는지 확인하고 SCTP 기능을 완전히 활성화하여 SCTP 기반 애플리케이션을 성공적으로 배포할 수 있습니다.

(BZ#1563742)

semanage 내보내기에 허용 도메인과 관련된 사용자 정의 표시

이번 업데이트를 통해 SELinux용 **policycoreutils** 패키지에 속하는 **semanage** 유틸리티가 허용 도메인과 관련된 사용자 지정을 표시할 수 있습니다. 이제 시스템 관리자는 **semanage export** 명령을 사용하여 시스템 간에 허용된 로컬 수정 사항을 전송할 수 있습니다.

(BZ#1417455)

오디카는 SELinux 거부에서 생성된 기존 컨테이너 정책에 새 허용 규칙을 추가할 수 있습니다.

udica 유틸리티에서 생성한 정책에서 실행 중인 컨테이너에서 SELinux 거부를 트리거하면 이제 **udica** 가 정책을 업데이트할 수 있습니다. 새 매개변수 **-a** 또는 **--append-rules** 를 사용하여 AVC 파일에서 규칙을 추가할 수 있습니다.

(BZ#1732704)

새로운 SELinux 유형을 사용하면 서비스가 제한된 상태로 실행될 수 있습니다.

이번 업데이트에서는 **unconfined_service_t 도메인에서** 실행하지 않고 다음 서비스가 SELinux 강제 모드에서 제한된 서비스로 실행될 수 있는 새로운 SELinux 유형이 도입되었습니다.

- **lldpd** 가 as **lldpad_t**실행
- **rrdcached** 가 **rrdcached_t**로 실행됩니다
- **stratisd** 는 이제 **stratisd_t**로 실행됩니다.
- **timedatex** 는 **timedatex_t**로 실행됩니다.

(BZ#1726246, BZ#1726255, BZ#1726259, BZ#1730204)

Clevis는 지정된 LUKS 장치에 대한 정책을 나열 할 수 있습니다.

이번 업데이트를 통해 **clevis luks list** 명령은 지정된 LUKS 장치에 대한 PBD 정책을 나열합니다. 이렇게 하면 사용 중인 Clevis 고정 및 고정 구성(예: Tang 서버 주소, **tpm2** 정책 세부 사항, SSS 임계값)에 대한 정보를 더 쉽게 찾을 수 있습니다.

(BZ#1766526)

Clevis는 키 상태를 보고하고 만료된 키를 다시 바인딩하기 위한 새로운 명령을 제공합니다.

clevis luks report 명령은 이제 특정 바인딩의 키에 회전이 필요한지 여부를 보고할 수 있는 간단한 방법을 제공합니다. Tang 서버의 일반 키 순환은 NBDE(Network-Bound Disk Encryption) 배포의 보안을 강화하므로 클라이언트는 만료된 키를 감지해야 합니다. 키가 만료되면 Clevis는 만료된 키 슬롯을 현재 키로 다시 바인딩하는 **clevis luks regen** 명령을 사용하도록 제안합니다. 이렇게 하면 키 순환 프로세스가 크게 간소화됩니다.

(BZ#1564559, BZ#1564566)

Clevis는 LUKS 장치에서 특정 슬롯을 바인딩하는 데 사용되는 암호를 추출할 수 있습니다

이번 업데이트를 통해 Clevis 정책 기반 암호 해독 프레임워크를 통해 LUKS 장치에서 특정 슬롯을 바인딩하는 데 사용되는 암호를 추출할 수 있습니다. 이전 버전에서는 LUKS 설치 암호를 지우면 관리자가 **sss** 임계값을 변경해야 할 때 Clevis에서 재암호화, 새 키 슬롯 활성화 및 Clevis와 같은 LUKS 관리 작업을 수

행할 수 없었습니다. 이번 업데이트에서는 특정 슬롯을 바인딩하는 데 사용되는 암호를 표시하는 **clevis luks pass** 명령이 도입되었습니다.

(BZ#1436780)

Clevis는 부팅 시 여러 LUKS 장치의 암호 해독 지원 개선

부팅 시 여러 LUKS 암호화된 장치의 암호 해독을 지원하도록 **clevis** 패키지가 업데이트되었습니다. 이 기능이 향상되기 전에 관리자는 부팅 시 Clevis를 통해 여러 장치를 올바르게 해독할 수 있도록 시스템 구성을 복잡한 변경 작업을 수행해야 했습니다. 이번 릴리스에서는 **clevis luks bind** 명령을 사용하고 **dracut -fv --regenerate-all** 명령을 통해 initramfs를 업데이트하여 암호 해독을 설정할 수 있습니다.

자세한 내용은 정책 기반 암호 해독 섹션을 사용하여 암호화된 볼륨의 자동화된 잠금 해제 구성 섹션을 참조하십시오.

(BZ#1784524)

OpenSSL-pkcs11 을 Salesforce.10으로 업데이트

openssl-pkcs11 패키지가 업스트림 버전 0.2.10으로 업그레이드되어 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다. **openssl-pkcs11** 패키지는 엔진 인터페이스를 통해 PKCS #11 모듈에 대한 액세스를 제공합니다. 새 버전에 의해 도입된 주요 변경 사항은 다음과 같습니다.

- ECDSA 개인 키를 로드할 때 개인 키에 해당하는 공개 키 오브젝트를 사용할 수 없는 경우 엔진은 일치하는 인증서에서 공개 키를 로드합니다(있는 경우).
- **openssl-pk cs11 엔진은 지정된 PKCS #11 URI와 일치하는 모든 토큰을 검색하므로 일반 PKCS #11 URI(예: pkcs11:type=public**)를 사용할 수 있습니다.
- 시스템은 단일 장치가 URI 검색과 일치하는 경우에만 PIN으로 로그인하려고 합니다. 이렇게 하면 일치하는 모든 토큰에 PIN을 제공하여 인증 실패를 방지합니다.
- 장치에 액세스할 때 **openssl-pkcs11** 엔진은 RSA 메서드가 **RSA_FLAG_FIPS_METHOD** 플래그로 구조를 나타냅니다. FIPS 모드에서 OpenSSL을 사용하려면 RSA 메서드 구조에 플래그를 설정해야 합니다. 엔진은 장치가 FIPS 인증인지 감지할 수 없습니다.

(BZ#1745082)

rsyslog 가 8.1911.0으로 업데이트

rsyslog 유틸리티가 업스트림 버전 8.1911.0으로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 다음 목록에는 주요 개선 사항이 포함되어 있습니다.

- 새 **omhttp** 모듈을 사용하면 HTTP REST 인터페이스를 통해 메시지를 보낼 수 있습니다.
- 파일 입력 모듈이 개선되어 안정성, 오류 보고 및 축소 탐지 기능이 향상됩니다.
- 모든 작업에 사용할 수 있는 새로운 **action.resumeIntervalMax** 매개변수는 지정된 값에서 재시도 간격 증가를 제한할 수 있습니다.
- TLS에 대한 새로운 **StreamDriver.PermitExpiredCerts** 옵션은 인증서가 만료된 경우에도 연결을 허용합니다.
- 이제 구성된 외부 파일 콘텐츠를 기반으로 출력을 일시 중지하고 재개할 수 있습니다. 이 기능은 다른 끝에 항상 메시지를 허용하고 메시지를 모두 처리할 수 없을 때 자동으로 메시지를 삭제하는 경우에 유용합니다.

- file 출력 모듈에 대한 오류 보고가 개선되고 이제 실제 파일 이름 및 오류 원인에 대한 자세한 정보가 포함되어 있습니다.
- 이제 디스크 대기열에서 다중 스레드를 실행하여 성능을 향상시킵니다.
- 더 엄격한 TLS 운영 모드를 설정할 수 있습니다. **extendedKeyUsage** 인증서 필드 확인 및 **CN/SAN** 인증서 필드의 엄격한 검사.

(BZ#1740683)

rsyslog 는 HTTP REST 인터페이스를 통한 통신용 omhttp 플러그인 제공

rsyslog 패키지 업데이트를 통해 새 **omhttp** 플러그인을 사용하여 Ceph 스토리지 플랫폼, Amazon S3(Amazon Simple Storage Service) 및 Grafana Loki와 같은 REST(Representational State Transfer) API를 사용하여 서비스와 호환되는 출력을 생성할 수 있습니다. 이 새로운 HTTP 출력 모듈은 구성 가능한 REST 경로 및 메시지 형식을 제공하며 다양한 일괄 처리 형식, 압축 및 TLS 암호화를 지원합니다.

자세한 내용은 **rsyslog-doc 패키지를** 사용하여 시스템에 설치된 **/usr/share/doc/rsyslog/html/configuration/modules/omhttp.html** 파일을 참조하십시오.

(BZ#1676559)

rsyslog 의 omelasticsearch 에서 rebindinterval지원

이번 **rsyslog** 패키지 업데이트에서는 **omelasticsearch** 모듈에서 기간 재연결 시간을 설정할 수 있도록 지원합니다. 시나리오에 따라 이 매개변수를 설정하여 Elasticsearch 노드의 클러스터에 레코드를 보낼 때 성능을 향상시킬 수 있습니다. **rebindinterval** 매개 변수 값은 **rsyslog** 가 연결을 닫고 새 노드를 설정한 후 노드에 제출된 작업 수를 나타냅니다. 기본값 **-1** 은 **rsyslog** 가 연결을 다시 설정하지 않음을 의미합니다.

(BZ#1692073)

rsyslog mmkubernetes 에서 메타데이터 캐시 만료 제공

이 **rsyslog** 패키지 업데이트를 통해mm **kubernetes** 모듈에 두 개의 새 매개변수를 사용하여 메타데이터 캐시 만료를 설정할 수 있습니다. 이렇게 하면 삭제된 Kubernetes 오브젝트가mm **kubernetes 정적** 캐시에서 제거됩니다. **cacheentrytl 매개 변수 값은 캐시** 항목의 최대 사용 기간을 초 단위로 나타냅니다. **cacheexpireinterval** 매개변수의 값은 다음과 같습니다.

- **-1** 캐시 만료 검사 비활성화
- **0** 캐시 만료 검사 활성화
- 정규 캐시 만료 검사의 경우 초 단위가 0보다 큽니다.

(BZ#1692072)

감사 버전 3.0-0.14로 업데이트

감사 패키지가 업스트림 버전 3.0-0.14로 업그레이드되어 이전 버전에 대해 많은 버그 수정 및 개선 사항을 제공합니다. 특히 다음과 같습니다.

- syslog 플러그인의 필드를 해석하는 옵션 추가
- **30ospp-v42.rules** 파일을 더 세분화된 파일로 나눕니다
- **/usr/share/audit/sample-rules/** 디렉토리로 예제 규칙 이동
- 원격 로깅을 위한 고정 감사 KRB5 전송 모드

(BZ#1757986)

이제 audit에 커널 v5.5-rc1의 많은 개선 사항이 포함되어 있습니다.

이 Linux 커널에는 감사 하위 시스템과 관련된 대부분의 개선 사항, 버그 수정 및 정리가 포함되며 버전 4.18과 5.5-rc1 간에 도입되었습니다. 다음 목록은 중요한 변경 사항을 강조 표시합니다.

- 필터링을 위한 **exe** 필드의 추가 사용
- v3 네임 스페이스 기능 지원
- 원격 파일 시스템에서 필터링 개선 사항
- **gid** 필터 규칙 수정
- 사용 후 메모리 손상 및 메모리 누수 수정
- 이벤트-레코드 연결 개선
- 팬의 **인터페이스**, 감사 구성 옵션 및 syscall 인터페이스 정리
- EVM(Extended Verification Module) 반환 값 수정
- 여러 레코드 형식의 수정 및 정리
- VFS(가상 파일 시스템) 감사의 간소화 및 수정

(BZ#1716002)

fapolicyd 가 0.2.1-2로 업데이트

RHEL 애플리케이션 화이트리스트를 제공하는 **fapolicyd** 패키지가 업스트림 버전 0.2.1-2로 업그레이드되었습니다. 주요 버그 수정 및 개선 사항은 다음과 같습니다.

- 프로세스 ID가 고정되었습니다.
- 제목 부분과 객체 부분은 이제 규칙에 따라 엄격하게 배치됩니다. 두 부분 모두 콜론으로 구분되며 필요한 권한(실행, 열기)이 포함됩니다.
- subject 및 object 속성이 통합됩니다.
- 새 규칙 형식은 다음과 같습니다.

```
DECISION PERMISSION SUBJECT : OBJECT
```

  예를 들면 다음과 같습니다.

```
allow perm=open exe=/usr/bin/rpm : all
```

(BZ#1759895)

sudo 가 1.8.29-3.el8로 업데이트

sudo 패키지가 업스트림 버전 1.8.29-3으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 새 버전에 의해 도입된 주요 변경 사항은 다음과 같습니다.

- **sudo** 는 표준 출력 또는 표준 오류 출력 대신 PAM(Pluggable Authentication Module) 메시지를 사용자 터미널에 작성합니다. 이렇게 하면 파일 및 파이프로 전송된 PAM 출력과 명령 출력의 혼동을 방지할 수 있습니다.

- 이제 LDAP 및 SSSD의 **notBefore 및 notAfter** 옵션이 작동하고 **sudo -l** 명령으로 올바르게 표시됩니다.

- 이제 LDIF에서 **sudoers** 및 JSON 형식으로 변환할 때 **cvtsudoers** 명령은 LDIF(비LDAP Data Interchange Format) 입력을 거부합니다.

- **sudoers** 에 대한 새로운 **log_allowed** 및 **log_denied** 설정을 사용하면 허용 및 거부된 명령의 로깅 및 감사를 비활성화할 수 있습니다.

- 이제 **sudo** 옵션을 **-g** 옵션과 함께 사용하여 **runas_spec** 사양에 그룹이 없는 경우에도 대상 사용자 그룹과 일치하는 그룹을 지정할 수 있습니다. 이전에는 그룹이 대상 사용자의 기본 그룹과 일치하는 경우에만 이를 수행할 수 있었습니다.

- **sudo** 가 호스트 이름과 **ipa_hostname** 값을 지정하면 **sssd.conf** 에서 일치하지 않도록 하는 버그 수정.

- **ALL** 키워드를 **사용하여 Runas** 사양에서 root로 명령을 실행할 **수 있는** 취약점(CVE-2019-14287)이 수정되었습니다.

- 허용 **sudoers** 항목에 대해 알 수 없는 사용자 및 그룹 ID(예: ALL 키워드 사용)가 비활성화되었습니다. **runas_allow_unknown_id** 설정(CVE-2019-19232)으로 활성화할 수 있습니다.

(BZ#1733961)

pam_namespace 모듈을 사용하여 tmpfs에 대한 추가 마운트 옵션을 지정할 수 있습니다.

이제 **nosuid**,**noexec** 및 **nodev** 마운트 옵션을 **/etc/security/namespace.conf** 구성 파일에서 각각 setuid bit effect를 비활성화하고, 실행 파일을 비활성화하고, 마운트된 **tmpfs** 파일 시스템에서 파일을 문자 또는 블록 장치로 해석하지 않도록 할 수 있습니다.

추가 마운트 옵션은 **tmpfs(5)** 도움말 페이지에 지정되어 있습니다.

(BZ#1252859)

pam_faillock 이 이제 faillock.conf 구성 파일에서 설정을 읽을 수 있습니다.

PAM(장착형 인증 모듈)의 일부인 **pam_faillock** 모듈은 이제 **/etc/security/faillock.conf** 에 있는 구성 파일에서 설정을 읽을 수 있습니다. 이렇게 하면 인증 실패 시 계정 잠금을 쉽게 설정하고, 이 기능에 대한 사용자 프로필을 제공하고, 단순히 **faillock.conf** 파일을 편집하여 다른 PAM 구성을 처리할 수 있습니다.

(BZ#1537242)

5.1.6. 네트워킹

사용자 공간 애플리케이션에서 커널에서 선택한 netns ID를 검색할 수 있습니다

사용자 공간 애플리케이션은 커널을 요청하여 새 **netns** ID를 선택하고 네트워크 네임 스페이스에 할당할 수 있습니다. 이 향상된 기능을 통해 커널에 **RTM _NETNSID netlink 메시지를 보낼 때 NLM_ F_ECHO** 플래그를 지정할 수 있습니다. 그런 다음 커널이 **netlink** 메시지를 사용자에게 다시 전송합니다. 이 메시지에는 커널이 선택한 값으로 설정된 **netns** ID가 포함됩니다. 결과적으로 사용자 공간 애플리케이션에 커널이 선택한 **넷링크** ID를 식별할 수 있는 안정적인 옵션이 있습니다.

(BZ#1763661)

firewalld 를 버전으로 업데이트

firewalld 패키지가 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- **firewalld** 의 이 버전에는 버전 0.7.0 이후의 모든 버그 수정이 포함되어 있습니다.
- **firewalld** 는 이제 **libnftables** JSON 인터페이스를 **nftables** 하위 시스템에 사용합니다. 이를 통해 규칙 애플리케이션의 성능과 안정성이 향상됩니다.
- 서비스 정의에서 새 **helper** 요소는 **모듈을** 대체합니다.
- 이 버전에서는 사용자 지정 도우미가 표준 도우미 모듈을 사용할 수 있습니다.

(BZ#1740670)

ndptool에서 IPv6 헤더에 대상 주소를 지정할 수 있음

이번 업데이트를 통해 **ndptool** 유틸리티는 IPv6 헤더에 주소를 지정하여 NS) 또는 Neighbor Advertisement(NA) 메시지를 특정 대상으로 보낼 수 있습니다. 결과적으로 링크-로컬 주소만 아닌 주소로 메시지를 보낼 수 있습니다.

(BZ#1697595)

nftables 에서 다차원 IP 집합 유형 지원

이 향상된 기능을 통해 **nftables** 패킷 필터링 프레임워크는 연결 및 간격이 있는 세트 유형을 지원합니다. 결과적으로 관리자는 더 이상 다차원 IP 집합 유형을 생성하기 위한 임시 해결책이 필요하지 않습니다.

(BZ#1593711)

nftables 가 4.4.3 버전으로 업데이트

nftables 패키지가 업스트림 버전 0.2.3으로 업그레이드되어 이전 버전에 비해 많은 버그 수정 및 개선 사항을 제공합니다.

- JSON API가 **libnftables** 라이브러리에 추가되었습니다. 이 라이브러리는 타사 애플리케이션에서 *nftables* 규칙 세트를 관리할 수 있는 고급 인터페이스를 제공합니다. Python에서 새 API를 사용하려면 **python3-nftables** 패키지를 설치합니다.
- 문은 IP 접두사 및 범위를 지원합니다(예: **192.0.2.0/24** 및 **192.0.2.0-192.0.2.30**).
- 예상된 운영 체제를 기반으로 패킷을 표시하기 위해 운영 체제 지문 지원이 추가되었습니다. 자세한 내용은 **nft(8)** 도움말 페이지의 **osf 표현식** 섹션을 참조하십시오.
- 패킷 헤더를 어떠한 방식으로든 변경하지 않고 패킷을 로컬 소켓으로 리디렉션하기 위해 투명한 프록시 지원이 추가되었습니다. 자세한 내용은 **nft(8)** 도움말 페이지의 **tproxy 문** 섹션을 참조하십시오.
- 기본적으로 **nft 체인은 nft** 체인을 만드는 동안 우선 순위 집합의 텍스트 이름을 표시합니다. 표준 우선 순위 숫자 값을 보려면 **-y** 옵션을 사용합니다. 자세한 내용은 표준 우선 순위 값 및 텍스트 이름 섹션을 참조하십시오.
- 보안 마크 지원이 추가되었습니다.
- 패킷 경로에서 업데이트를 설정하도록 동적 세트 업데이트에 대한 지원이 개선되었습니다.
- 전송 헤더 포트 일치에 대한 지원이 추가되었습니다.

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

- https://lore.kernel.org/netfilter-devel/20190624164910.defehs5giqziqnir@salvia/
- https://lore.kernel.org/netfilter-devel/20190819115807.myv6owxzblj2bthd@salvia/
- https://lore.kernel.org/netfilter-devel/20191202211737.xvmd6e6xxj4xvvjl@salvia/

(BZ#1643192)

firewalld 서비스의 규칙은 비표준 포트에서 실행되는 서비스에 연결 추적 도우미를 사용할 수 있습니다.

firewalld 서비스의 사용자 정의 도우미는 이제 표준 커널 도우미 모듈을 사용할 수 있습니다. 이를 통해 관리자는 **firewalld** 규칙을 생성하여 비표준 포트에서 실행되는 서비스에 연결 추적 도우미를 사용할 수 있습니다.

(BZ#1733066)

whois 패키지를 사용할 수 있습니다

이번 개선된 기능을 통해 이제 RHEL 8.2.0에서 **whois** 패키지를 사용할 수 있습니다. 결과적으로 특정 도메인 이름 또는 IP 주소에 대한 정보를 검색할 수 있습니다.

(BZ#1734183)

eBPF for tc 가 이제 완전히 지원됨

tc(트래픽 제어) 커널 하위 시스템과 the **tc** 툴은 eBPF(extended Berkeley Packet Filtering) 프로그램을 패킷 분류기 및 수신 및 송신 큐링 규칙 모두에 대한 작업으로 연결할 수 있습니다. 이는 커널 네트워크 데이터 경로 내에서 프로그래밍 가능한 패킷 처리를 가능하게 합니다. 이전에 기술 프리뷰로 사용 가능한 eBPF for **tc** 는 이제 RHEL 8.2에서 완전하게 지원됩니다.

(BZ#1755347)

5.1.7. 커널

RHEL 8.2의 커널 버전

Red Hat Enterprise Linux 8.2는 커널 버전 4.18.0-193과 함께 배포됩니다.

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

(BZ#1797671)

RHEL 8.2에 대한 Extended Berkeley Packet Filter

eBPF(Extended Berkeley Packet Filter)는 제한된 기능 집합에 액세스할 수 있는 제한된 샌드박스 환경에서 커널 공간에서 코드를 실행할 수 있는 커널 내 가상 시스템입니다. 가상 시스템은 특수 어셈블리와 유사한 코드를 실행합니다. **eBPF** 바이트코드는 먼저 커널로 로드된 다음 확인, 실시간 컴파일만 사용하여 네이티브 시스템 코드로 코드 변환한 다음 가상 시스템에서 코드를 실행합니다.

Red Hat은 **eBPF** 가상 시스템을 활용하는 다양한 구성 요소를 제공합니다. 각 구성 요소는 다른 개발 단계에 있으므로 현재 모든 구성 요소가 완전히 지원되지는 않습니다. RHEL 8.2에서는 다음 **eBPF** 구성 요소가 지원됩니다.

- 효율적인 커널 추적 및 조작 프로그램을 생성하기 위해 **eBPF** 가상 시스템을 사용하는 동적 커널 추적 유틸리티의 사용자 공간 컬렉션인 **BCC(BPF Compiler Collection)** 툴 패키지. **BCC** 는 **eBPF** 를 사용하여 Linux 운영 체제의 I/O 분석, 네트워킹 및 모니터링을 위한 툴을 제공합니다.

- **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.

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

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

- **bpftrace** 추적 언어
- **eXpress Data Path(XDP)** 기능

기술 프리뷰 구성 요소에 대한 자세한 내용은 기술 프리뷰를 참조하십시오.

(BZ#1780124)

Intel ® Fedora-Path Architecture(OPA) 호스트 소프트웨어

Intel-Path Architecture(OPA) 호스트 소프트웨어는 Red Hat Enterprise Linux 8.2에서 완벽하게 지원됩니다. Intel OPA는 클러스터형 환경의 컴퓨팅 노드와 I/O 노드 간의 고성능 데이터 전송(고급 대역폭, 높은 메시지 속도, 짧은 대기 시간)을 위해 HFI(Host Fabric Interface) 하드웨어에 초기화 및 설정을 제공합니다.

Intel✓-Path 아키텍처 문서 설치에 대한 지침은 https://cdrdv2.intel.com/v1/dl/getContent/616368를 참조하십시오.

(BZ#1833541)

Control Group v2 가 RHEL 8에서 완전 지원

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

이전 버전과 달리 **Control Group v2**에는 하나의 계층만 있습니다. 이 단일 계층을 통해 Linux 커널에서는 다음을 수행할 수 있습니다.

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

Control Group v2 에서는 다양한 컨트롤러를 지원합니다. 몇 가지 예는 다음과 같습니다.

- CPU 컨트롤러가 CPU 사이클의 배분을 조정합니다. 이 컨트롤러는 다음을 구현합니다.
  - 일반적인 스케줄링 정책에 대한 가중치 및 절대 대역폭 제한 모델
  - 실시간 스케줄링 정책에 대한 절대 대역폭 할당 모델.
- cpuset 컨트롤러는 프로세스의 프로세서 및/또는 메모리 배치를 **cpuset** 인터페이스 파일에 지정된 언급된 리소스로만 제한합니다.
- 메모리 컨트롤러가 메모리 할당을 조정합니다. 현재 다음과 같은 유형의 메모리 사용을 추적할 수 있습니다.
  - Userland 메모리 - 페이지 캐시 및 익명 메모리
  - dentries 및 inode와 같은 커널 데이터 구조

    - TCP 소켓 버퍼

- I/O 컨트롤러가 I/O 리소스 배분을 제한합니다.
- 쓰기 저장 컨트롤러는 메모리 및 I/O 컨트롤러와 상호작용하며 **Control Group v2** 고유의 것입니다.

위의 정보는 Control Group v2 업스트림 문서를 기반으로 했습니다. 동일한 링크를 참조하여 특정 **Control Group v2** 컨트롤러에 대한 자세한 정보를 얻을 수 있습니다.

아직 RHEL 8에서 업스트림 문서에 언급된 모든 기능이 구현되어 있는 것은 아닙니다.

(BZ#1401552)

사용 가능한 목록 임의화: 다이렉트 매핑 메모리 측 캐시의 성능 및 활용 향상

이 향상된 기능을 통해 페이지 할당자를 활성화하여 무료 목록을 임의로 설정하고 직접 매핑된 메모리 측 캐시의 평균 사용률을 향상시킬 수 있습니다. 커널 명령줄 옵션 **page_alloc.shuffle** 을 사용하면 페이지 할당자가 사용 가능한 목록을 임의로 설정하고 부울 플래그를 **True** 로 설정할 수 있습니다. **/sys/module/page_alloc/parameters/shuffle** 에 있는 **sysfs** 파일은 플래그 상태를 읽고, DRAM(Dynamic Random Access Memory)이 캐시되고, DRAM과 영구 메모리 사이의 대기 시간 대역폭이 줄어듭니다. 따라서 일반적인 서버 플랫폼에서 더 높은 용량과 낮은 대역폭을 가진 영구 메모리를 사용할 수 있습니다.

(BZ#1620349)

TPM 사용자 공간 도구가 마지막 버전으로 업데이트되었습니다

tpm2-tools 사용자 공간 도구가 버전 3.2.1로 업데이트되었습니다. 이번 업데이트에서는 특히 플랫폼 구성 등록 코드 및 도움말 페이지 정리와 관련된 여러 버그 수정을 제공합니다.

(BZ#1725714)

C620 시리즈 PCH 칩셋에서 Intel Trace Hub 기능을 지원

이번 업데이트에서는 Lewisburg PCH라고도 하는 C620 시리즈 PCH(Platform Controller Hub)에서 Intel Trace Hub (TH)에 대한 하드웨어 지원을 추가합니다. C620 시리즈 PCH를 사용하는 사용자는 이제 Intel TH를 사용할 수 있습니다.

(BZ#1714486)

perf 툴은 CLX-AP 및 CPX 프로세서에 대한 종료 이벤트 집계를 지원합니다.

이번 업데이트를 통해 이제 **perf** 툴에서 종료된 Intel CPU의 다이별 이벤트 수 집계를 지원합니다. 이 모드를 사용하려면 Xeon Cascade Lake **-AP(CLX-AP) 및 CPX(Extended Lake) 시스템 프로세서의 -a 옵션 외에도 --die** 옵션을 추가합니다. 결과적으로 이 업데이트는 종료 사이에 균형이 맞지 않습니다. **perf stat** 명령은 이벤트 수를 캡처하고 출력을 다음과 같이 표시합니다.

```
# perf stat -e cycles --per-die -a -- sleep 1
 Performance counter stats for 'system wide':
S0-D0        8      21,029,877      cycles
S0-D1        8      19,192,372      cycles
```

(BZ#1660368)

crashkernel=auto 의 임계값이 IBM Z에서 감소

이제 **crashkernel=auto** kernel 명령줄 매개 변수의 임계값이 IBM Z 시스템의 1G에서 1G로 줄어듭니다. 이

구현을 통해 IBM Z는 AMD64 및 Intel 64 시스템의 임계값에 맞춰 **crashkernel=auto** 의 더 낮은 임계값에서 동일한 예약 정책을 공유할 수 있습니다. 결과적으로 크래시 커널은 4GB 미만의 시스템에서 **kdump** 메모리를 자동으로 예약할 수 있습니다.

(BZ#1780432)

numactl manual 항목은 메모리 사용량 출력을 명확하게 표시합니다.

이번 RHEL 8 릴리스에서는 **numactl** 의 도움말 페이지에는 시스템의 상주 페이지만 반영되어 메모리 사용량 정보가 반영되어 있음을 명시적으로 언급합니다. 이렇게 추가되는 이유는 메모리 사용량 정보가 상주 페이지 또는 가상 메모리와 관련이 있는지 여부를 사용자에게 혼동할 수 있기 때문입니다.

(BZ#1730738)

Kdump FCoE 대상 지원을 포함하도록 kexec-tools 문서가 업데이트되었습니다.

이번 릴리스에서는 FCoE(Kdump Fibre Channel over Ethernet) 대상 지원을 포함하도록 **/usr/share/doc/kexec-tools/supported-kdump-targets.txt** 파일이 업데이트되었습니다. 결과적으로 사용자는 FCoE 대상 지원에서 **kdump** 크래시 덤프 메커니즘의 상태 및 세부 사항을 더 잘 이해할 수 있습니다.

(BZ#1690729)

펌웨어 지원 덤프에서 PowerNV 지원

이제 PowerNV 플랫폼에서 펌웨어 지원 덤프(**fadump**) 메커니즘이 지원됩니다. 이 기능은 IBM POWER9 FW941 펌웨어 버전에서 지원됩니다. 시스템 장애 발생 시 **fadump** 는 **vmcore 파일과** 함께 opal **core 파일도** 내보냅니다. opal **core** 파일에는 분석 시 OpenPOWER 추상화 계층(OPAL) 메모리 상태에 대한 정보가 포함되어 있습니다. opal **core** 파일은 OPAL 기반 시스템의 충돌을 디버깅하는 데 유용합니다.

(BZ#1524687)

kernel-rt 소스 트리가 최신 RHEL 8 트리와 일치

최신 RHEL 커널 소스 트리를 사용하도록 **kernel-rt** 소스가 업데이트되었습니다. 실시간 패치 세트도 최신 업스트림 v5.2.21-rt13 버전으로 업데이트되었습니다. 이 두 업데이트 모두 여러 버그 수정 및 개선 사항을 제공합니다.

(BZ#1680161)

rngd 는 루트가 아닌 권한으로 실행할 수 있습니다.

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

(BZ#1692435)

RHEL 8.2 이상 POWER 9 이상에서 가상 영구 메모리 지원

IBM POWER9 하드웨어에서 PowerVM 하이퍼바이저를 사용하여 RHEL 8.2 이상의 호스트를 실행하는 경우 이제 호스트에서 vPMEM(Virtual Persistent Memory) 기능을 사용할 수 있습니다. vPMEM을 사용하면 물리적 서버가 꺼질 때까지 애플리케이션에서 데이터가 유지되고 파티션이 다시 시작됩니다. 따라서 vPMEM을 사용하는 워크로드를 다시 시작하면 훨씬 빨라집니다.

시스템에서 vPMEM을 사용할 수 있으려면 다음 요구 사항을 충족해야 합니다.

- HMC(하드웨어 관리 콘솔) V9R1 M940 이상

- 펌웨어 수준 FW940 이상
- E980 시스템 펌웨어 FW940 이상
- L922 시스템 펌웨어 FW940 이상
- PowerVM 수준 V3.1.1

현재 vPMEM과 함께 RHEL 8에서 알려진 여러 문제가 발생합니다. 자세한 내용은 기술 자료 문서를 참조하십시오.

- pmem 메모리의 핫플러그/연결 해제로 인해 POWER9에서 커널 패닉 상태가 발생할 수 있습니다.
- 캡처 커널의 부팅은 vPMEM 네임스페이스를 kdump/fadump의 덤프 대상으로 사용하는 데 시간이 오래 걸립니다.

(BZ#1859262)

5.1.8. 파일 시스템 및 스토리지

LVM에서 dm-writecache 캐싱 방법 지원

이제 LVM 캐시 볼륨에서 기존 **dm-cache 방법 외에도 dm-write cache** 캐싱 방법을 제공합니다.

dm-cache

이 방법은 빠른 볼륨에 캐싱하여 자주 사용하는 데이터에 대한 액세스를 가속화합니다. 이 방법은 읽기 및 쓰기 작업을 모두 캐시합니다.

dm-writecache

이 메서드는 쓰기 작업만 캐시합니다. SSD 또는 영구 메모리(PMEM) 디스크의 빠른 볼륨은 쓰기 작업을 먼저 저장한 다음 백그라운드의 느린 디스크로 마이그레이션합니다.

캐싱 방법을 구성하려면 **lvconvert** 유틸리티와 함께 **--type cache 또는 --type writecache** 옵션을 사용합니다.

자세한 내용은 캐싱 활성화를 통해 논리 볼륨 성능을 향상시키는 것을 참조하십시오.

(BZ#1600174)

VDO 비동기 정책이 ACID와 호환

이번 릴리스에서는 VDO **비동기** 쓰기 모드가 이제 Atomicity, Consistency, Isolation, Durability(ACID)와 호환됩니다. VDO가 **비동기** 모드에서 데이터를 작성하는 동안 시스템이 예기치 않게 중지되면 복구된 데이터가 항상 일관되게 유지됩니다.

ACID 규정 준수로 인해 이제 **비동기** 성능이 이전 릴리스에 비해 더 낮습니다. 원래 성능을 복원하려면 VDO 볼륨의 쓰기 모드를 ACID와 호환되지 않는 **비동기-비** 보안 모드로 변경할 수 있습니다.

자세한 내용은 Selecting a VDO write mode 에서 참조하십시오.

(BZ#1657301)

VDO 볼륨을 가져올 수 있습니다

vdo 유틸리티를 사용하면 현재 시스템에 등록되어 있지 않은 기존 VDO 볼륨을 가져올 수 있습니다. VDO 볼륨을 가져오려면 **vdo import** 명령을 사용합니다.

또한 **vdo import** 명령을 사용하여 VDO 볼륨의 UUID(Universally Unique Identifier)를 수정할 수도 있습니다.

(BZ#1713749)

mountstats 및 nfsiostat의 출력에서 새로운 per-op 오류 카운터를 사용할 수 있습니다.

NFS 클라이언트 시스템에서 마이너 지원 기능을 사용할 수 있습니다. nfs **-utils** 의 **mountstats** 및 **nfsiostat** 명령의 출력에는 작업 **별 오류** 수가 있습니다. 이 향상된 기능을 통해 이러한 툴은 NFS 클라이언트 시스템의 특정 NFS 마운트 지점에서 문제를 줄이는 데 도움이 되는 작업 **별 오류** 수 및 백분율을 표시할 수 있습니다. 이러한 새 통계는 Red Hat Enterprise Linux 8.2 커널 내에 있는 커널 변경 사항에 따라 달라집니다.

(BZ#1719983)

cgroup 인식을 사용하여 쓰기 IO를 XFS에서 사용할 수 있습니다

이번 릴리스에서 XFS는 **cgroup** 인식을 통해 나중 IO를 지원합니다. 일반적으로 **cgroup** 쓰기에는 기본 파일 시스템의 명시적 지원이 필요합니다. 지금까지 XFS의 writeback IO는 루트 **cgroup** 의 속성입니다.

(BZ#1274406)

FUSE 파일 시스템에서 copy_file_range()을 구현합니다.

copy_file_range() 시스템 호출은 파일 시스템에서 효율적인 데이터 복사 메커니즘을 구현할 수 있는 방법을 제공합니다. 이번 업데이트를 통해 FUSE(Userspace) 프레임워크에서 Filesystem을 사용하는 GlusterFS는 이 메커니즘을 활용합니다. FUSE 파일 시스템의 읽기/쓰기 기능에는 여러 개의 데이터 사본이 포함되어 있으므로 **copy_file_range()** 를 사용하면 성능이 크게 향상될 수 있습니다.

(BZ#1650518)

mountstats 및 nfsiostat 명령에 대해 작업별 통계 지원을 사용할 수 있습니다.

이제 NFS 클라이언트 시스템에서 지원 기능을 사용할 수 있습니다. **/proc/self/mountstats** 파일에는 작업 **별 오류 카운터** 가 있습니다. 이번 업데이트를 통해 각 **작업별** 통계 행에서 9번째 숫자는 상태 값 0으로 완료된 작업 수를 나타냅니다. 이 상태 값은 오류가 있음을 나타냅니다. 자세한 내용은 이러한 새 오류 수를 표시하는 **nfs -utils의 mountstats 및 nfs iostat** 프로그램에 대한 업데이트를 참조하십시오.

(BZ#1636572)

/proc/self/mountstats 파일에서 새 마운트 stats lease_time 및 lease_expired 를 사용할 수 있습니다.

NFSv4.x 클라이언트 시스템에서 지원 기능을 사용할 수 있습니다. **nfsv4로 시작하는 행의 끝에 /proc/self/mountstats 파일에는 lease_time 및 lease_expired 필드가 있습니다. lease_time** 필드는 NFSv4 리스 시간의 초 수를 나타냅니다. **lease_expired** 필드는 리스가 만료된 이후 초 수를 나타내며 리스가 만료되지 않은 경우 0을 나타냅니다.

(BZ#1727369)

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)

5.1.9. 고가용성 및 클러스터

다른 리소스에 영향을 미치지 않는 경우에만 리소스를 비활성화하는 새로운 명령 옵션

다른 리소스에 영향을 미치지 않는 경우에만 리소스를 비활성화해야 합니다. 복잡한 리소스 관계가 설정되면 이러한 상황이 직접 수행할 수 없도록 합니다. 이 요구를 해결하기 위해 **pcs resource disable** 명령에서 다음 옵션을 지원합니다.

- **pcs resource disable --simulate**: 클러스터 구성을 변경하지 않고 지정된 리소스 비활성화의 효과 표시
- **pcs resource disable --safe**: 한 노드에서 다른 노드로 마이그레이션되는 등 다른 리소스가 영향을 받지 않는 경우에만 지정된 리소스를 비활성화합니다.
- **pcs resource disable --safe --no-strict**: 다른 리소스가 중지되거나 강등되지 않는 경우에만 지정된 리소스를 비활성화합니다.

또한 **pcs resource safe-disable** 명령은 **pcs resource disable --safe** 의 별칭으로 도입되었습니다.

(BZ#1631519)

리소스 간의 관계를 표시하는 새 명령

새로운 **pcs resource Relations** 명령을 사용하여 트리 구조에서 클러스터 리소스 간 관계를 표시할 수 있습니다.

(BZ#1631514)

기본 사이트 및 복구 사이트 클러스터의 상태를 표시하는 새로운 명령

복구 사이트로 사용할 클러스터를 구성한 경우 **pcs dr** 명령을 사용하여 해당 클러스터를 복구 사이트 클러스터로 구성할 수 있습니다. 그런 다음 **pcs dr** 명령을 사용하여 단일 노드에서 기본 사이트 클러스터와 복구 사이트 클러스터의 상태를 모두 표시할 수 있습니다.

(BZ#1676431)

제한 조건을 나열할 때 만료된 리소스 제약 조건이 기본적으로 숨겨집니다.

기본적으로 리소스 제한 조건을 나열하지 않으면 만료된 제약 조건이 표시됩니다. 만료된 보존을 포함하려면 pcs constraint **명령** 의 **--all** 옵션을 사용합니다. 그러면 만료된 제약 조건이 나열되고 해당 제한 조건 및 관련 규칙이 디스플레이의 **(수료됨)** 로 표시됩니다.

(BZ#1442116)

정리 노드 종료 시 중지된 상태로 유지되도록 리소스를 구성하는 Pacemaker 지원

클러스터 노드가 종료되면 Pacemaker의 기본 응답은 해당 노드에서 실행 중인 모든 리소스를 중지하고 다른 위치에서 복구하는 것입니다. 일부 사용자는 오류에 대해서만 고가용성을 유지하고 정리된 종료를

예약된 중단으로 처리하는 것을 선호합니다. 이 문제를 해결하기 위해 Pacemaker에서 **shutdown-lock** 및 **shutdown-lock-limit** 클러스터 속성을 지원하여 다음 노드가 다시 참여할 때까지 종료할 때 노드에서 활성화된 리소스가 중지되도록 지정합니다. 이제 사용자는 수동 조작 없이 예약된 중단으로 클린 종료를 사용할 수 있습니다. 클린 노드 종료 시 중지된 상태로 유지되도록 리소스를 구성하는 방법에 대한 자세한 내용은 링크를 참조하십시오. 정리 노드 종료 시 중지된 상태로 유지되도록 리소스 구성 .

(BZ#1712584)

단일 노드에서 클러스터 환경 실행 지원

하나의 멤버만 구성된 클러스터는 이제 클러스터 환경에서 리소스를 시작하고 실행할 수 있습니다. 이를 통해 사용자는 백업에 단일 노드를 사용하는 다중 노드 클러스터에 대해 별도의 재해 복구 사이트를 구성할 수 있습니다. 하나의 노드만 있는 클러스터는 내결함성이 없습니다.

(BZ#1700104)

5.1.10. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

새 모듈: python38

RHEL 8.2에는 새 모듈 **python38** 및 **ubi8/python-38** 컨테이너 이미지에서 제공하는 Python 3.8이 도입되었습니다.

Python 3.6과 비교하여 주요 개선 사항은 다음과 같습니다.

- **contextvars**,**dataclasses** 또는 **importlib.resources**와 같은 새로운 Python 모듈
- 할당 표현식 (so- called walrus operator, **:=**) 또는 위치 전용 매개변수와 같은 새로운 언어 기능
- **breakpoint()** 기본 제공 함수, **=** 형식 문자열 사양 및 디버그 및 비디버그 빌드와 확장 모듈 간의 호환성 개선
- 성능 향상
- 선택적 정적 유형 힌트 지원 개선
- 쉬운 디버깅을 위해 형식화된 문자열 리터럴(f-strings)에 **=** 지정자를 추가했습니다.
- **pip**,**requests** 또는 **Cython**과 같은 업데이트된 패키지 버전

Python 3.8 및 여기에 구축된 패키지는 동일한 시스템에서 Python 3.6과 병렬로 설치할 수 있습니다.

python38 모듈에는 python 36 모듈에 제공된 시스템 도구(RPM, DNF, SELinux 등)에 대한 동일한 바이너리 바인딩이 포함되어 있지 않습니다.

python38 모듈에서 패키지를 설치하려면 다음을 사용합니다. 예를 들면 다음과 같습니다.

```
# yum install python38
# yum install python38-Cython
```

python38:3.8 모듈 스트림은 자동으로 활성화됩니다.

인터프리터를 실행하려면 다음을 사용합니다.

```
$ python3.8
$ python3.8 -m cython --help
```

자세한 내용은 Python 사용을 참조하십시오.

Red Hat은 RHEL 8의 라이프 사이클이 종료될 때까지 Python 3.6에 대한 지원을 계속 제공합니다. Python 3.8은 라이프사이클이 짧고 RHEL 8 Application Streams 라이프 사이클을 참조하십시오.

(BZ#1747329)

mod_wsgi 설치의 변경 사항

이전에는 **yum install mod_wsgi** 명령을 사용하여 **mod_wsgi** 모듈을 설치하려고 할 때 **python3-mod_wsgi** 패키지가 항상 설치되었습니다. RHEL 8.2에서는 Python 3.6에 추가된 Python 3.8이 도입되었습니다. 이번 업데이트를 통해 설치할 **mod_wsgi** 버전을 지정해야 합니다. 그렇지 않으면 오류 메시지가 반환됩니다.

Python 3.6 버전의 **mod_wsgi** 를 설치하려면 다음을 수행합니다.

```
# yum install python3-mod_wsgi
```

Python 3.8 버전의 **mod_wsgi** 를 설치하려면 다음을 수행합니다.

```
# yum install python38-mod_wsgi
```

python3-mod_wsgi 및 **python38-mod_wsgi** 패키지가 서로 충돌하며 Apache HTTP Server의 제한으로 인해 하나의 **mod_wsgi** 모듈만 시스템에 설치할 수 있습니다.

이러한 변경으로 BZ#1829692 에 설명된 종속성에 알려진 문제가 발생했습니다.

(BZ#1779705)

IBM Z의 zlib 에서 하드웨어 가속화 제거 지원

이번 업데이트에서는 하드웨어 가속화 제거 알고리즘을 IBM Z 메인프레임의 **zlib** 라이브러리에 추가로 지원합니다. 그 결과 IBM Z 벡터 시스템의 압축 및 압축 해제 성능이 향상되었습니다.

(BZ#1659433)

IBM Power Systems에서 gzip 압축을 풀 때 성능이 향상되었습니다. little endian

이번 업데이트에서는 little endian인 IBM Power Systems의 **zlib** 라이브러리에 32비트 Cyclic 중복 검사(CRC32)에 대한 최적화를 추가합니다. 그 결과 **gzip** 파일 압축 해제 성능이 향상되었습니다.

(BZ#1666798)

새 모듈 스트림: maven:3.6

RHEL 8.2에는 새로운 모듈 스트림 **maven:3.6** 이 도입되었습니다. 이 버전의 Maven 소프트웨어 프로젝트 관리 및 이해 도구에서는 RHEL 8.0과 함께 배포된 **maven:3.5** 스트림에 대해 수많은 버그 수정 및 다양한 개선 사항을 제공합니다.

maven:3.6 스트림을 설치하려면 다음을 사용합니다.

```
# yum module install maven:3.6
```

maven:3.5 스트림에서 업그레이드하려면 이후 스트림으로 전환을 참조하십시오.

(BZ#1783926)

mod_md 가 ACMEv2 프로토콜 지원

mod_md 모듈이 버전 2.0.8로 업데이트되었습니다. 이번 업데이트에는 여러 가지 기능이 추가되어 특히 IETF(Internet Engineering Task Force) 표준(RFC 8555)인 ACME(Automatic Certificate Management Environment) 인증서 발급 및 관리 프로토콜 버전 2를 지원합니다. 원래 ACMEv1 프로토콜은 계속 지원되지만 인기 있는 서비스 프로바이더가 더 이상 사용되지 않습니다.

(BZ#1747923)

PHP 7.3의 새로운 확장 기능

php:7.3 모듈 스트림이 2개의 새로운 PHP 확장을 제공하도록 업데이트되었습니다(**rrd** 및 **Xdebug**).

rrd 확장에서는 **RRDtool** C 라이브러리에 대한 바인딩을 제공합니다. **RRDtool** 은 시계열 데이터를 위한 고성능 데이터 로깅 및 그래프 시스템입니다.

Xdebug 확장 기능은 디버깅 및 개발을 지원하기 위해 포함되어 있습니다. 확장 기능은 개발 목적으로만 제공되며 프로덕션 환경에서 사용해서는 안 됩니다.

RHEL 8에서 PHP를 설치 및 사용하는 방법에 대한 자세한 내용은 PHP 스크립팅 언어 사용을 참조하십시오.

(BZ#1769857, BZ#1764738)

새로운 패키지: perl-LDAP 및 perl-Convert-ASN1

이번 업데이트에서는 **perl-LDAP** 및 **Perl-Convert-ASN1** 패키지가 RHEL 8에 추가되었습니다. **perl-LDAP** 패키지는 Perl 언어에 대한 LDAP 클라이언트를 제공합니다. **perl-LDAP 에는 perl-Convert-ASN1** 패키지가 필요합니다. 이 패키지는 AASN.1) 데이터 구조를 인코딩 및 디코딩합니다.

(BZ#1663063, BZ#1746898)

SSCG 에서 암호로 보호되는 개인 키 파일 생성 지원

sscg 유틸리티는 이제 암호로 보호되는 개인 키 파일을 생성할 수 있습니다. 이로 인해 개인 키에 대한 또 다른 보호 수준이 추가되며 FreeRADIUS와 같은 일부 서비스에 필요합니다.

(BZ#1717880)

5.1.11. 컴파일러 및 개발 도구

Grafana 가 6.3.6 버전으로 업데이트

grafana 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 6.3.6으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- 데이터베이스: 성능 향상을 위해 시스템 통계 쿼리를 다시 작성합니다.
- 탐색:
  - Safari 브라우저의 분할 뷰에서 쿼리 필드 레이아웃을 수정합니다.
  - 지원되는 데이터 소스에 대한 Live 옵션을 추가하고 공유를 위해 URL에 **orgId** 를 추가합니다.
  - 레이블 엔드포인트에 대한 새로운 **loki start** 및 **end** 매개 변수에 대한 지원을 추가합니다.
  - Explore에서 원시 쿼리 모드 전환을 지원하여 메트릭과 로그 간에 전환할 수 있습니다.

- 는 로그 줄 컨텍스트를 표시합니다. 필드 또는 레이블에서 제공하는 경우 로그 수준을 구문 분석하지 않습니다.
- 새 **LogQL** 필터링 구문을 지원합니다.
- Grafana/UI의 새로운 **TimePicker** 를 사용합니다.
- **LogRow** Highlighter에서 줄 바꿈 처리.
- 대시보드 패널로 돌아가는 수정 사항.
- 픽스는 로그 그래프의 시리즈 수준별로 필터링합니다.
- 로드 및 그래프/테이블이 축소될 때 문제를 해결합니다.
- 로그 행의 선택/복사 수정.

- 대시보드: 대시보드 **init** 이 누락된 패널 링크를 사용하여 대시보드 init 로드 오류를 수정하고 쉼표로 구분된 값(CSV) 데이터 링크로 내보내는 동안 시간대 대시보드 설정을 수정합니다.
- 편집기: 전체 행만 복사되는 문제를 해결합니다.
- LDAP: **다중 ldap 및 ldap 인증 구성 요소 통합.**
- **프로필/사용자관리자: 32비트 빌드의 grafana-server 를 충돌하는 사용자 에이전트 구문 분석기를 수정합니다.**
- **Prometheus:**
  - **Prometheus 데이터 소스로 전환하는 동안 패널 편집기 충돌을 방지하고 소괄호 삽입을 덜어줍니다.**
  - **label_replace 로 쿼리를 수정하고 쿼리 편집기를 로드할 때 $1 일치를 제거합니다.**
  - **편집기에서 여러 줄로 쿼리하여 단계 정렬을 고려하는 시간대를 일관되게 허용합니다.**
  - **대시보드 범위 대신 $__range 에 재정의된 패널 범위를 사용합니다.**
  - **시계열 필터를 쿼리, 이스케이프 | 보간 PromQL 변수의 리터럴에 추가합니다.**
  - **Explore에 콜론이 포함된 지표의 레이블을 추가하는 동안 수정됩니다.**

- **auth: HTTP API**에 사용자 인증 토큰을 나열하는 동안 **API** 키 만료, 장치, **os** 및 브라우저를 반환하고, **UI**에서 사용자 인증 토큰을 나열하고 취소할 수 있습니다.

- **DataLinks:** 범위가 지정된 변수를 데이터 링크에 올바르게 적용하고, 그래프 컨텍스트 메뉴에 데이터 포인트 타임스탬프를 표시하는 동안 시간대를 따라 변수를 보간 경우 데이터 포인트 타임스탬프를 올바르게 사용하고 **${__series_name}** 의 잘못된 보간을 수정합니다.

- 그래프**:** 시리즈 줄 아이콘을 클릭하고 창에 수평 스크롤바가 표시되는 문제를 해결하고 새로운 채우기 **gradient** 옵션을 추가합니다.

- 그래프**:** 단일 값 배열 변수의 글러브를 방지하고 별칭 함수가 마지막으로 이동되는 문제를 해결하고 변수 매개 변수를 사용하여 **seriesByTag &** 함수의 문제를 수정하고 **/metrics/find** 요청에 **POST** 를 사용합니다.

- **TimeSeries:** 값이 모든 숫자라고 가정합니다.

- 게이지**(Gauge)**/가우게**(Gauge):** 손실된 임계값과 **avg** 통계를 사용하여 **Gauge**를 로드하는 문제를 해결합니다.

- 패널 링크**:** 패널 링크 **(drill down link)**로 **Gauge & Bar Gauge** 패널의 충돌 문제를 수정하고 패널 설명이 없는 동안 렌더링 문제를 해결합니다.

- **OAuth:** 동일한 쿠키 정책으로 인해 누락된 상태 **OAuth** 로그인 오류를 수정하고 **DS** 프록시의 **OAuth** 새로 고침에서 잘못된 사용자 토큰에 대한 수정 사항을 수정합니다.

- 인증 프록시**:** 추가 헤더를 캐시 키의 일부로 포함합니다.

- **cli: dev** 모드에서 **sql** 오류로 인해 **encrypt-datasource-passwords** 오류가 발생한 문제를 해결합니다.

- 권한**:** 관리자 이외의 사용자의 탐색에 플러그인을 표시하지만 플러그인 구성을 숨깁니다.

- **timepicker:** 빠른 범위 드롭다운의 최대 높이를 높이고 사용자 지정 범위 팝업에 대한 스타일 문제를 수정합니다.

- 로키: 탐색에서 올바른 순서로 실시간 테일링된 로그를 표시합니다.
- 시간 범위: 사용자 지정 시간 범위가 UC(Universal Time Coordinated)를 따르지 않은 버그 수정.
- remote_cache: redis connstr 구문 분석 수정.
- 경고: 지정된 모든 이메일 주소에 이메일 알림을 보내려고 시도하는 경고 규칙에 태그를 추가하고, 경고 규칙 테스트를 개선하며 Discord 경고 알림 알림에 대한 콘텐츠 필드 구성을 지원합니다.
- Alertmanager: 레이블 이름에서 잘못된 문자를 밑줄로 바꿉니다.
- AzureMonitor: 변경 사항은 Azure 로그의 기본 제공 Grafana 변수 또는 매크로 이름을 충돌합니다.
- CloudWatch: AWS(Amazon Web Services) Cloudwatch Expressions에 대해 리전을 표시한 경우 AWS DocDB 지표를 추가합니다.
- GraphPanel: 범례 테이블과 정렬 열이 표시되지 않을 때 시리즈를 정렬하지 마십시오.
- InfluxDB: 탐색에서 로그 시각화 지원.
- MySQL/Postgres/MSSQL: 일, 주, 연도 간격을 매크로에 대한 구문 분석 기능을 추가하여 주기적으로 클라이언트 인증서를 다시 로드할 수 있도록 지원합니다.
- 플러그인: dataFormats 목록을 plugin.json 파일의 skipDataQuery 플래그로 교체합니다.
- 새로 고침 선택기: 빈 간격을 처리합니다.

- **singlestat: singlestat에 y min/max 구성을 추가합니다.**

- **템플릿: 페이지를 다시 로드한 후 다중 값 변수에 __text 를 올바르게 표시하고, 다중 값 변수의 필터링된 값을 모두 선택할 수 있습니다.**

- **프론트엔드: Json 트리 구성 요소가 작동하지 않는 문제를 해결합니다.**

- **InfluxDB: 레이블 값 필터에서 이스케이프되지 않은 작은따옴표로 문제를 해결합니다.**

- **config: defaults.ini 파일의 remote_cache 에 대한 connectionstring 옵션을 수정합니다.**

- **Elasticsearch: 빈 쿼리(템플릿 변수를 통해)를 와일드카드로 전송하고 기본 최대 동시 shard 요청을 수정하고 탐색기에서 로그 시각화를 지원합니다.**

- **TablePanel: 주석 표시를 수정합니다.**

- **Grafana-CLI: 명령줄을 통해 플래그 수신, RPM/DEB 패키지 내의 grafana-cli 에 대한 래퍼 및 config/homepath 가 이제 전역 플래그입니다.**

- **HTTPServer: X-XSS-Protection 헤더 포맷, 새 헤더 X-Content-Type-Options,X- XSS-Protection 및 Strict- Transport -Security를 반환하는 옵션에서 Strict-Transport -Security 헤더를 수정하고 사용자 지정 URL 경로 접두사를 사용하여 Grafana를 제공합니다.**

(BZ#1725278)

PCP 는 5.0.2 버전으로 업데이트

pcp 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 5.0.2로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- **pcp-webapp-* 패키지는 이제 grafana-pcp 패키지 및 pmproxy 로 교체됩니다.**

- **pcp-collectl** 툴이 **pmrep** 구성으로 교체되었습니다.
- 새로운 성능 지표 도메인 에이전트(**PMDA**):
  - **pmdamssql: Microsoft SQL Server** 구현을 위한 새로운 **PMDA.**
  - **pmdanetcheck:** 네트워크 점검을 수행하는 새로운 **PMDA.**
  - **pmdaopenmetrics: prometheus** 에이전트의 이름을 **openmetrics** 로 바꿉니다.
  - **pmdanfsclient:** 작업 당 및 마운트 당 **rpc** 오류 지표를 추가합니다.
  - **pmdalmsensors:** 이름 구문 분석 및 오류 처리 개선 사항.
  - **pmdaperfevent:** 다중 노드 시스템에서 **hv_24x7** 중첩 이벤트를 지원합니다.
  - **pmdalinux:**
    - 스파스 또는 중단된 마이크로마 노드를 올바르게 처리합니다.
    - **CPU** 당 **numa** 통계의 **instid**가 아닌 **cpu in stname** 을 사용합니다.
    - **slabinfo v2** 구문 분석에 활성 및 총 슬래브 추가
    - 여러 **unix** 소켓, **icmp6** 메트릭, **hugepage** 메트릭 값을 수정합니다. 계산, 큰 **CPU** 수가 있는 인터럽트 코드의 **segfault**
    - **--container** 네임스페이스에서 더 많은 네트워크 지표를 가져옵니다.

- **pmdabcc: bcc 0.10.0** 이상 버전의 **tracepoints** 모듈 수정
- **pmdabpftrace: bpftrace** 스크립트의 메트릭에 대한 새로운 **PMDA**
- **pmdaproc:**
  - **pidlist** 새로 고침의 메모리 누수 수정.
  - **cgroups_scan** 에서 과도한 통계 호출을 방지합니다.
  - **cgroup** 경로를 유지하고 인스턴스 이름만 분리합니다.
- **pmdaroot: cgroup** 동작을 캐시하거나 비활성으로 처리하고 **cgroup fs** 에서 컨테이너를 완전히 새로 고침합니다.

- 수집기(서버) 툴 수정:
  - **pmproxy: Openmetrics**는 **/metrics** 엔드포인트를 통해 지원하고 **pmseries/grafana REST API**를 통합하며 새로운 비동기 **PMWEBAPI(3) REST API** 구현을 추가합니다.
  - **selinux:** 수많은 **pcp** 정책 업데이트.
  - **python pmdas:** 인증 지원, 새로운 **set_comm_flags** 메서드를 활성화하여 통신 플래그를 설정합니다.
  - **python api: pmdaGetContext()** 를 내보내고 디버깅 래퍼를 추가합니다.
  - **perl api: python** 래퍼와 같이 **PMDA** 저장소에 대해 컨텍스트를 설정합니다.
  - **systemd:** 모든 서비스에 **120s** 시간 초과를 추가하고 **pmlogger** 서비스를 시작하지 못

한 수정 사항을 추가합니다.

- 분석 (클라이언트) 도구 수정:
  - **pmchart:** 가져오기 오류 조건에서 차트 자동 스케일링을 수정합니다.
  - **pmrep: gather I-dm-sD** 및 **collectl-sD** 에 대한 **wait.formula** 를 수정합니다.
  - **PMseries: delta** 키워드 및 더 나은 타임스탬프를 지원합니다.
  - **pcp-atop: proc vs hotproc** 지표를 처리하도록 쓰기 모드(**-w**)를 수정합니다.
  - **pcp-atopsar:** 몇 가지 명령행 인수의 오용을 수정합니다.
  - **pcp-dstat: CSV** 출력의 헤더가 잘못 정렬되고 **--bits** 명령줄 옵션 처리가 수정되었습니다.
  - **libpcp:** 손상된 아카이브에 대한 로컬 컨텍스트 및 다중 아카이브 재생 오류 처리를 사용하여 **cockpit-pcp segv** 를 수정합니다.

(BZ#1723598)

RHEL 8.2에서 Grafana -pcp 사용 가능

grafana-pcp 패키지는 **grafana**와 **PCP** 를 연결하는 새로운 **grafana** 데이터 소스 및 애플리케이션 플러그인을 제공합니다 . **grafana-pcp** 패키지를 사용하면 각각 **pmseries** 쿼리 언어와 **pm webapi** 라이브 서비스를 사용하여 기록 **PCP** 지표 및 실시간 **PCP** 지표를 분석할 수 있습니다. 자세한 내용은 Performance Co-Pilot Grafana 플러그인을 참조하십시오.

(BZ#1685315)

업데이트된 GCC 툴 세트 9

GCC Toolset 9는 최신 버전의 개발 툴을 제공하는 컴파일러 툴셋입니다. **AppStream** 리포지토리의

소프트웨어 컬렉션 형태로 애플리케이션 스트림으로 사용할 수 있습니다.

RHEL 8.2에서 도입한 주요 변경 사항은 다음과 같습니다.

- GCC 컴파일러가 버전 9.2.1로 업데이트되어 업스트림 GCC에서 사용할 수 있는 많은 버그 수정 및 개선 사항을 제공합니다.
- 이제 GCC Toolset 9 구성 요소를 두 컨테이너 이미지에서 사용할 수 있습니다.
  - rhel8/gcc-toolset-9-toolchain 에는 GCC 컴파일러, GDB 디버거 및 make 자동화 도구가 포함됩니다.
  - rhel8/gcc-toolset-9-perftools 는 SystemTap 및 Valgrind와 같은 성능 모니터링 툴을 포함합니다.

    컨테이너 이미지를 가져오려면 다음 명령을 root로 실행합니다.

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

다음 도구와 버전은 GCC Toolset 9에서 제공합니다.

툴	버전
GCC	9.2.1
GDB	8.3
valgrind	3.15.0
SystemTap	4.1
Dyninst	10.1.0
binutils	2.32
elfutils	0.176
dwz	0.12

툴	버전
Make	4.2.1
strace	5.1
ltrace	0.7.91
annobin	9.08

GCC Toolset 9를 설치하려면 root로 다음 명령을 실행합니다.

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

GCC Toolset 9에서 도구를 실행하려면 다음을 수행합니다.

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

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

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

자세한 내용은 GCC Toolset 사용을 참조하십시오.

(BZ#1789401)

GCC Toolset 9에서 NVIDIA ICX 대상 오프로딩 지원

GCC Toolset 9의 GCC 컴파일러는 NVIDIA의 OpenMP 대상 오프로딩을 지원합니다.

(BZ#1698607)

업데이트된 GCC 컴파일러를 RHEL 8.2에 사용할 수 있습니다.

시스템 GCC 컴파일러 버전 8.3.1이 업스트림 GCC에서 사용할 수 있는 수많은 버그 수정 및 개선 사항을 포함하도록 업데이트되었습니다.

GCC(GNU 컴파일러 컬렉션)는 C, C++ 및 Fortran 프로그래밍 언어를 사용하여 애플리케이션을 개발하기 위한 툴을 제공합니다.

사용법 정보는 RHEL 8에서 C 및 C++ 애플리케이션 개발에서 참조하십시오.

(BZ#1747157)

glibc에서 최대 fastbin 크기를 변경하는 새로운 튜닝 가능 항목

fat oc 함수는 재사용 가능한 메모리 청크를 특정 크기까지 유지하는 일련의 fastbins를 사용합니다. 기본 청크 크기는 32비트 시스템의 경우 80바이트이고 64비트 시스템에서 160바이트입니다. 이 향상된 기능으로 최대 fastbin 크기를 변경할 수 있는 새로운 glibc.malloc.mxfast 튜닝 가능 항목이 glibc에 추가되었습니다.

(BZ#1764218)

GCC Toolset 9에서 GNU Fortran에 대해 벡터화된 수학 라이브러리가 활성화됨

이 향상된 기능을 통해 GCC 도구 세트의 GNU Fortran은 이제 벡터화된 수학 라이브러리 libmvec 의 루틴을 사용할 수 있습니다. 이전에는 GCC 툴 세트의 Fortran 컴파일러가 GNU C 라이브러리 glibc 에서 제공하는 libmvec 의 루틴을 사용하기 전에 Fortran 헤더 파일이 필요했습니다.

(BZ#1764238)

glibc.malloc.tcache 튜닝 가능 항목이 향상되었습니다.

glibc.malloc.tcache_count 튜닝 가능 항목을 사용하면 스레드별 캐시(tcache)에 저장할 수 있는 각 크기의 최대 메모리 청크 수를 설정할 수 있습니다. 이번 업데이트를 통해 glibc.malloc.tcache_count 튜닝 가능 항목의 상한이 127에서 65535로 증가했습니다.

(BZ#1746933)

glibc 동적 로더가 상속되지 않는 라이브러리 사전 로드 메커니즘을 제공하도록 향상되었습니다.

이 향상된 기능을 통해 이제 --preload 옵션으로 사용자 프로그램을 로드하도록 로더를 호출하고, 사전 로드할 콜론으로 구분된 라이브러리 목록을 추가할 수 있습니다. 이 기능을 사용하면 상속되지 않는 라이브러리 사전 로드 목록을 사용하여 로더를 통해 직접 프로그램을 호출할 수 있습니다.

이전에는 환경을 통해 모든 하위 프로세스에서 상속한 LD_PRELOAD 환경 변수를 사용해야 했습니다.

(BZ#1747453)

GDB는 IBM Z 아키텍처에서 ARCH(13) 확장 지원

이번 개선된 기능을 통해 GDB(GNU Debugger)는 IBM Z 아키텍처에서 ARCH(13) 확장에 의해 구현된 새 명령을 지원합니다.

(BZ#1768593)

elfutils 를 버전 0.178로 다시 기반

elfutils 패키지가 여러 버그 수정 및 개선 사항을 제공하는 버전 0.178으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- elfclassify: ELF 객체를 분석하는 새로운 툴입니다.
- debuginfod: 인덱스에 대한 새로운 서버, 클라이언트 툴 및 라이브러리가 HTTP를 통해 파일 및 RPM 아카이브에서 ELF, DWARF, 소스를 자동으로 가져옵니다.
- 이제 libebl 이 libdw.so 로 직접 컴파일됩니다.
- eu-readelf 에는 메모, 섹션 번호 지정 및 기호 테이블에 대한 여러 개의 새 플래그가 있습니다.
- libdw 는 멀티스레딩 지원이 개선되었습니다.
- libdw 는 추가 GNU DWARF 확장을 지원합니다.

(BZ#1744992)

SystemTap 버전 4.2로 업데이트

SystemTap 계측 툴이 버전 4.2로 업데이트되었습니다. 주요 개선 사항은 다음과 같습니다.

- 이제 backtraces에 소스 파일 이름과 행 번호가 포함될 수 있습니다.
- 이제 반복, 타이밍 및 기타 프로세스와 같이 수많은 BPF(Berkeley Packet Filter) 백엔드 확장을 사용할 수 있습니다.
- SystemTap 스크립트를 관리하는 새 서비스를 사용할 수 있습니다. 이 서비스는 Prometheus 호환 모니터링 시스템에 지표를 보냅니다.
- SystemTap은 elfutils 라는 새 HTTP 파일 서버의 기능을 상속했습니다. debuginfod. 이 서버는 디버깅 리소스를 SystemTap에 자동으로 전송합니다.

(BZ#1744989)

IBM Z 시리즈 성능 카운터 개선 사항

IBM Z 시리즈 유형 0x8561, 0x8562 및 0x3907(z14 ZR1) 시스템은 이제 libpfm 에서 인식됩니다. IBM Z 시리즈에서 ECC(elliptic-curve cryptography) 작업을 모니터링하기 위한 성능 이벤트를 사용할 수 있습니다. 이를 통해 IBM Z 시리즈 시스템에서 추가 하위 시스템을 모니터링할 수 있습니다.

(BZ#1731019)

히스토리 툴셋을 버전 1.41로 업데이트

satellite Toolset이 1.41 버전으로 업데이트되었습니다. 주요 변경 사항은 다음과 같습니다.

- 이제 고아 규칙이 덜 엄격하기 때문에 새로운 특성을 쉽게 구현할 수 있습니다.
- 이제 #[non_exhaustive] 특성을 struct, enum 또는 enum 변형에 연결할 수 있습니다.
- FFI(상하 기능 인터페이스)에서 Box<T> 를 사용하면 이제 더 많은 보장이 제공됩니다. Box<T> 는 FFI에서 T* 포인터와 동일한 ABI(Application Binary Interface)를 가집니다.

- 컴파일 시 메모리 보안 버그를 감지해야 하지만 이전의 검사기에는 제한 사항이 있으며 정의되지 않은 동작과 메모리가 안전하지 않았습니다. 새로운 비연산 수명 검사기(NLL)는 메모리 안전하지 않은 문제를 하드 오류로 보고할 수 있습니다. 이 에디션은 현재 2015년과 2018년 에디션에 적용됩니다. 이전에는 2015년 NLL에서 이러한 문제에 대한 경고만 제기했습니다.

parent -toolset 모듈을 설치하려면 root로 다음 명령을 실행합니다.

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

사용 정보는 사용 정보 사용을 참조하십시오.

(BZ#1776847)

LLVM Toolset을 버전 9.0.1로 업데이트

LLVM Toolset이 버전 9.0.1로 업그레이드되었습니다. 이번 업데이트를 통해 이제 asm goto 문이 지원됩니다. 이러한 변경으로 AMD64 및 Intel 64 아키텍처에서 Linux 커널을 컴파일할 수 있습니다.

llvm-toolset 모듈을 설치하려면 root로 다음 명령을 실행합니다.

```
# yum module install llvm-toolset
```

자세한 내용은 LLVM Toolset 사용을 참조하십시오.

(BZ#1747139)

Go Toolset을 버전 1.13으로 다시 설정

Go Toolset이 1.13 버전으로 업그레이드되었습니다. 주요 개선 사항은 다음과 같습니다.

- 이제 RHEL 시스템이 FIPS 모드에서 부팅될 때 FIPS 인증 암호화 모듈을 사용할 수 있습니다. 사용자는 GOLANG_FIPS=1 환경 변수를 사용하여 이 모드를 수동으로 활성화할 수 있습니다.

- 이제 Delve 디버거 버전 1.3.2를 Go에 사용할 수 있습니다. Go(golang) 프로그래밍 언어의 소스 수준 디버거입니다.

go-toolset 모듈을 설치하려면 root로 다음 명령을 실행합니다.

```
# yum module install go-toolset
```

Delve 디버거를 설치하려면 root로 다음 명령을 실행합니다.

```
# yum install delve
```

Delve를 사용하여 helloworld.go 프로그램을 디버깅하려면 다음 명령을 실행합니다.

```
$ dlv debug helloworld.go
```

Go Toolset에 대한 자세한 내용은 Go Toolset 사용을 참조하십시오.

Delve에 대한 자세한 내용은 업스트림 Delve 문서를 참조하십시오.

(BZ#1747150)

OpenJDK에서 secp256k1도 지원

이전에는 OpenJDK(Open Java Development Kit)에서 NSS 라이브러리의 곡선만 사용할 수 있었습니다. 그 결과 OpenJDK는 ECC(원격 곡선 암호화)를 위한 secp256r1, secp384r1, secp521r1 곡선만 제공했습니다. 이번 업데이트를 통해 OpenJDK는 내부 ECC 구현을 사용하며 secp256k1 곡선도 지원합니다.

(BZ#1746875, BZ#1746879)

5.1.12. IdM (Identity Management)

IdM에서 새로운 Ansible 관리 모듈 지원

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

- **ipauser** 모듈은 사용자 추가 및 제거를 자동화합니다.
- **ipagroup** 모듈은 사용자 및 사용자 그룹으로부터 사용자 그룹 추가 및 제거를 자동화합니다.
- **ipahost** 모듈은 호스트 추가 및 제거를 자동화합니다.
- **ipahostgroup** 모듈은 호스트 그룹 내 및 호스트 그룹 추가 및 제거를 자동화합니다.
- **ipasudorule** 모듈은 **sudo** 명령 및 **sudo** 규칙의 관리를 자동화합니다.
- **ipapwpolicy** 모듈은 **IdM**에서 암호 정책 구성을 자동화합니다.
- **ipahbacrule** 모듈은 **IdM**에서 호스트 기반 액세스 제어의 관리를 자동화합니다.

두 개 이상의 **ipauser** 호출을 **users** 변수와 함께 사용하거나 사용자가 포함된 **JSON** 파일을 사용할 수 있습니다. 마찬가지로, 두 개 이상의 **ipahost** 호출을 **hosts** 변수와 함께 결합하거나 또는 호스트를 포함하는 **JSON** 파일을 사용할 수 있습니다. 또한 **ipahost** 모듈은 호스트에 대해 여러 개의 **IPv4** 및 **IPv6** 주소가 있는지 확인할 수 있습니다.

(JIRA:RHELPLAN-37713)

IdM 상태 점검 에서 임시 **DNS** 레코드 지원

이번 업데이트에서는 **IdM(Identity Management)** 서버의 **DNS** 레코드에 대한 독립 실행형 수동 테스트가 도입되었습니다.

테스트는 **Healthcheck** 도구를 사용하고 **etc/resolv.conf** 파일의 로컬 확인자를 사용하여 **DNS** 쿼리를 수행합니다. 이 테스트를 통해 자동 검색에 필요한 예상 **DNS** 레코드를 확인할 수 있습니다.

(JIRA:RHELPLAN-37777)

SSSD를 사용하여 **RHEL**을 **AD**에 직접 통합하면 **FIPS** 지원

이 향상된 기능을 통해 **SSSD(System Services Security Daemon)**는 이제 **ISV(Federal Information Processing Standard)**에서 승인한 암호화 유형을 사용하는 **AD(Active Directory)** 배포와 통합됩니다. 개선된 기능을 통해 **FIPS** 기준을 충족해야 하는 환경에서 **RHEL** 시스템을 **AD**에 직접 통합할 수 있습니다.

(BZ#1841170)

기본적으로 **Samba** 서버 및 클라이언트 유틸리티에서 **SMB1** 프로토콜이 비활성화되었습니다

Samba 4.11에서는 서버 최소 프로토콜 및 클라이언트 최소 프로토콜 매개 변수의 기본값이 **NT1** 에서 **SMB2_02** 로 변경되었습니다. 서버 메시지 블록 버전 **1(SMB1)** 프로토콜은 더 이상 사용되지 않습니다. **/etc/samba/smb.conf** 파일에 이러한 매개변수를 설정하지 않은 경우:

- **SMB1**만 지원하는 클라이언트는 더 이상 **Samba** 서버에 연결할 수 없습니다.
- **smbclient** 와 같은 **Samba** 클라이언트 유틸리티 및 **libsmbclient** 라이브러리는 **SMB1**만 지원하는 서버에 연결하지 못합니다.

Red Hat은 **SMB1** 프로토콜을 사용하지 않는 것이 좋습니다. 그러나 환경에 **SMB1**이 필요한 경우 프로토콜을 수동으로 다시 활성화할 수 있습니다.

Samba 서버에서 **SMB1**을 다시 활성화하려면 다음을 수행합니다.

- **/etc/samba/smb.conf** 파일에 다음 설정을 추가합니다.

```
server min protocol = NT1
```

- **smb** 서비스를 다시 시작하십시오.

```
# systemctl restart smb
```

Samba 클라이언트 유틸리티 및 **libsmbclient** 라이브러리를 위해 **SMB1**을 다시 활성화하려면 다음을 수행합니다.

- /etc/samba/smb.conf 파일에 다음 설정을 추가합니다.

```
client min protocol = NT1
```

- smb 서비스를 다시 시작하십시오.

```
# systemctl restart smb
```

SMB1 프로토콜은 향후 Samba 릴리스에서 제거될 예정입니다.

(BZ#1785248)

Samba 가 버전 **4.11.2**로 업데이트

samba 패키지가 업스트림 버전 **4.11.2**로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 기본적으로 서버 메시지 블록 버전 1(SMB1) 프로토콜은 이제 Samba 서버, 클라이언트 유틸리티 및 libsmbclient 라이브러리에서 비활성화됩니다. 그러나 server min protocol 및 client min protocol 매개변수를 수동으로 NT1로 설정하여 SMB1 을 다시 활성화할 수 있습니다. Red Hat은 SMB1 프로토콜을 다시 활성화하는 것을 권장하지 않습니다.

- lanman auth 및 encrypt password 매개 변수는 더 이상 사용되지 않습니다. 이러한 매개 변수는 안전하지 않은 인증을 활성화하며 더 이상 사용되지 않는 SMB1 프로토콜에서만 사용할 수 있습니다.

- o 매개 변수가 onode 클러스터형 일반 데이터베이스(CTDB) 유틸리티에서 제거되었습니다.

- 이제 Samba에서 암호화를 위해 GnuTLS 라이브러리를 사용합니다. 결과적으로 RHEL의 FIPS 모드가 활성화된 경우 Samba가 FIPS 표준을 준수합니다.

- ctdbd 서비스는 이제 CPU 스레드의 90% 이상을 사용할 때 로그를 기록합니다.

- 더 이상 사용되지 않는 Python 2 지원이 제거되었습니다.

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

주요 변경 사항에 대한 자세한 내용은 업데이트하기 전에 업스트림 릴리스 노트를 참조하십시오. https://www.samba.org/samba/history/samba-4.11.0.html

(BZ#1754409)

디렉토리 서버가 버전 **1.4.2.4**로 업데이트

389-ds-base 패키지가 업스트림 버전 **1.4.2.4**로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항의 전체 목록은 업데이트하기 전에 업스트림 릴리스 노트를 읽어 보십시오.

- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-4.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-3.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-2.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-1-4-2-1.html

(BZ#1748994)

일부 레거시 스크립트가 **Directory Server**에서 교체되었습니다

이 향상된 기능을 통해 **Directory Server**에서 지원되지 않는 **dbverify,validate-syntax.pl,cl-dump.pl,fixup-memberuid.pl** 및 **repl-monitor.pl** 레거시 스크립트를 대체할 수 있습니다. 이러한 스크립트는 다음 명령으로 교체되었습니다.

- **dbverify**: **dsctl** *instance_name* **dbverify**

- validate-syntax.pl: dsconf schema validate-syntax
- CL-dump.pl:dsconf 복제 dump-changelog
- fixup-memberuid.pl:dsconf plugin posix-winsync fixup
- REPL-monitor.pl:dsconf 복제 모니터

모든 레거시 스크립트 및 대체 스크립트 목록은 Red Hat Directory Server 11에서 명령행 유틸리티 교체를 참조하십시오.

(BZ#1739718)

숨겨진 복제본으로 IdM 설정이 완전히 지원됨

RHEL 8.2의 IdM(Identity Management)은 IdM 서버를 숨겨진 복제본으로 설정할 수 있도록 지원합니다. 숨겨진 복제본은 모든 서비스가 실행 중이고 사용 가능한 IdM 서버입니다. 그러나 DNS의 서비스에 대한 SRV 레코드가 없고 LDAP 서버 역할이 활성화되어 있지 않으므로 다른 클라이언트 또는 마스터에 알리지 않습니다. 따라서 클라이언트는 서비스 검색을 사용하여 숨겨진 복제본을 탐지할 수 없습니다.

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

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

자세한 내용은 IdM 숨겨진 복제본 설치를 참조하십시오.

(BZ#1719767)

Kerberos 티켓 정책이 인증 표시기 지원

인증 표시기는 티켓을 획득하는 데 사용된 사전 인증 메커니즘을 기반으로 Kerberos 티켓에 연결됩니다.

- 이중 인증을 위한 OTP (암호 + OTP)
- RADIUS 인증을 위한 준비
- PKINIT, 스마트 카드 또는 인증서 인증을 위한 Pkinit
- 강화된 암호를 위한 강화 (SPAKE 또는 FAST)

KDC(Kerberos Distribution Center)는 인증 표시기를 기반으로 하는 서비스 티켓 요청에 서비스 액세스 제어, 최대 티켓 수명, 최대 재생 기간과 같은 정책을 시행할 수 있습니다.

이 향상된 기능을 통해 관리자는 사용자 티켓에서 특정 인증 표시기가 필요하므로 서비스 티켓 발급에 대해 보다 세부적인 제어를 달성할 수 있습니다.

(BZ#1777564)

krb5 패키지가 FIPS와 호환됨

이 향상된 기능을 통해 비준수 암호화는 금지됩니다. 결과적으로 관리자는 FIPS로 연결된 환경에서 Kerberos를 사용할 수 있습니다.

(BZ#1754690)

Directory Server는 시스템 전체 암호화 정책에 따라 sslVersionMin 매개변수를 설정합니다.

기본적으로 Directory Server는 이제 시스템 전체 암호화 정책에 따라 sslVersionMin 매개변수 값을 설정합니다. /etc/crypto-policies/config 파일에서 crypto 정책 프로필을 다음과 같이 설정하는 경우:

- DEFAULT,FUTURE 또는 FIPS, Directory Server는 sslVersionMin 을 TLS1.2로 설정합니다.

- LEGACY, Directory Server는 sslVersionMin 을 TLS1.0으로 설정합니다.

또는 crypto 정책에 정의된 값보다 sslVersionMin 을 수동으로 더 높은 값으로 설정할 수 있습니다.

```
# dsconf -D "cn=Directory Manager" __ldap://server.example.com__ security set --tls-protocol-min
TLS1.3
```

(BZ#1828727)

SSSD에서 기본적으로 AD GPO 적용

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

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

(JIRA:RHELPLAN-51289)

5.1.13. 데스크탑

듀얼-GPU 시스템에서 Wayland 활성화

이전 버전에서는 GNOME 환경은 기본적으로 랩탑의 X11 세션과 두 개의 그래픽 처리 장치(GPU)가 있는 기타 시스템에서 기본 설정되어 있었습니다. 이번 릴리스에서는 GNOME이 듀얼-GPU 시스템의 Wayland 세션으로 기본 설정되어 단일 GPU 시스템과 동일한 동작입니다.

(BZ#1749960)

5.1.14. 그래픽 인프라

새로운 그래픽 카드 지원

이제 다음과 같은 그래픽 카드가 지원됩니다.

- Intel HD Graphics 610, 620, 630은 인텔트레이크 H 및 U 프로세서에서 찾을 수 있습니다.

- Intel Ice Lakeœ Graphics 910 및 Iris Plus Graphics 930, 940 및 950.

  Intel Ice Lake 그래픽을 지원하기 위해 alpha_support 커널 옵션을 설정할 필요가 없습니다.

- AMD Navi 10 제품군은 다음과 같은 모델을 포함합니다.

  - Radeon RX 5600
  - Radeon RX 5600 XT
  - Radeon RX 5700
  - Radeon RX 5700 XT
  - Radeon Pro W5700

- 다음 모델을 포함하는 Nvidia rpming TU116 제품군.

  노보 그래픽 드라이버는 아직 Nvidiaing TU116 제품군으로 3D 가속화를 지원하지 않습니다.

  - GSM GTX 1650 슈퍼
  - GSM GTX 1660
  - GSM GTX 1660 슈퍼

- Tix GTX 1660 Ti
- GTX 1660 Ti Max-Q

또한 다음 그래픽 드라이버가 업데이트되었습니다.

- Matrox mgag2000 드라이버
- Aspeed ast 드라이버
- Intel i915 드라이버

(JIRA:RHELPLAN-41384)

5.1.15. 웹 콘솔

이제 관리자는 클라이언트 인증서를 사용하여 RHEL 8 웹 콘솔에 인증할 수 있습니다

이 웹 콘솔의 향상된 기능을 통해 시스템 관리자는 클라이언트 인증서를 사용하여 인증서 인증이 내장된 브라우저를 사용하여 로컬로 또는 원격으로 RHEL 8 시스템에 액세스할 수 있습니다. 추가 클라이언트 소프트웨어는 필요하지 않습니다. 이러한 인증서는 일반적으로 스마트 카드 또는 유비키에서 제공되거나 브라우저로 가져올 수 있습니다.

인증서로 로그인할 때 사용자는 현재 웹 콘솔에서 관리 작업을 수행할 수 없습니다. 그러나 사용자는 암호를 사용하여 인증한 후 sudo 명령을 사용하여 터미널 페이지에서 수행할 수 있습니다.

(JIRA:RHELPLAN-2507)

TLS 클라이언트 인증서를 사용하여 웹 콘솔에 로그인하는 옵션

이번 업데이트를 통해 브라우저 또는 스마트 카드 또는 TitaniumbiKey와 같은 장치에서 제공하는 TLS 클라이언트 인증서로 로그인하도록 웹 콘솔을 구성할 수 있습니다.

(BZ#1678465)

웹 콘솔 로그인 관련 변경 사항

RHEL 웹 콘솔이 다음과 같은 변경 사항으로 업데이트되었습니다.

- 웹 콘솔은 15분 동안 활동이 없으면 현재 세션에서 자동으로 로그아웃합니다. /etc/cockpit/cockpit.conf 파일에서 시간 제한(분)을 구성할 수 있습니다.

- SSH와 마찬가지로 웹 콘솔은 이제 로그인 화면에서 배너 파일의 콘텐츠를 선택적으로 표시할 수 있습니다. 사용자는 /etc/cockpit/cockpit.conf 파일에서 기능을 구성해야 합니다.

자세한 내용은 cockpit.conf(5) 매뉴얼 페이지를 참조하십시오.

(BZ#1754163)

RHEL 웹 콘솔이 PatternFly 4 사용자 인터페이스 설계 시스템을 사용하도록 재설계되었습니다.

새 설계는 더 나은 접근성을 제공하며 OpenShift 4의 설계와 일치합니다. 업데이트는 다음과 같습니다.

- Overview(개요) 페이지가 완전히 다시 설계되었습니다. 예를 들어, 정보는 이해하기 쉬운 패널로 그룹화되고, 상태 정보가 더 중요하며, 리소스 그래프가 자체 페이지로 이동되었으며 하드웨어 정보 페이지를 찾기가 쉬워졌습니다.

- 사용자는 탐색 메뉴의 새로운 Search(검색) 필드를 사용하여 키워드를 기반으로 하는 특정 페이지를 쉽게 찾을 수 있습니다.

PatternFly에 대한 자세한 내용은 PatternFly 프로젝트 페이지를 참조하십시오.

(BZ#1784455)

가상 머신 페이지 업데이트

웹 콘솔의 **Virtual Machines** 페이지에 몇 가지 스토리지가 개선되었습니다.

- 이제 스토리지 볼륨 생성이 **libvirt** 지원 유형에 적용됩니다.
- 스토리지 풀은 **LVM** 또는 **iSCSI**에서 만들 수 있습니다.

또한 **Virtual Machines**(가상 시스템) 페이지에서는 가상 네트워크 인터페이스의 생성 및 제거를 지원합니다.

(BZ#1676506, BZ#1672753)

웹 콘솔 스토리지 페이지 업데이트

사용성 테스트에서는 **RHEL** 웹 콘솔 스토리지 페이지의 *기본 마운트 지점* 개념이 파악하기가 어렵고 이로 인해 혼란이 발생했습니다. 이번 업데이트를 통해 파일 시스템을 마운트할 때 웹 콘솔에서 더 이상 *기본* 선택 사항을 제공하지 않습니다. 이제 새 파일 시스템을 생성하려면 항상 지정된 마운트 지점이 필요합니다.

또한 웹 콘솔은 구성(**/etc/fstab**)과 런타임 상태(**/proc/mounts**) 간의 차이점을 숨깁니다. 웹 콘솔에서 변경한 내용은 항상 구성 및 런타임 상태에 모두 적용됩니다. 구성과 런타임 상태가 서로 다르면 웹 콘솔에 경고가 표시되고 사용자가 쉽게 다시 동기화할 수 있습니다.

(BZ#1784456)

5.1.16. 가상화

설치 트리에서 **RHEL** 가상 머신을 생성하려고 하면 이제 더 유용한 오류 메시지가 반환됩니다.

경우에 따라 **--location** 옵션과 함께 **virt-install** 유틸리티를 사용하여 생성된 **RHEL 7** 및 **RHEL 8** 가상 머신은 부팅되지 않습니다. 이번 업데이트에서는 이 문제를 해결하는 방법에 대한 지침을 제공하는 **virt-install** 오류 메시지가 추가되었습니다.

(BZ#1677019)

KVM 게스트에서 지원되는 **Intel Xeon** 플래티넘 **9200** 시리즈 프로세서

Intel Xeon 플래티넘 9200 시리즈 프로세서(이전의 Cascade Lake)에 대한 지원이 이제 KVM 하이퍼바이저 및 커널 코드와 libvirt API에 추가되었습니다. 이를 통해 KVM 가상 머신은 Intel Xeon 플래티넘 9200 시리즈 프로세서를 사용할 수 있습니다.

(JIRA:RHELPLAN-13995)

EDK2 가 stable201908 버전으로 업데이트

EDK2 패키지가 여러 개선사항을 제공하는 stable201908 버전으로 업그레이드되었습니다. 특히:

- *EDK2* 에는 이제 OpenSSL-1.1.1 지원이 포함되어 있습니다.
- 업스트림 프로젝트의 라이센스 요구 사항을 준수하기 위해 *EDK2* 패키지 라이센스가 BSD 및 OpenSSL 및 MIT에서 BSD -2-Clause-Patent 및 OpenSSL 및 MIT 로 변경되었습니다.

(BZ#1748180)

중첩된 가상 머신 생성

이번 업데이트를 통해 RHEL 8을 사용하는 Intel 64 호스트에서 실행되는 KVM(VM)에 중첩된 가상화가 완전히 지원됩니다. 이 기능을 사용하면 물리적 RHEL 8 호스트에서 실행되는 RHEL 7 또는 RHEL 8 VM이 하이퍼바이저 역할을 하며 고유한 VM을 호스팅할 수 있습니다.

AMD64 시스템에서 중첩된 KVM 가상화는 기술 프리뷰로 남아 있습니다.

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

5.1.17. 컨테이너

/etc/containers/registries.conf의 기본 레지스트리 검색 목록이 업데이트되었습니다.

/etc/containers/registries .conf의 기본 registries. search 목록은 Red Hat 및 해당 파트너가 큐레이션, 패치 및 유지 관리하는 컨테이너 이미지를 제공하는 신뢰할 수 있는 레지스트리만 포함하도록 업데이트되었습니다.

다음과 같은 정규화된 이미지 이름을 사용하는 것이 좋습니다.

- 레지스트리 서버(전체 DNS 이름)
- 네임스페이스
- 이미지 이름
- 태그(예: registry.redhat.io/ubi8/ubu:latest)

짧은 이름을 사용하는 경우 항상 스푸핑할 위험이 있습니다. 예를 들어, 사용자가 레지스트리에서 foobar 라는 이미지를 가져와서 myregistry.com 에서 온 것으로 예상합니다. myregistry.com 이 검색 목록에 먼저 없는 경우 공격자는 검색 목록 앞의 레지스트리에 다른 foobar 이미지를 배치할 수 있습니다. 사용자가 의도한 콘텐츠가 아니라 공격자 이미지 및 코드를 실수로 가져와서 실행했습니다. Red Hat은 알 수 없거나 익명 사용자가 임의 이름으로 계정을 생성할 수 없는 레지스트리인 신뢰할 수 있는 레지스트리만 추가하는 것이 좋습니다. 이렇게 하면 이미지가 스푸핑되거나, 스푸핑되거나, 비보안되지 않게 되는 것을 방지할 수 있습니다.

(BZ#1810053)

Podman은 더 이상 oci-systemd-hook에 의존하지 않습니다.

Podman은 container - tools:rhel8 및 container-tools:2.0 모듈 스트림에서 제거된 oci- systemd-hook 패키지를 필요로 하거나 의존하지 않습니다.

(BZ#1645280)

5.2. 외부 커널 매개변수로 중요한 변경

이 장에서는 시스템 관리자에게 Red Hat Enterprise Linux 8.2와 함께 배포된 커널의 중요한 변경 사항을 요약합니다. 이러한 변경 사항에는 proc 항목, sysctl 및 sysfs 기본값, 부팅 매개 변수, 커널 구성 옵션 또는 눈에 보이는 동작 변경이 포함됩니다.

5.2.1. 새 커널 매개변수

CPUidle.governor = [CPU_IDLE]

사용할 cpuidle governor의 이름입니다.

deferred_probe_timeout = [KNL]

지연된 프로브가 프로브에 대한 종속성 대기를 중지할 때까지 시간 초과(초)를 설정하는 디버깅 매개 변수입니다.

옵트된 특정 종속성(하위 시스템 또는 드라이버)만 무시됩니다. 시간 제한 **0**은 **initcall** 끝에 시간 초과됩니다. 이 매개변수는 재시도 후에도 지연된 프로브 목록에 장치를 덤프합니다.

kvm.nx_huge_pages = [KVM]

이 매개 변수는 **X86_BUG_ITLB_MULTIHIT** 버그에 대한 소프트웨어 해결 방법을 제어합니다.

옵션은 다음과 같습니다.

- **force -** 항상 해결방법을 배포합니다.
- **off -** 해결방법을 배치하지 마십시오.
- **auto** (기본값) **- X86_BUG_ITLB_MULTIHIT** 를 기반으로 해결방법을 배포합니다.

호스트에 소프트웨어 해결방법이 활성화된 경우 중첩 게스트에 대해 게스트를 활성화할 필요가 없습니다.

kvm.nx_huge_pages_recovery_ratio = [KVM]

이 매개변수는 주기적으로 대규모 페이지로 다시 설정되는 **4KiB** 페이지 수를 제어합니다. **0**은 복구를 비활성화합니다. 값이 **N**인 경우 **KVM**(커널 기반 가상 시스템)은 **1**분마다 **4KiB** 페이지의 **1/N**을 정지합니다. 기본값은 **60**입니다.

page_alloc.shuffle = [KNL]

페이지 할당자가 사용 가능한 목록을 임의로 조정해야 하는지 여부를 제어하는 부울 플래그입니다.

커널이 직접 매핑 메모리 측 캐시가 있는 플랫폼에서 실행되고 있음을 감지하면 임의화를 자동으로 활성화할 수 있습니다. 이 매개 변수는 해당 동작을 재정의/비활성화하는 데 사용할 수 있습니다.

플래그 상태는 **/sys/module/page_alloc/parameters/shuffle** 파일에서 **sysfs** 의사 파일 시스템

에서 읽을 수 있습니다.

panic_print =

패닉이 발생할 때 시스템 정보를 인쇄하기 위한 비트마스크.

사용자는 다음 비트의 조합을 선택할 수 있습니다.

- 비트 0: 모든 작업 정보 출력
- 비트 1: 인쇄 시스템 메모리 정보
- 비트 2: 타이머 정보 인쇄
- 비트 3: CONFIG_LOCKDEP 커널 구성이 있는 경우 정보 잠금
- 비트 4: ftrace 버퍼 인쇄
- 비트 5: 버퍼에서 모든 printk 메시지 인쇄

rcutree.sysrq_rcu = [KNL]

sysrq 키를 명령을 실행하여 새 유예 기간이 아직 시작되지 않은 이유를 확인하기 위해 주의해서 Tree RCU의 rcu_node 트리를 덤프합니다.

rcutorture.fwd_progress = [KNL]

이 개념을 지원하는 RCU 유형에 대해 RCU(Read-copy update) grace-period forward-progress 테스팅을 활성화합니다.

rcutorture.fwd_progress_div = [KNL]

CPU-stall-warning 기간의 일부를 지정하여 엄격한 전방향 진행 테스트를 수행합니다.

rcutorture.fwd_progress_holdoff = [KNL]

연속적인 전방향 진행 테스트 사이에 대기하는 시간(초)입니다.

rcutorture.fwd_progress_need_resched = [KNL]

Close-loop forward-progress 테스팅 중에 need_resched() 를 검사 내에서 cond_resched() 호출 을 포함합니다.

tsx = [X86]

이 매개변수는 TSX 제어를 지원하는 Intel 프로세서의 TSX(Transactional Synchronization Extensions) 기능을 제어합니다.

옵션은 다음과 같습니다.

- 의 - 시스템에서 TSX를 활성화합니다. 알려진 모든 보안 취약점에 대한 완화 조치가 있지만 TSX는 이전의 몇 가지 추측 관련 CVE를 가속화했습니다. 따라서 활성화된 상태로 두는 것과 관련된 알 수 없는 보안 위험이 있을 수 있습니다.
- off - 시스템에서 TSX를 비활성화합니다. 이 옵션은 MDS(Microarchitectural Data Sampling)에 취약하지 않은 최신 CPU에만 적용됩니다. 즉, MSR_IA32_ARCH_CAPABILITIES.MDS_NO=1 이 있고 마이크로 코드 업데이트를 통해 새 IA32_TSX_CTRL 모델별 레지스터(MSR)를 가져옵니다. 이 새로운 MSR을 사용하면 TSX 기능을 안정적으로 비활성화할 수 있습니다.
- auto - X86_BUG_TAA 가 있는 경우 TSX를 비활성화합니다. 그렇지 않으면 시스템에서 TSX를 활성화합니다.

이 매개변수를 지정하지 않는 것은 tsx=off 와 동일합니다.

자세한 내용은 업스트림 커널 설명서를 참조하십시오.

tsx_async_abort = [X86,INTEL]

이 매개변수는 TSX Async Abort (TAA) 취약점에 대한 완화 기능을 제어합니다.

MDS(Micro-architectural Data Sampling)와 유사하게 TSX(Transactional Synchronization Extensions)를 지원하는 특정 CPU는 CPU 내부 버퍼에 대한 공격에 취약합니다. 이 취약점은 특정 조건에서 공개된 가젯에 정보를 전달할 수 있습니다.

취약한 프로세서에서 예측 가능한 전달된 데이터를 캐시 사이드 채널 공격에 사용하여 공격자가 직접 액세스할 수 없는 데이터에 액세스할 수 있습니다.

옵션은 다음과 같습니다.

- **full - TSX**가 활성화된 경우 취약한 **CPU**에서 **TAA** 완화를 활성화합니다.

- **full,nosmt - TAA** 완화를 활성화하고 취약한 **CPU**에서 **SMT(Simultaneous Multi Threading)**를 비활성화합니다. **TSX**가 비활성화되면 **CPU**가 크로스 스레드 **TAA** 공격에 취약하지 않기 때문에 **SMT**가 비활성화되지 않습니다.

- **off - TAA** 완화를 무조건 비활성화합니다.

MDS 영향을 받는 시스템에서 두 취약점이 동일한 메커니즘으로 완화되므로 활성 **MDS** 완화를 통해 **tsx_async_abort=off** 매개 변수를 방지할 수 있습니다. 따라서 이 완화를 비활성화하려면 **mds=off** 매개 변수도 지정해야 합니다.

이 옵션을 지정하지 않으면 **tsx_async_abort=full** 과 동일합니다. 영향을 받는 **MDS** 완화 및 **MDS** 완화를 배포하는 **CPU**에서는 **TAA** 완화가 필요하지 않으며 추가 완화 기능을 제공하지 않습니다.

자세한 내용은 업스트림 커널 설명서를 참조하십시오.

5.2.2. 업데이트된 커널 매개변수

intel_iommu = [DMAR]

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

옵션은 다음과 같습니다.

- **sm_on [Default Off] -** 하드웨어에서 확장 가능한 모드 변환을 지원한다고 알려도 기본적으로 확장 가능한 모드 모드가 비활성화됩니다. 이 옵션을 설정하면 지원하려는 하드웨어에서 확장 가능 모드가 사용됩니다.

isolcpus = [KNL,SMP,ISOL]

이 매개변수는 지정된 CPU 세트를 방해하지 않도록 격리합니다.

- managed_irq - 분리된 CPU를 포함하는 인터럽트 마스크가 있는 관리 인터럽트에서 격리된 CPU를 대상으로 하지 못하게 하는 하위 매개 변수입니다. 관리되는 인터럽트의 선호도는 커널에서 처리하며 /proc/irq/* 인터페이스를 통해 변경할 수 없습니다.

  이러한 격리는 최상의 노력이며, 장치 큐의 자동으로 할당된 인터럽트 마스크에 분리 및 하우스키핑 CPU가 포함된 경우에만 효과적입니다. 하우스키핑 CPU가 온라인 상태인 경우 이러한 인터럽트가 하우스키핑 CPU로 전달되어 하우스키핑 CPU에 제출된 I/O가 분리된 CPU를 방해할 수 없습니다.

  큐의 선호도 마스크에 격리된 CPU만 포함된 경우 이 매개변수는 인터럽트 라우팅 결정에 영향을 미치지 않습니다. 그러나 인터럽트는 격리된 CPU에서 실행되는 작업이 I/O를 제출할 때만 전달됩니다. 하우스키핑 CPU에서 제출된 I/O는 해당 큐에 영향을 미치지 않습니다.

mds = [X86,INTEL]

옵션 변경 사항:

- 꺼짐 - TSX Async Abort (TAA) 영향을 받는 시스템에서 mds=off 는 두 취약점이 동일한 메커니즘으로 완화되므로 활성 TAA 완화로 방지할 수 있습니다. 따라서 이 완화 기능을 비활성화하려면 tsx_async_abort=off 커널 매개변수도 지정해야 합니다.

이 매개 변수를 지정하지 않는 것은 mds=full 과 동일합니다.

자세한 내용은 업스트림 커널 설명서를 참조하십시오.

mem_encrypt = [X86-64]

AMD SME(Secure Memory Encryption) 제어

...

메모리 암호화를 활성화할 수 있는 시기에 대한 자세한 내용은 업스트림 커널 설명서 를 참조하십시오.

완화 방법 =

옵션 변경 사항:

- **off -** 모든 선택적 **CPU** 완화를 비활성화합니다. 이로 인해 시스템 성능이 향상되지만 여러 **CPU** 취약점에 사용자가 노출될 수도 있습니다.

  다음과 같습니다.

  - **nopti [X86,PPC]**
  - **kpti=0 [ARM64]**
  - **nospectre_v1 [X86,PPC]**
  - **nobp=0 [S390]**
  - **nospectre_v2 [X86,PPC,S390,ARM64]**
  - **spectre_v2_user=off [X86]**
  - **spec_store_bypass_disable=off [X86,PPC]**
  - **ssbd=force-off [ARM64]**
  - **l1tf=off [X86]**
  - **mds=off [X86]**
  - **tsx_async_abort=off [X86]**

- kvm.nx_huge_pages=off [X86]

  예외:

  kvm.nx_huge_pages=force인 경우 kvm.nx_huge_pages =force 에는 아무 영향도 미치지 않습니다.

- auto,nosmt - 모든 CPU 취약점을 완화하여 필요한 경우 SMT(동시 멀티 스레드)를 비활성화합니다. 이 옵션은 SMT를 손실하는 것을 의미하더라도 항상 완전히 완화하려는 사용자를 위한 것입니다.

  다음과 같습니다.

  - l1tf=flush,nosmt [X86]
  - mds=full,nosmt [X86]
  - tsx_async_abort=full,nosmt [X86]

rcutree.jiffies_till_sched_qs = [KNL]

이 매개 변수는 RCU(읽기 복사 업데이트)가 rcu_note_context_switch() 및 cond_resched() 함수에서 quigrad-state 도움말을 요청하기 전에 지정된 유예 기간에 필요한 기간을 설정합니다. 지정되지 않은 경우 커널은 rcutree.jiffies_current_ first_fqs 및 rcutree.jiffies_ still_next_fqs 커널 매개 변수의 최신 설정을 기반으로 값을 계산합니다.

계산된 이 값은 rcutree.jiffies_to_sched_qs 커널 매개 변수에서 볼 수 있습니다. rcutree.jiffies_to_sched_qs를 설정하려는 모든 시도가 덮어쓰기됩니다.

tsc =

이 매개 변수는 TSC(Time Stamp Counter)에 대한 클록 소스 안정성 검사를 비활성화합니다.

형식: <string>

옵션은 다음과 같습니다.

- **reliable [x86] - TSC** 클록소스를 신뢰할 수 있는 것으로 표시합니다. 이 옵션은 런타임 시 클록 소스 확인 및 부팅 시 수행되는 안정성 검사를 비활성화합니다. 또한 이 옵션을 사용하면 이전 하드웨어와 가상화 환경에서 고해상도 타이머 모드를 사용할 수 있습니다.

- **noirqtime [x86] - TSC**를 사용하여**IRQ(Interrupt Request)** 회계를 수행하지 마십시오. **RDTSC (Read Time-Stamp Counter)**가 느리고 이 회계는 오버헤드를 추가할 수 있는 모든 플랫폼에서 **IRQ_TIME_ACCOUNTING** 을 비활성화하는 데 사용됩니다.

- **unstable [x86] - TSC** 클럭소스를 불안정한 것으로 표시합니다. 이 옵션은 부팅 시 무조건 불안정한 **TSC**를 표시하며, **TSC** 감시 알림이 있으면 추가 차단을 방지합니다.

- **nowatchdog [x86] - clocksource watchdog**를 비활성화합니다. 옵션은 클럭소스 워치독에서 중단이 허용되지 않는 엄격한 대기 시간 요구 사항이 있는 경우에 사용됩니다.

5.2.3. 새로운 /proc/sys/kernel 매개변수

panic_print

패닉이 발생할 때 시스템 정보를 인쇄하기 위한 비트마스크.

사용자는 다음 비트의 조합을 선택할 수 있습니다.

- 비트 **0:** 모든 작업 정보 출력

- 비트 **1:** 인쇄 시스템 메모리 정보

- 비트 **2:** 타이머 정보 인쇄

- 비트 **3: CONFIG_LOCKDEP** 커널 구성 항목이 있는 경우 정보 잠금

- 비트 **4: ftrace** 버퍼 인쇄

예를 들어 패닉에서 작업 및 메모리 정보를 인쇄하려면 다음을 실행합니다.

```
# echo 3 > /proc/sys/kernel/panic_print
```

sched_energy_aware

이 매개변수는 에너지 인식 스케줄링(EAS)을 활성화하거나 비활성화합니다.

EAS는 에너지 모델을 사용할 수 있는 비대칭 CPU 토폴로지가 있는 플랫폼에서 자동으로 시작됩니다.

플랫폼에서 EAS의 요구 사항을 충족하지만 사용하지 않으려면 이 값을 0으로 변경합니다.

5.2.4. 업데이트된 /proc/sys/kernel 매개변수

threads-max

이 매개변수는 fork() 함수에서 생성할 수 있는 최대 스레드 수를 제어합니다.

초기화 중에 커널은 최대 스레드 수를 생성하는 경우에도 이 값을 사용 가능한 RAM 페이지의 일부(1/8번째)만 차지합니다.

thread -max 에 쓸 수 있는 최소 값은 1입니다. 최대 값은 상수 FUTEX_TID_MASK (0x3fffff) 에서 제공합니다.

이 범위를 벗어난 값이thread -max에 작성되면 EINVAL 오류가 발생합니다.

5.2.5. 업데이트된 /proc/sys/net 매개변수

bpf_jit_enable

이 매개 변수는 BPF JIT(Berkeley Packet Filter Just-in-Time) 컴파일러를 활성화합니다.

BPF 는 다양한 후크 지점에서 바이트코드를 실행할 수 있는 유연하고 효율적인 인프라입니다. 네트워킹(예: XDP,tc), 추적(예: kprobes,uprobes ,tracepoints) 및 보안(예: seccomp)과 같은 여러 Linux 커널 하위 시스템에서 사용됩니다.

LLVM 에는 제한된 C를 BPF 명령 시퀀스로 컴파일할 수 있는 BPF 백엔드가 있습니다. 프로그램 로드를 bpf() 시스템 호출을 통해 커널의 검증기를 전달한 후 JIT 는 이러한 BPF 프로파일을 기본 CPU 지침으로 변환합니다.

JIT 에는 두 가지 플레이버가 있으며 최신 eBPF JIT 는 현재 다음 CPU 아키텍처에서 지원됩니다.

- x86_64
- arm64
- ppc64 (작은 큰 endian 모두)
- s390x

5.3. 장치 드라이버

이 장에서는 새 장치 드라이버 또는 Red Hat Enterprise Linux 8.2에서 업데이트한 모든 장치 드라이버에 대한 포괄적인 목록을 제공합니다.

5.3.1. 새 드라이버

네트워크 드라이버

- gVNIC 드라이버 (gve.ko.xz)
- Broadcom UniMAC MDIO 버스 컨트롤러 (mdio-bcm-unimac.ko.xz)
- 소프트웨어 iWARP 드라이버 (siw.ko.xz)

그래픽 드라이버 및 기타 드라이버

- vRAM 메모리 관리 도우미 (drm_vram_helper.ko.xz)

- **haltpoll governor의 CPUidle 드라이버 (cpuidle-haltpoll.ko.xz)**
- **stm_ftrace 드라이버(stm_ftrace.ko.xz)**
- **stm_console 드라이버 (stm_console.ko.xz)**
- **시스템 추적 모듈 장치 클래스 (stm_core.ko.xz)**
- **dummy_stm device (dummy_stm.ko.xz)**
- **stm_ humanbeat 드라이버 (stm_ humanbeat.ko.xz)**
- **Intel® Trace Hub Global Trace Hub 드라이버 (intel_th_gth.ko.xz)**
- **Intel® Trace Hub PTI/LPP 출력 드라이버(intel_th_pti.ko.xz)**
- **Intel® Trace Hub 컨트롤러 드라이버(intel_th.ko.xz)**
- **Intel® Trace Hub Memory Storage Unit 드라이버 (intel_th_msu.ko.xz)**
- **Intel® Trace Hub Software Trace Hub 드라이버(intel_th_sth.ko.xz)**
- **Intel® Trace Hub Memory Storage Unit Software sink (intel_th_msu_sink.ko.xz)**
- **Intel® Trace Hub PCI 컨트롤러 드라이버 (intel_th_pci.ko.xz)**
- **Intel® Trace Hub ACPI 컨트롤러 드라이버 (intel_th_acpi.ko.xz)**

- Intel 10nm 서버 프로세서 용 MC 드라이버 (i10nm_edac.ko.xz)
- 장치 DAX: 직접 액세스 매핑 장치 (dax_pmem_core.ko.xz)
- PMEM DAX: 영구 메모리에 직접 액세스 (dax_pmem.ko.xz)
- PMEM DAX: 사용되지 않는 /sys/class/dax 인터페이스 지원 (dax_pmem_compat.ko.xz)
- Intel PMC Core platform init (intel_pmc_core_pltdrv.ko.xz)
- MSR 인터페이스 (intel_rapl_msr.ko.xz)를 통한 Intel RAPL (Executning Average Power Limit) 제어
- Intel Runtime Average Power Limit (RAPL) 공통 코드 (intel_rapl_common.ko.xz)

스토리지 드라이버

- MD(md-cluster.ko.xz) 클러스터링 지원

5.3.2. 업데이트된 드라이버

네트워크 드라이버 업데이트

- VMware vmxnet3 가상 NIC 드라이버(vmxnet3.ko.xz)가 버전 1.4.17.0-k로 업데이트되었습니다.
- Intel® 10 기가비트 가상 기능 네트워크 드라이버(ixgbevf.ko.xz)가 버전 4.1.0-k-rh8.2.0으로 업데이트되었습니다.
- Intel® 10 기가비트 PCI Express 네트워크 드라이버(ixgbe.ko.xz)가 버전 5.1.0-k-rh8.2.0으로 업데이트되었습니다.
- Intel® Ethernet Connection E800 Series Linux Driver(ice.ko.xz)가 버전 5.5.1-k로 업데이트되었습니다.

- **NFS(Netronome Flow Processor)** 드라이버(**nfp.ko.xz**)가 **4.18.0-185.el8.x86_64**로 업데이트되었습니다.

- **EA(Elastic Network Adapter)(ena.ko.xz)**가 버전 **2.1.0K**로 업데이트되었습니다.

그래픽 및 기타 드라이버 업데이트

- **HPE** 워치독 드라이버(**hpwdt.ko.xz**)가 버전 **2.0.3**으로 업데이트되었습니다.

- **Intel I/OAT DMA Linux** 드라이버(**ioatdma.ko.xz**)가 버전으로 업데이트되었습니다.

스토리지 드라이버 업데이트

- **HPE Smart Array Controller(hpsa.ko.xz)**용 드라이버가 버전 **3.4.20-170-RH4**로 업데이트되었습니다.

- **LSI MPT Fusion SAS 3.0** 장치 드라이버(**mpt3sas.ko.xz**)가 버전 **32.100.00.00**으로 업데이트되었습니다.

- **Qlogic FCoE Driver(bnx2fc.ko.xz)**가 버전 **2.12.10**으로 업데이트되었습니다.

- **Emulex LightPulse Fibre Channel SCSI** 드라이버(**lpfc.ko.xz**)가 버전 **0:12.6.0.2**로 업데이트되었습니다.

- **Qlogic FastLinQ 4xxxx FCoE** 모듈(**qedf.ko.xz**)이 버전 **8.42.3.0**으로 업데이트되었습니다.

- **Qlogic** 파이버 채널 **HBA** 드라이버(**qla2xxx.ko.xz**)가 버전 **10.01.00.21.08.2-k**로 업데이트되었습니다.

- **Microsemi Smart Family Controller** 버전(**smartpqi.ko.xz**)용 드라이버가 버전 **1.2.10-025**로 업데이트되었습니다.

- Qlogic FastLinQ 4xxxx iSCSI 모듈(qedi.ko.xz)이 8.37.0.20 버전으로 업데이트되었습니다.

- BroadcomRAID SAS Driver(megaraid_sas.ko.xz)가 07.710.50.00-rc1 버전으로 업데이트되었습니다.

5.4. 버그 수정

이 부분에서는 사용자에게 중요한 영향을 미치는 Red Hat Enterprise Linux 8.2에서 수정된 버그에 대해 설명합니다.

5.4.1. 설치 프로그램 및 이미지 생성

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

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

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

(BZ#1637472)

설치 프로그램에서 s390x의 보안 부팅 지원

이전에는 RHEL 8.1에서 보안 부팅을 사용한 IBM Z 환경에서 사용하기 위한 부팅 디스크 준비 지원이 제공되었습니다. 설치 중에 사용되는 서버 및 하이퍼바이저의 기능은 디스크상의 디스크 형식에 보안 부팅 지원이 포함되어 있는지 여부를 결정합니다. 설치하는 동안 디스크 형식에 영향을 미칠 수 있는 방법이 없었습니다. 결과적으로 보안 부팅을 지원하는 환경에 RHEL 8.1을 설치한 경우 일부 페일오버 시나리오에서처럼 보안 부팅 지원이 부족한 환경으로 이동할 때 시스템을 부팅할 수 없었습니다.

이번 업데이트를 통해 이제 zipl 툴의 보안 부팅 옵션을 설정할 수 있습니다. 이를 위해 다음 중 하나를 사용할 수 있습니다.

- Kickstart zipl 명령과 옵션 중 하나는 --secure-boot,--no-secure -boot, --force-secure-boot 입니다.

- GUI의 설치 요약 창에서 시스템 > 설치 대상 > 전체 디스크 요약 및 부트 로더 링크를 선택하

고 부팅 장치를 설정할 수 있습니다. 결과적으로 이제 안전한 부팅 지원이 없는 환경에서 설치를 부팅할 수 있습니다.

(BZ#1659400)

보안 부팅 기능을 사용할 수 있습니다.

이전에는 **secure=** 부팅 옵션의 기본값이 **auto** 로 설정되지 않아 보안 부팅 기능을 사용할 수 없었습니다. 이번 업데이트를 통해 이전에 구성하지 않은 경우 기본값이 **auto** 로 설정되고 보안 부팅 기능을 사용할 수 있습니다.

(BZ#1750326)

/etc/sysconfig/kernel 파일은 더 이상 **new- kernel-pkg** 스크립트를 참조하지 않습니다.

이전에는 **/etc/sysconfig/kernel** 파일에서 **new-kernel-pkg** 스크립트를 참조했습니다. 그러나 **new-kernel-pkg** 스크립트는 **RHEL 8** 시스템에 포함되지 않습니다. 이번 업데이트를 통해 **new-kernel-pkg** 스크립트에 대한 참조가 **/etc/sysconfig/kernel** 파일에서 제거되었습니다.

(BZ#1747382)

설치에서 부트 장치 **NVRAM** 변수에서 허용되는 최대 장치 수를 설정하지 않습니다.

이전에는 **RHEL 8** 설치 프로그램에서 부트 장치 **NVRAM** 변수에서 허용되는 최대 장치 수를 설정했습니다. 이로 인해 최대 장치 수를 초과하는 시스템에서 설치에 실패했습니다. 이번 업데이트를 통해 **RHEL 8** 설치 프로그램은 이제 최대 장치 설정을 확인하고 허용되는 장치 수만 추가합니다.

(BZ#1748756)

설치는 네트워크 이외의 위치에 있는 **Kickstart** 파일에서 **URL** 명령을 사용하는 이미지 위치에 대해 작동합니다.

이전에는 비네트워크 위치에 있는 **Kickstart** 파일에서 **URL** 명령으로 이미지 원격 위치에 의해 트리거된 네트워크 활성화를 프로세스 초기에 설치하지 못했습니다. 이번 업데이트에서는 네트워크 이외의 위치에 있는 **Kickstart** 파일에서 **URL** 명령을 사용하여 이미지 위치를 제공하는 문제 및 설치(예: **CD-ROM** 또는 로컬 블록 장치)가 예상대로 작동합니다.

(BZ#1649359)

RHEL 8 설치 프로그램은 포맷되지 않은 장치에 대해서만 ECKD DASD를 확인합니다.

이전에는 포맷되지 않은 장치를 확인할 때 설치 프로그램이 모든 **DASD** 장치를 확인했습니다. 그러나 설치 프로그램은 **ECKD DASD** 장치만 확인해야 합니다. 그 결과 **SWAPGEN**이 있는 **FBA DASD** 장치를 사용할 때 설치에 실패했습니다. 이번 업데이트를 통해 설치 프로그램이 **FBA DASD** 장치를 확인하지 않고 설치가 성공적으로 완료되었습니다.

(BZ#1715303)

5.4.2. 소프트웨어 관리

yum repolist 가 첫 번째 사용 가능한 저장소에서 종료되지 않음

이전에는 리포지토리 구성 옵션 **skip_if_unavailable** 이 기본적으로 다음과 같이 설정되었습니다.

```
skip_if_unavailable=false
```

이 설정을 사용하면 **yum repolist** 명령이 첫 번째로 사용할 수 없는 리포지토리에서 오류, 종료 상태 **1** 에서 종료되었습니다. 결과적으로 **yum repolist** 는 사용 가능한 리포지토리를 계속 나열하지 않았습니다.

이번 업데이트를 통해 **yum repolist** 가 더 이상 다운로드가 필요하지 않도록 수정되었습니다. 결과적으로 **yum repolist** 는 메타데이터가 필요한 출력을 제공하지 않으므로 이제 명령이 예상대로 사용 가능한 리포지토리를 계속 나열합니다.

사용 가능한 패키지 수는 **yum repolist --verbose** 또는 **yum repo info** 에서만 반환되며 여전히 사용 가능한 메타데이터가 필요합니다. 따라서 이러한 명령은 처음 사용할 수 없는 리포지토리로 끝납니다.

(BZ#1697472)

5.4.3. 쉘 및 명령행 툴

자동 업데이트

RHEL 8.2에는ReaR(Relax-and- recovery) 유틸리티에 대한 여러 업데이트가 도입되었습니다.

빌드 디렉터리 처리가 변경되었습니다. 이전에는 **ReaR** 이 실패할 경우 빌드 디렉터리가 임시 위치에 유지되었습니다. 이번 업데이트를 통해 디스크 공간을 사용하지 않도록 기본적으로 비대화형 실행에서 빌드 디렉터리가 삭제됩니다.

KEEP_BUILD_DIR 구성 변수의 의미 체계가 새 오류 값을 포함하도록 향상되었습니다. **KEEP_BUILD_DIR** 변수를 다음 값으로 설정할 수 있습니다.

- 디버깅 을 위한 오류 (이전 동작)
- 빌드 디렉토리를 항상 유지하기 위한 **Y (true)**
- 빌드 디렉토리를 보존하지 않는 **N (false)**

기본값은 **ReaR**이 대화형(터미널에서) 및 **ReaR** 이 비대화형으로 실행되는 경우 **false**인 오류가 있는 빈 문자열입니다. 디버그 모드(**-d**) 및 디버그 스크립트 모드(**-D**)에서는 **KEEP_BUILD_DIR** 이 자동으로 **true** 로 설정됩니다. 이 동작은 변경되지 않았습니다.

주요 버그 수정은 다음과 같습니다.

- **NetBackup 8.0** 지원이 수정되었습니다.
- 재정렬 은 **xrealloc**와 유사한 **bash** 오류로 더 이상 중단되지 않습니다. 그룹당 다수의 사용자, 그룹 및 사용자가 있는 시스템에 할당할 수 없습니다.
- 이제 **bconsole** 명령으로 **Bacula** 통합을 사용할 때 복원 작업을 수행할 수 있는 프롬프트가 표시됩니다.
- 이제 **docker** 서비스가 실행 중이지만 **Docker** 루트 디렉터리가 정의되어 있지 않거나 **Docker** 서비스의 상태를 확인할 수 없는 경우에도 파일을 올바르게 백업합니다 .
- 씬 풀을 사용하거나 마이그레이션 모드에서 시스템을 복구할 때 더 이상 복구에 실패하지 않습니다.
- **LVM**을 사용하여 복구 프로세스 중에 **initramfs** 를 매우 느리게 다시 빌드하는 속도가 매우 느립니다.
-

이제 UEFI 부트로더를 사용할 때 AMD 및 Intel 64비트 아키텍처에서 작동하는 부팅 가능한 ISO 이미지를 생성합니다. 이 설정에서 복구 이미지를 부팅해도 오류 메시지 알 수 없는 명령 'configfile' (...)을 사용하여 Grub에서 더 이상 중단되지 않습니다.) 복구 모드로 들어가기.... 이전에 XFS 파일 시스템 지원이 누락되어 실패한 GRUB_RESCUE도 수정되었습니다.

(BZ#1729501)

mlocate 패키지 설치 중에 mlocate-updatedb.timer 이 활성화되었습니다

이전에는 mlocate 패키지 설치 후 mlocate-updatedb.timer 타이머가 비활성화되었으므로 파일 데이터베이스의 재지정이 자동으로 수행되지 않았습니다. 이번 업데이트를 통해 mlocate-updatedb.timer 타이머는 이제 90-default.preset 파일의 일부이며 mlocate 패키지 설치 후 기본적으로 활성화됩니다. 결과적으로 파일 데이터베이스가 자동으로 업데이트됩니다.

(BZ#1817591)

5.4.4. 인프라 서비스

dnsmasq 에서 되풀이되지 않는 DNS 쿼리를 올바르게 처리

이전에는 dnsmasq 가 비재귀적 모든 쿼리를 업스트림 서버에 전달하여 다른 응답을 생성했습니다. 이번 업데이트를 통해 /etc/hosts 파일에서 읽은 DHCP 호스트 리스 이름 또는 호스트와 같은 로컬 알려진 이름에 대한 비재귀적 쿼리는 dnsmasq 에 의해 처리되며 업스트림 서버로 전달되지 않습니다. 결과적으로 알려진 이름에 대한 재귀적 쿼리와 동일한 응답이 반환됩니다.

(BZ#1700916)

시스템 시간이 변경된 후 dhclient 가 더 이상 IP 주소를 갱신하지 못합니다.

이전에는 시스템 시간이 변경되면 커널이 제거되어 할당된 IP 주소가 손실될 수 있었습니다. 이번 업데이트를 통해 dhclient 는 monotonic 타이머를 사용하여 이전 시간 건너뛰기를 탐지하고 시스템 시간이 중단되는 경우 리스 확장을 위해 DHCPREQUEST 메시지를 발행합니다. 결과적으로 시스템은 설명된 시나리오에서 더 이상 IP 주소를 손실하지 않습니다.

(BZ#1729211)

ipcalc 에서 /31 네트워크의 올바른 브로드캐스트 주소를 반환합니다.

이번 업데이트에서는 RFC 3021 표준을 올바르게 따르도록 ipcalc 유틸리티가 수정되었습니다. 결과적으로 /31 접두사가 인터페이스에 사용되는 경우 ipcalc 는 올바른 브로드캐스트 주소를 반환합니다.

(BZ#1638834)

/etc/services 에 적절한 NRPE 포트 정의 포함

이번 업데이트에서는 **/etc/services** 파일에 적절한 **NRPE(Remote Plug-in Executor)** 서비스 포트 정의가 추가되었습니다.

(BZ#1730396)

postfix DNS 확인자 코드에서 res_ query 대신 res_search 를 사용합니다.

postfix 에서 이전 업데이트 이후 **DNS** 확인기 코드는 **res_ search** 함수 대신 **res_ query** 함수를 사용했습니다. 그 결과 **DNS** 확인자는 다음 **postfix** 구성을 사용하여 현재 및 상위 도메인에서 호스트 이름을 검색하지 않았습니다.

```
# postconf -e "smtp_host_lookup = dns"
# postconf -e "smtp_dns_resolver_options = res_defnames, res_dnsrch"
```

예를 들면 다음과 같습니다.

```
# postconf -e "relayhost = [smtp]"
```

또한 ***example.com*** 형식의 도메인 이름인 **DNS** 확인자는 릴레이에 **smtp.*example.com*** **SMTP** 서버를 사용하지 않았습니다.

이번 업데이트를 통해 **res_ query** 대신 **res_ search** 를 사용하도록 **DNS** 확인자 코드가 변경되었으며 이제 현재 및 상위 도메인에서 호스트 이름을 올바르게 검색합니다.

(BZ#1723950)

PCRE, CDB 및 SQLite를 Postfix와 함께 사용할 수 있음

RHEL 8에서 **postfix** 패키지는 여러 하위 패키지로 분할되었으며 각 하위 패키지는 특정 데이터베이스에 대한 플러그인을 제공합니다. 이전에는 **postfix-pcre,postfix- cdb** 및 **postfix-sqlite** 플러그인을 포함하는 **RPM** 패키지가 배포되지 않았습니다. 결과적으로 이러한 플러그인의 데이터베이스를 **Postfix**와 함께 사용할 수 없었습니다. 이번 업데이트에서는 **PCRE, CDB** 및 **SQLite** 플러그인을 포함하는 **RPM** 패키지가 **AppStream** 리포지토리에 추가되었습니다. 따라서 이러한 플러그인은 적절한 **RPM** 패키지를 설치한 후 사용할 수 있습니다.

(BZ#1745321)

5.4.5. 보안

fapolicyd 가 더 이상 RHEL 업데이트를 금지하지 않음

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

RHBA-2020:5243 권고가 릴리스되면서 **fapolicyd** 는 바이너리 경로의 접미사를 무시하므로 바이너리가 신뢰 데이터베이스와 일치할 수 있습니다. 결과적으로 **fapolicyd** 는 규칙을 올바르게 적용하고 업데이트 프로세스를 완료할 수 있습니다.

(BZ#1897091)

OpenSSL-pkcs11 은 더 이상 여러 장치에 로그인하여 장치를 잠그지 않습니다.

이전에는 **openssl-pkcs11** 엔진이 제공된 **PKCS #11 URI**를 사용하여 첫 번째 검색 결과에 로그인하려고 시도했으며 첫 번째 결과가 의도한 장치가 아니고 **PIN**이 다른 장치와 일치하는 경우에도 제공된 **PIN**을 사용했습니다. 이러한 실패한 인증 시도는 장치를 잠급니다.

이제 **OpenSSL-pkcs11** 이 제공된 **PKCS #11 URI**가 단일 장치와 일치하는 경우에만 장치에 로그인하려고 합니다. 이제 **PKCS #11** 검색에서 둘 이상의 장치를 발견하는 경우 엔진이 의도적으로 실패합니다. 따라서 **openssl-pkcs11** 을 사용하여 장치에 로그인할 때 단일 장치만 일치하는 **PKCS #11 URI**를 제공해야 합니다.

(BZ#1705505)

rpmverifyfile 을 사용하여 OpenSCAP 오프라인 스캔이 제대로 작동합니다

이번 업데이트 이전에는 **OpenSCAP** 스캐너가 오프라인 모드에서 현재 작업 디렉터리를 올바르게 변경하지 않았으며 **fchdir** 함수가 **OpenSCAP rpmverifyfile** 프로브에서 올바른 인수와 함께 호출되지 않았습니다. **OpenSCAP** 스캐너는 오프라인 모드에서 현재 작업 디렉터리를 올바르게 변경하도록 수정되었으며 **rpmverifyfile** 에서 올바른 인수를 사용하도록 **fchdir** 기능이 수정되었습니다. 결과적으로 **OVAL rpmverifyfile**이 포함된 **SCAP** 콘텐츠를 사용하여 임의의 파일 시스템을 스캔할 수 있습니다.

(BZ#1636431)

PKCS #11 장치에 저장된 공개 키와 일치하지 않고 **ECDSA** 개인 키를 사용하는 경우 **httpd** 가 올바르게 시작됩니다.

RSA 키와 달리 **ECDSA** 개인 키에는 공개 키 정보가 반드시 포함되어 있지 않습니다. 이 경우 **ECDSA** 개인 키에서 공개 키를 가져올 수 없습니다. 이러한 이유로 **PKCS #11** 장치는 공개 키 오브젝트인지 인증서 오브젝트인지 여부에 관계없이 공개 키 정보를 별도의 개체에 저장합니다. **OpenSSL**은 개인 키에 공개 키 정보를 포함하도록 엔진에서 제공하는 **EVP_PKEY** 구조를 예상했습니다. **OpenSSL**에 제공할 **EVP_PKEY** 구조를 채울 때 **openssl-pkcs11** 패키지의 엔진은 일치하는 공개 키 오브젝트에서만 공개 키 정보를 가져오고 현재 인증서 오브젝트를 무시하려고 했습니다.

OpenSSL이 엔진에서 **ECDSA** 개인 키를 요청했을 때, 공개 키가 **PKCS #11** 장치에 없는 경우, 제공된 **EVP_PKEY** 구조에 공개 키가 없는 경우 공개 키 정보가 포함되지 않았습니다. 그 결과 공개 키가 필요한 **X509_check_private_key()** 함수라는 **Apache httpd** 웹 서버가 시작 프로세스에서 시작되지 않았기 때문에 **httpd** 가 이 시나리오에서 시작되지 못했습니다. **public-key** 오브젝트를 사용할 수 없는 경우 인증서에서 **EC** 공개 키를 로드하여 이 문제가 해결되었습니다. 결과적으로 **ECDSA** 키가 **PKCS #11** 장치에 저장될 때 **httpd** 가 올바르게 시작됩니다.

(BZ#1664807)

감사 규칙의 **scap-security-guide PCI-DSS** 수정이 올바르게 작동합니다.

이전에는 **scap-security-guide** 패키지에 다음과 같은 시나리오 중 하나가 될 수 있는 수정 및 검사가 포함되어 있었습니다.

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

결과적으로 **RHEL** 설치 프로세스 중에 설치된 시스템의 검사에서 일부 감사 규칙이 실패했거나 오류로 보고되었습니다.

이번 업데이트를 통해 수정이 수정되었으며 **PCI-DSS** 보안 정책으로 설치된 시스템 검사가 더 이상 감사 규칙에 대해 오탐을 보고하지 않습니다.

(BZ#1754919)

OpenSCAP 에서 가상 머신 및 컨테이너의 오프라인 스캔 제공

이전에는 OpenSCAP 코드베이스를 리팩토링하면 특정 RPM 프로브가 오프라인 모드에서 VM 및 컨테이너 파일 시스템을 스캔하지 못했습니다. 결과적으로 openscap-utils 패키지에 oscap- vm 및 oscap-chroot 를 포함할 수 없었습니다. 또한 openscap-containers 패키지는 RHEL 8에서 완전히 제거되었습니다. 이번 업데이트를 통해 프로브의 문제가 수정되었습니다.

결과적으로 RHEL 8에는 openscap-utils 패키지에 oscap-podman, oscap-vm 및 oscap- chroot 툴이 포함됩니다.

(BZ#1618489)

OpenSCAP rpmverifypackage 가 올바르게 작동합니다.

이전에는 chdir 및 chroot 시스템 호출이 rpmverifypackage 프로브에 의해 두 번 호출되었습니다. 그 결과 사용자 지정 OVAL(Open Vulnerability and Assessment Language) 콘텐츠로 OpenSCAP 스캔 중에 프로브를 사용할 때 오류가 발생했습니다. rpmverifypackage 프로브가 chdir 및 chroot 시스템 호출을 올바르게 활용하도록 수정되었습니다. 결과적으로 rpmverifypackage 가 올바르게 작동합니다.

(BZ#1646197)

5.4.6. 네트워킹

qdisc_run 함수에서 잠금으로 인해 커널 충돌이 발생하지 않습니다

이전에는 트래픽을 분리하는 동안 pfifo_fast 대기열이 재설정될 때 패킷 전송이 해제된 후 경쟁 조건이 발생했습니다. 그 결과 커널이 예기치 않게 종료되는 경우가 있었습니다. 이번 업데이트를 통해 qdisc_run 함수의 잠금이 개선되었습니다. 따라서 설명된 시나리오에서 커널이 더 이상 충돌하지 않습니다.

(BZ#1744397)

org.fedoraproject.FirewallD1.config.service의 DBus API가 예상대로 작동합니다.

이전 버전에서는 DBus API getIncludes,setIncludes 및 queryIncludes 함수의 org.fedoraproject.FirewallD1 에서 오류 메시지를 반환했습니다 . org.fedoraproject.FirewallD1.Exception: 잘못된 인덱싱으로 인해 범위를 벗어납니다. 이번 업데이트를 통해 DBus API getIncludes,setIncludes 및 queryIncludes 기능이 예상대로 작동합니다.

(BZ#1737045)

RHEL은 더 이상 ipvs 모듈을 언로드 할 때 커널 경고를 기록하지 않습니다

이전에는 IP 가상 서버(ipvs) 모듈에서 잘못된 참조 수를 사용했기 때문에 모듈을 언로드할 때 경쟁 조건이 발생했습니다. 그 결과 RHEL은 커널 경고를 기록했습니다. 이번 업데이트에서는 경합 조건이 수정되었습니다. 결과적으로 ipvs 모듈을 언로드하면 커널에서 경고를 더 이상 기록하지 않습니다.

(BZ#1687094)

nft 유틸리티는 더 이상 옵션 이외의 첫 번째 인수 이후 인수를 명령줄 옵션으로 해석하지 않습니다.

이전에는 nft 유틸리티에서 nft 명령의 모든 옵션을 허용했습니다. 예를 들어 관리자는 옵션 이외의 인수 간 또는 이후에 옵션을 사용할 수 있습니다. 그 결과 선행 대시로 인해 nft 가 음수 우선 순위 값을 옵션으로 해석하고 명령이 실패했습니다. 첫 번째 비옵션 인수를 읽은 후 대시로 시작하는 인수를 해석하지 않도록 nft 유틸리티의 명령줄 구문 분석기가 업데이트되었습니다. 결과적으로 관리자는 음수 우선 순위 값을 nft 로 전달하는 해결방법이 더 이상 필요하지 않습니다.

이 변경으로 인해 이제 첫 번째 옵션이 아닌 첫 번째 인수 전에 모든 command-options를 nft 로 전달해야 합니다. 업데이트하기 전에 이 업데이트를 설치한 후 스크립트가 예상대로 작동하는지 확인하기 위해 이 새 기준과 일치하도록 nftables 스크립트를 확인하십시오.

(BZ#1778883)

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

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

(BZ#1663556)

영역 드리프트를 비활성화하기 위해 구성 매개 변수가 firewalld 에 추가되었습니다.

이전에는 firewalld 서비스에 "zone drifting"이라는 문서화되지 않은 동작이 포함되어 있었습니다. RHEL 8.0은 보안에 부정적인 영향을 미칠 수 있으므로 이 동작을 제거했습니다. 그 결과 이 동작을 사용하여 범용 또는 폴백 영역을 구성하는 호스트에서 firewalld 는 이전에 허용된 연결을 거부했습니다. 이번 업데이트에서는 영역 드리프트 동작을 구성 가능한 기능으로 다시 추가합니다. 결과적으로 사용자는 이제 영역 드리프트 사용을 결정하거나 더 안전한 방화벽 설정에 대한 동작을 비활성화할 수 있습니다.

기본적으로 RHEL 8.2에서는 /etc/firewalld/firewalld.conf 파일의 새로운 AllowZoneDrifting 매개 변수가 yes 로 설정됩니다. 매개 변수가 활성화된 경우 firewalld 로그는 다음과 같습니다.

```
WARNING: AllowZoneDrifting is enabled. This is considered an insecure configuration option. It will
be removed in a future release. Please consider disabling it now.
```

(BZ#1772208)

5.4.7. 커널

하위 섹션 메모리 핫플러그가 완전히 지원됨

이전에는 일부 플랫폼은 **DMM(Dual In-Line Modules)**과 같은 실제 메모리 영역을 조정하고 인터리브 세트를 **64MiB** 메모리 경계로 조정했습니다. 그러나 **Linux** 핫플러그 하위 시스템은 **128MiB**의 메모리 크기를 사용하므로 새 장치를 핫플러그하면 여러 메모리 영역이 단일 핫플러그 메모리 창에서 중복되었습니다. 이로 인해 다음 또는 유사한 호출 추적을 사용하여 사용 가능한 영구 메모리 네임스페이스가 나열되지 않았습니다.

```
WARNING: CPU: 38 PID: 928 at arch/x86/mm/init_64.c:850
add_pages+0x5c/0x60
   [..]
   RIP: 0010:add_pages+0x5c/0x60
   [..]
   Call Trace:
    devm_memremap_pages+0x460/0x6e0
    pmem_attach_disk+0x29e/0x680 [nd_pmem]
    ? nd_dax_probe+0xfc/0x120 [libnvdimm]
    nvdimm_bus_probe+0x66/0x160 [libnvdimm]
```

이번 업데이트에서는 문제를 해결하고 **Linux** 핫플러그 하위 시스템을 지원하여 여러 메모리 지역이 단일 핫플러그 메모리 창을 공유할 수 있도록 합니다.

(BZ#1724969)

데이터 손상으로 인해 WARN 메시지 대신 BUG가 트리거됩니다.

이번 개선된 기능을 통해 **lib/list_debug.c** 의 목록 손상이 이제 **vmcore** 가 포함된 보고서를 생성하는 **BUG**가 트리거됩니다. 이전 버전에서는 데이터 손상이 발생하면 눈에 띄지 않은 간단한 **WARN**이 생성되었습니다. **CONFIG_BUG_ON_DATA_CORRUPTION**을 설정하면 이제 커널에서 충돌을 생성하고 데이터 손상에 대한 응답으로 **BUG**를 트리거합니다. 이로 인해 추가 손상을 방지하고 보안 위험을 줄입니다. **kdump** 는 이제 데이터 손상 버그 보고를 개선하는 **vmcore** 를 생성합니다.

(BZ#1714330)

Intel Valsville 카드 지원은 사용할 수 있지만 **RHEL 8.2**에서 확인되지 않았습니다.

Intel Valsville 카드 지원은 제공되지만 Red Hat Enterprise Linux 8.2에서는 테스트되지 않았습니다.

(BZ#1720227)

RPS 및 XPS가 더 이상 분리된 CPU에 작업을 배치하지 않음

이전에는 RPM(Receive Packet Buildering) 소프트웨어 대기열 메커니즘과 XPS(Transmit Packet Trackering) 전송 대기열 선택 메커니즘이 격리된 CPU를 포함하여 모든 CPU 세트에서 할당된 작업을 수행했습니다. 결과적으로 대기 시간에 민감한 워크로드가 RPS 또는 XPS 작업이 실행 중인 동일한 CPU를 사용하는 경우 실시간 환경에서 예기치 않은 대기 시간이 급증할 수 있었습니다. 이번 업데이트를 통해 store_rps_map() 함수에는 RPS 구성을 위해 격리된 CPU가 포함되지 않습니다. 마찬가지로 XPS 구성에 사용되는 커널 드라이버는 CPU 격리를 사용합니다. 결과적으로 RPS 및 XPS가 설명된 시나리오에서 격리된 CPU에 더 이상 작업을 배치하지 않습니다. /sys/devices/pci*/net/dev/queues/rx-*/rps_cpus 파일에서 격리된 CPU를 구성하는 경우 다음 오류가 나타납니다.

```
Error: "-bash: echo:write error: Invalid argument"
```

그러나 /sys/devices/pci*/net/dev/queues/tx-*/xps_cpus 파일에서 격리된 CPU를 수동으로 구성하면 분리된 CPU에 XPS 작업이 성공적으로 할당됩니다.

격리된 CPU가 있는 환경의 네트워킹 워크로드에는 몇 가지 성능 변형이 발생할 수 있습니다.

(BZ#1867174)

5.4.8. 파일 시스템 및 스토리지

SCSI 드라이버가 더 이상 과도한 양의 메모리를 사용하지 않습니다

이전에는 특정 SCSI 드라이버에서 RHEL 7보다 많은 양의 메모리를 사용했습니다. 특정 경우(예: 파이버 채널 HBA(호스트 버스 어댑터)에 vPort 생성) 시스템 구성에 따라 메모리 사용량이 과도하게 사용되었습니다.

메모리 사용량 증가는 블록 계층의 메모리 사전 할당으로 인해 발생했습니다. 각 I/O 요청에 대해 다중 대기열 블록 장치 스케줄링(BLK-MQ) 및 다중 대기열 SCSI 스택(SCSI-MQ) 모두 사전 할당된 메모리로 이어 메모리 사용량이 증가합니다.

이번 업데이트를 통해 블록 계층은 메모리 사전 할당 양을 제한하므로 SCSI 드라이버에서 더 이상 과도한 양의 메모리를 사용하지 않습니다.

(BZ#1698297)

UDS가 다시 빌드를 완료하기 전에 VDO를 일시 중지할 수 있습니다.

이전에는 UDS 인덱스가 다시 빌드되는 동안 VDO 볼륨을 일시 중지하려고 하면 dmsetup suspend 명령이 응답하지 않았습니다. 명령은 다시 빌드한 후에만 완료됩니다.

이번 업데이트를 통해 문제가 해결되었습니다. dmsetup suspend 명령은 응답하지 않고 UDS 재빌드를 수행하기 전에 완료할 수 있습니다.

(BZ#1737639)

5.4.9. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

mod_cgid 로깅의 문제가 해결되었습니다

이 업데이트 이전에는 mod_cgid Apache httpd 모듈이 스레드 MPM(Multi-processing module)에서 사용된 경우 다음과 같은 로깅 문제가 발생했습니다.

- CGI 스크립트의 stderr 출력 앞에는 표준 타임스탬프 정보가 포함되지 않았습니다.
- CGI 스크립트의 stderr 출력이 VirtualHost 에 대한 로그 파일로 올바르게 리디렉션되지 않았습니다(설정된 경우).

이번 업데이트에서는 문제가 해결되어 mod_cgid 로깅이 예상대로 작동합니다.

(BZ#1633224)

5.4.10. 컴파일러 및 개발 도구

dlopen 에 실패하는 경우 할당되지 않고 초기화되지 않은 공유 오브젝트로 인해 더 이상 실패하지 않습니다.

이전에는 dlopen 호출이 실패하면 오류를 보고하기 전에 glibc 동적 링커에서 NODELETE 표시가 있는 공유 개체를 제거하지 않았습니다. 결과적으로 재배치되지 않고 초기화되지 않은 공유 오브젝트가 프로세스 이미지에 남아 있어 어설션 실패 또는 충돌이 발생했습니다. 이번 업데이트를 통해 동적 로더는 보류 중인 NODELETE 상태를 사용하여 dlopen 실패 시 공유 개체를 제거한 후 이를 영구적으로

NODELETE 로 표시합니다. 결과적으로 프로세스가 재배치되지 않은 오브젝트를 그대로 두지 않습니다. 또한 ELF 생성자와 구조자가 실행되는 동안 지연 바인딩 오류는 이제 프로세스를 종료합니다.

(BZ#1410154)

64비트 ARM 아키텍처의 고급 SIMD 기능은 lazily가 해결되면 더 이상 잘못 컴파일되지 않습니다.

이전에는 고급 SIMD 기능을 지연할 때 특정 호출자 저장 레지스터를 올바르게 저장하고 복원하지 않은 고급 SIMD의 새로운 CVS(Varlier Procedure Call Standard)가 실패했습니다. 이로 인해 런타임 시 바이너리가 잘못될 수 있었습니다. 이번 업데이트를 통해 기호 테이블의 Advanced SIMD 및 SVE 벡터 함수는 .variant_pcs 와 함께 표시되며 그 결과 동적 링커가 이러한 기능을 조기에 바인딩합니다.

(BZ#1726641)

sudo 래퍼 스크립트에서 옵션을 구문 분석합니다

이전에는 /opt/redhat/devtoolset*/root/usr/bin/sudo 래퍼 스크립트가 sudo 옵션을 올바르게 구문 분석하지 않았습니다. 결과적으로 일부 sudo 옵션(예: sudo -i)을 실행할 수 없습니다. 이번 업데이트를 통해 더 많은 sudo 옵션이 올바르게 구문 분석되고 sudo 래퍼 스크립트가 /usr/bin/sudo 처럼 작동합니다.

(BZ#1774118)

glibc 에서 TLS 변수 정렬이 수정되었습니다

이전에는 특정 조건에서 정렬된 스레드-로컬 스토리지(TLS) 데이터가 예상 정렬 없이 인스턴스화될 수 있었습니다. 이번 업데이트를 통해 모든 조건에서 올바르게 정렬되도록 POSIX 스레드 라이브러리 libpthread 가 향상되었습니다. 결과적으로 정렬된 TLS 데이터가 올바른 정렬을 통해 모든 스레드에 대해 올바르게 인스턴스화됩니다.

(BZ#1764214)

EINTR 또는 E AGAIN 오류 다음에 반복된 pututxline 호출이 더 이상 utmp 파일이 손상되지 않음

pututxline 함수가 잠금을 획득하려고 시도하고 시간 내에 성공하지 못하면 이 함수는 EINTR 또는 E AGAIN 오류 코드를 반환합니다. 이전에는 pututxline 을 즉시 호출하여 잠금을 얻기 위해 관리하면 utmp 파일에서 이미 할당된 일치하는 슬롯을 사용하지 않았지만 다른 항목을 추가했습니다. 그 결과 사용되지 않은 이러한 항목은 utmp 파일의 크기를 크게 높였습니다. 이번 업데이트에서는 문제가 해결되어 이제 utmp 파일에 항목이 올바르게 추가됩니다.

(BZ#1749439)

내부 오류가 발생할 때 더 이상 mtrace 가 중단되지 않습니다

이전에는 mtrace 툴 구현의 결함으로 인해 메모리 추적이 중단될 수 있었습니다. 이 문제를 해결하기 위해 mtrace 메모리 추적 구현이 내부 오류가 발생해도 중단되지 않도록 더욱 강력해졌습니다. 결과적으로 사용자가 mtrace 를 호출할 수 있으며 더 이상 중단되지 않고 바인딩된 시간으로 완료합니다.

(BZ#1764235)

fork 기능은 pthread_atfork사용과 관련된 특정 교착 상태를 방지합니다.

이전 버전에서는 프로그램이 atfork 핸들러를 등록하고 비동기-신호 처리기에서 포크 를 호출한 경우 내부 구현 의존적 잠금의 결함으로 인해 프로그램이 중단될 수 있었습니다. 이번 업데이트를 통해 단일 스레드 프로그램에서 fork 및 해당 atfork 핸들러 구현이 조정되어 교착 상태가 발생하지 않습니다.

(BZ#1746928)

strstr 는 더 이상 잘린 패턴에 대해 잘못된 일치 항목을 반환하지 않습니다

특정 IBM Z 플랫폼(이전 arch13으로 알려짐)에서 페이지 경계를 통과하는 검색 패턴을 처리할 때 strstr 함수가 CPU 레지스터를 올바르게 업데이트하지 않았습니다. 그 결과 strstr 가 잘못된 일치를 반환했습니다. 이번 업데이트에서는 문제가 해결되어 strstr 가 언급된 시나리오에서 예상대로 작동합니다.

(BZ#1777241)

glibc 에서 c.UTF-8 로케일 소스 줄임표 표현식이 수정되었습니다.

이전에는 C.UTF-8 소스 로케일의 결함으로 인해 U+10000 이상의 모든 유니코드 코드 포인트에 배치 가중치가 없었습니다. 그 결과 U+10000 이상의 모든 코드 포인트는 예상대로 조회되지 않았습니다. C.UTF-8 소스 로케일이 수정되었으며 새로 컴파일된 바이너리 로케일의 모든 유니코드 코드 포인트에 대한 배치 가중치가 있습니다. 컴파일된 C.UTF-8 로케일은 이번 수정의 결과로 5.3MiB 더 큽니다.

(BZ#1361965)

getpwent()를 호출하지 않고 setpwent() 를 호출할 때 glibc 가 더 이상 실패하지 않습니다.

/etc/nsswitch.conf 파일이 Berkeley DB (db) 암호 공급자를 가리키는 경우, 먼저 setpwent()를 호출하지 않고 getpwent() 함수를 사용하여 데이터를 요청할 수 있습니다. endpwent() 함수를 호출할 때, 새

쿼리를 허용하도록 **end pwent()**를 재설정할 수 없기 때문에 **setpwent()** 를 먼저 호출하지 않고 **get pwent()** 에 대한 추가 호출으로 **glibc** 가 실패했습니다. 이번 업데이트에서는 문제가 해결되었습니다. 결과적으로 **endpwent()**로 하나의 쿼리를 종료하면 **set pwent()** 를 호출하지 않아도 **getpwent()** 에 대한 추가 호출이 새 쿼리를 시작합니다.

(BZ#1747502)

ltrace 는 강화된 바이너리에서 시스템 호출을 추적할 수 있음

이전에는 **ltrace** 가 **AMD** 및 **Intel 64**비트 아키텍처에서 시스템 바이너리와 같은 강화된 특정 바이너리에서 결과를 생성하지 않았습니다. 이번 업데이트를 통해 이제 **ltrace** 가 강화된 바이너리에서 시스템 호출을 추적할 수 있습니다.

(BZ#1655368)

Intel의 **JCC** 취약점이 더 이상 **GCC** 컴파일러에서 상당한 성능 저하를 초래하지 않음

특정 **Intel CPU**는 **JCC(Jump Conditional Code)** 버그의 영향을 받기 때문에 시스템 지침이 잘못 실행됩니다. 결과적으로 영향을 받는 **CPU**가 프로그램을 제대로 실행하지 못할 수 있습니다. 전체 수정을 위해서는 취약한 **CPU**의 마이크로 코드를 업데이트하여 성능 저하를 일으킬 수 있습니다. 이번 업데이트를 통해 어셈블러에서 성능 손실을 줄이는 데 도움이 되는 해결 방법을 사용할 수 있습니다. 해결방법은 기본적으로 활성화되어 있지 않습니다.

해결방법을 적용하려면 **GCC**를 **-Wa,-mbranches-with-32B-boundaries** 명령줄 옵션과 함께 사용하여 프로그램을 다시 컴파일합니다. 이 명령줄 옵션으로 다시 컴파일된 프로그램은 **JCC** 취약점의 영향을 받지 않지만 시스템을 완전히 보호하는 데 여전히 마이크로 코드 업데이트가 필요합니다.

해결방법을 적용하면 프로그램의 크기가 증가하며 재컴파일이 없으면 성능이 저하될 수 있습니다.

(BZ#1777002)

병렬 빌드를 사용할 때 더 이상 느려지지 않음

이전에는 병렬 빌드를 실행하는 동안 전환을 기다리는 동안 하위 프로세스가 일시적으로 응답하지 않을 수 있었습니다. 결과적으로 높은 **-j** 값이 있는 빌드가 더 낮은 유효 **-j** 값에서 느려지거나 실행되었습니다. 이번 업데이트를 통해 이제 **make** 의 작업 제어 논리가 차단되지 않았습니다. 결과적으로 상위 **-j** 값이 있는 빌드가 **full -j** 속도로 실행됩니다.

(BZ#1774790)

ltrace 툴에서 함수 호출을 올바르게 보고합니다

모든 **RHEL** 구성 요소에 적용된 바이너리 강화 기능이 개선되어 이전에 **ltrace** 툴에서 **RHEL** 구성 요소의 바이너리 파일의 함수 호출을 탐지할 수 없었습니다. 결과적으로 이러한 바이너리 파일에 사용될 때 탐지된 호출을 보고하지 않았기 때문에 **ltrace** 출력이 비어 있었습니다. 이번 업데이트에서는 **ltrace** 가 함수 호출을 처리하는 방식이 수정되어 설명된 문제가 발생하지 않습니다.

(BZ#1618748)

5.4.11. IdM (Identity Management)

dsctl 유틸리티가 하이픈 이름으로 더 이상 인스턴스를 관리하지 못합니다.

이전에는 **dsctl** 유틸리티가 **Directory Server** 인스턴스 이름에서 하이픈을 올바르게 구문 분석하지 않았습니다. 결과적으로 관리자는 **dsctl** 을 사용하여 이름으로 하이픈으로 인스턴스를 관리할 수 없었습니다. 이번 업데이트에서는 문제가 해결되어 이제 **dsctl** 이 언급된 시나리오에서 예상대로 작동합니다.

(BZ#1715406)

Directory Server 인스턴스 이름은 이제 최대 **103**자를 가질 수 있습니다.

LDAP 클라이언트가 **Directory Server**에 대한 연결을 설정하면 서버는 로컬 버퍼에 클라이언트 주소와 관련된 정보를 저장합니다. 이전에는 이 버퍼의 크기가 **46**자보다 긴 **LDAPI** 경로 이름을 저장하기에 너무 작았습니다. 예를 들어 **Directory Server** 인스턴스의 이름이 너무 긴 경우입니다. 결과적으로 버퍼 오버플로로 인해 서버가 예기치 않게 종료되었습니다. 이번 업데이트에서는 **NSPR(Netscape Portable Runtime)** 라이브러리에서 경로 이름에 대해 지원하는 최대 크기까지 버퍼 크기가 증가합니다. 결과적으로 **Directory Server**가 더 이상 충돌하지 않습니다.

NSPR 라이브러리의 제한으로 인해 인스턴스 이름은 최대 **103**자일 수 있습니다.

(BZ#1748016)

pkidestroy 유틸리티에서 올바른 인스턴스를 선택

이전 버전에서는 **pkidestroy --force** 명령을 반 삭제 인스턴스에서 실행한 경우 **-i** 인스턴스 옵션으로 지정된 인스턴스 이름에 관계없이 기본적으로 **pki-tomcat** *인스턴스*를 선택했습니다.

결과적으로 원하는 인스턴스 대신 **pki-tomcat** 인스턴스가 제거되어 **--remove-logs** 옵션이 의도한 인스턴스의 로그를 제거하지 않았습니다. **pkidestroy** 는 이제 올바른 인스턴스 이름을 적용하여 원하는 인

스턴스의 남은 작업만 제거합니다.

(BZ#1698084)

sssd-ldap 도움말 페이지에서 ldap_user_authorized_service 설명이 업데이트되었습니다.

RHEL 8에서는 PAM(Pluggable Authentication Module) 스택이 변경되었습니다. 예를 들어 systemd 사용자 세션은 이제 systemd-user PAM 서비스를 사용하여 PAM 대화를 시작합니다. 이제 이 서비스에는 pam_sss.so 인터페이스가 포함될 수 있는 system-auth PAM 서비스가 재귀적으로 포함됩니다. 즉, SSSD 액세스 제어는 항상 호출됩니다.

RHEL 8 시스템에 대한 액세스 제어 규칙을 설계할 때 이러한 변경 사항을 알고 있어야 합니다. 예를 들어 systemd-user 서비스를 허용된 서비스 목록에 추가할 수 있습니다.

IPA HBAC 또는 AD GPO와 같은 일부 액세스 제어 메커니즘의 경우 systemd-user 서비스가 기본적으로 허용된 서비스 목록에 추가되어 작업을 수행할 필요가 없습니다.

이 정보를 포함하도록 sssd-ldap 도움말 페이지가 업데이트되었습니다.

(BZ#1669407)

IdM에서 AD 신뢰 지원을 활성화하면 필수 DNS 레코드에 대한 정보가 표시됩니다.

이전 버전에서는 외부 DNS 관리를 통한 Red Hat Enterprise Linux IdM(Identity Management) 설치에 대한 AD(Active Directory) 신뢰 지원을 활성화할 때 필수 DNS 레코드에 대한 정보가 표시되지 않았습니다. 수동으로 ipa dns-update-system-records --dry-run 명령을 입력하는 것은 IdM에 필요한 모든 DNS 레코드 목록을 가져오는 것이 바람직했습니다.

이번 업데이트를 통해 ipa-adtrust-install 명령은 DNS 영역에 수동으로 추가하기 위한 DNS 서비스 레코드를 올바르게 나열합니다.

(BZ#1665051)

5.4.12. 데스크탑

소프트웨어 렌더러를 사용할 때 Wayland의 GNOME 쉘이 더 이상 느리게 작동하지 않음

이전에는 소프트웨어 렌더러를 사용할 때 GNOME Shell의 Wayland 백엔드에서 캐시 가능한 프레임 버퍼를 사용하지 않았습니다. 그 결과 Wayland에서 소프트웨어 렌더링 GNOME 쉘이 X.org 백엔드의 소프트웨어 렌더링된 GNOME 쉘과 비교했을 때 속도가 느렸습니다.

이번 업데이트를 통해 Wayland의 GNOME 쉘에 중간 섀도 프레임 버스퍼가 추가되었습니다. 그 결과 Wayland에서 소프트웨어 렌더링 GNOME 쉘은 물론 X.org에서 GNOME 쉘도 수행할 수 있게 되었습니다.

(BZ#1737553)

5.4.13. 가상화

10세대 Intel Core 프로세서에서 VM을 시작하면 더 이상 실패하지 않습니다

이전에는 Icelake-Server라고도 하는 10세대 Intel Core 프로세서를 사용하는 호스트 모델에서 VM(가상 시스템)을 시작하지 못했습니다. 이번 업데이트를 통해 libvirt 는 QEMU에서 지원하지 않는 pconfig CPU 기능을 더 이상 비활성화하지 않습니다. 따라서 10세대 Intel 프로세서를 실행하는 호스트 모델에서 VM을 시작하면 더 이상 실패하지 않습니다.

(BZ#1749672)

이제 cloud-init 를 사용하여 Microsoft Azure에 가상 머신 프로비저닝이 올바르게 작동합니다.

이전에는 Microsoft Azure 플랫폼에서 RHEL 8 가상 시스템(VM)을 프로비저닝하는 데 cloud-init 유틸리티를 사용할 수 없었습니다. 이번 업데이트에서는 Azure 끝점의 cloud-init 처리가 수정되어 Azure에서 RHEL 8 VM 프로비저닝이 예상대로 진행됩니다.

(BZ#1641190)

RHEL 7 호스트의 RHEL 8 가상 머신의 해상도가 매우 높아진 상태에서 안정적으로 볼 수 있습니다.

이전 버전에서는 RHEL 7 호스트 시스템에서 실행 중인 RHEL 8 가상 머신(VM)을 사용할 때 kiosk 모드에서 애플리케이션 실행과 같은 VM의 그래픽 출력을 표시하는 특정 방법을 사용할 수 없었습니다. 더 큰 해상도를 사용할 수 없었습니다. 결과적으로 이러한 방법을 사용하는 VM은 호스트 하드웨어에서 더 높은 해상도를 지원하더라도 최대 redhatx1200까지만 작동했습니다. 이번 업데이트에서는 설명된 문제가 발생하지 않도록 Kiali 및 QXL 드라이버를 조정합니다.

(BZ#1635295)

cloud-init 를 사용하여 ESXi VM 사용자 정의 및 VM 재부팅이 올바르게 작동합니다.

이전 버전에서는 VMware ESXi 하이퍼바이저에서 실행 중인 VM(가상 시스템)을 수정하는 데 고정 IP를 사용하고 VM을 복제한 경우, 경우에 따라 새 복제 VM이 재부팅하는 데 시간이 오래 걸렸습니다. 이번 업데이트에서는 cloud-init 에서 VM의 고정 IP를 DHCP에 다시 작성하지 않도록 수정하여 설명된 문제가 발생하지 않습니다.

(BZ#1666961, BZ#1706482)

5.4.14. 컨테이너

quay.io 레지스트리에서 이미지를 가져오면 더 이상 의도하지 않은 이미지가 발생하지 않습니다.

이전에는 /etc/containers/registries.conf에 제공된 기본 레지스트리 검색 목록에 quay. io 컨테이너 이미지 레지스트리가 나열되어 짧은 이름을 사용할 때 사용자가 스푸핑된 이미지를 가져올 수 있었습니다. 이 문제를 해결하기 위해 quay.io 컨테이너 이미지 레지스트리가 /etc/containers/registries.conf 의 기본 레지스트리 검색 목록에서 제거되었습니다. 결과적으로 quay.io 레지스트리에서 이미지를 가져오려면 사용자가 quay.io /myorg/myimage 와 같은 전체 리포지토리 이름을 지정해야 합니다. quay.io 레지스트리를 /etc/containers/registries.conf 의 기본 레지스트리 검색 목록에 다시 추가하여 짧은 이름을 사용하여 컨테이너 이미지 가져오기를 다시 활성화할 수 있지만 보안 위험이 발생할 수 있으므로 권장되지는 않습니다.

(BZ#1784267)

5.5. 기술 프리뷰

다음 부분에서는 Red Hat Enterprise Linux 8.2에서 사용할 수 있는 모든 기술 프리뷰 목록을 제공합니다.

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

5.5.1. 네트워킹

NMState 를 기술 프리뷰로 사용 가능

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

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

(BZ#1674456)

AF_XDP 를 기술 프리뷰로 사용 가능(_X)

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

(BZ#1633143)

XDP를 기술 프리뷰로 이용 가능

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

(BZ#1503672)

KTLS는 기술 프리뷰로 사용 가능

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

(BZ#1570255)

dracut 유틸리티는 NetworkManager를 기술 프리뷰로 지원하는 initrd 이미지 생성을 지원

기본적으로 dracut 유틸리티는 쉘 스크립트를 사용하여 초기 RAM 디스크(initrd)의 네트워킹을 관리합니다. 경우에 따라 시스템이 RAM 디스크에서 NetworkManager를 사용하여 네트워크를 구성하는 운영 체제로 전환되는 경우 문제가 발생할 수 있습니다. 예를 들어 RAM 디스크의 스크립트가 이미 IP 주소를 요청한 경우에도 NetworkManager에서 다른 DHCP 요청을 보낼 수 있습니다. 이 RAM 디스크의 요청으로 인해 시간이 초과될 수 있었습니다.

이러한 종류의 문제를 해결하기 위해 RHEL 8.2의 dracut 을 이제 RAM 디스크에서 NetworkManager를 사용할 수 있습니다. 다음 명령을 사용하여 기능을 활성화하고 RAM 디스크 이미지를 다시 생성합니다.

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

Red Hat은 기술 프리뷰 기능을 지원하지 않습니다. 그러나 이 기능에 대한 피드백을 제공하려면 **Red Hat** 지원팀에 문의하십시오.

(BZ#1626348)

mlx5_core 드라이버는 **Mellanox ConnectX-6 Dx** 네트워크 어댑터를 기술 프리뷰로 지원

이번 개선된 기능에는 **Mellanox ConnectX-6 Dx** 네트워크 어댑터의 **PCI ID**가 **mlx5_core** 드라이버에 추가됩니다. 이 어댑터를 사용하는 호스트에서 **RHEL**은 **mlx5_core** 드라이버를 자동으로 로드합니다. **Red Hat**은 지원되지 않는 기술 프리뷰로 이 기능을 제공합니다.

(BZ#1687434)

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)

5.5.2. 커널

기술 프리뷰로 **kexec** 빠른 재부팅

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

(BZ#1769727)

eBPF를 기술 프리뷰로 이용 가능

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

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

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

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

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

- eBPF 가상 시스템을 활용하는 고급 추적 언어인 bpftrace.
- eBPF 가상 시스템을 사용하여 커널에서 빠른 패킷 처리를 가능하게 하는 네트워킹 기술인 eXpress Data Path(XDP) 기능입니다.

(BZ#1559616)

libbpf는 기술 프리뷰로 사용 가능

libbpf 패키지는 현재 기술 프리뷰로 사용할 수 있습니다. libbpf 패키지는 bpf trace 및 bpf /xdp 개발과 같은 bpf 관련 애플리케이션에 중요합니다.

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

(BZ#1759154)

RHEL 8의 기술 프리뷰로 사용 가능한 igc 드라이버

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

(BZ#1495358)

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)

5.5.3. 파일 시스템 및 스토리지

NVMe/TCP를 기술 프리뷰로 사용 가능

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

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

NVMe/TCP 대상 기술 프리뷰는 테스트 목적으로만 포함되며 현재는 완전 지원을 위해 계획되어 있지 않습니다.

(BZ#1696451)

ext4 및 XFS에서 기술 프리뷰로 파일 시스템 DAX 사용 가능

Red Hat Enterprise Linux 8.2에서 DAX 파일 시스템 DAX는 기술 프리뷰로 사용할 수 있습니다. DAX는 애플리케이션이 영구 메모리를 주소 공간으로 직접 매핑할 수 있는 수단을 제공합니다. DAX를 사용하려면 시스템에 몇 가지 형태의 영구 메모리를 사용할 수 있어야 합니다. 일반적으로 하나 이상의 비 Volatile 듀얼 인라인 메모리 모듈(NVDIMM) 형식이며 DAX를 지원하는 파일 시스템은 NVDIMM에서 생성해야 합니다. 또한 dax 마운트 옵션을 사용하여 파일 시스템을 마운트해야 합니다. 그런 다음 dax 마운트된 파일 시스템에 있는 파일의 mmap 을 통해 스토리지가 애플리케이션의 주소 공간에 직접 매핑됩니다.

(BZ#1627455)

OverlayFS

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

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

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

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

- 현재 XFS만 더 낮은 계층 파일 시스템으로 사용하도록 지원됩니다.

또한 OverlayFS를 사용하는 경우 다음 규칙과 제한 사항이 적용됩니다.

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

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

  - O_RDONLY 로 열린 하위 파일은 파일을 읽을 때 st_atime 업데이트를 받지 않습니다.

  - O_RDONLY 로 더 낮은 파일을 연 다음 MAP_SHARED 로 매핑된 파일은 후속 수정과 일치하지 않습니다.

- 전체 호환 **st_** 또는 **d_** 값은 **RHEL 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.

- **XFS**에 사용되는 명령:

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

- **SELinux** 보안 레이블은 **OverlayFS**를 사용하여 지원되는 모든 컨테이너 엔진에서 기본적으로 활성화됩니다.

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

(BZ#1690207)

Stratis를 기술 프리뷰로 사용 가능

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

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

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

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

Stratis는 기술 프리뷰로 제공됩니다.

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

RHEL 8.2에서 **Stratis**를 버전 **2.0.0**으로 업데이트합니다. 이 버전은 안정성과 **Stratis DBus API**를 향상시킵니다.

(JIRA:RHELPLAN-1212)

IdM에서 **IdM** 도메인 멤버에서 기술 프리뷰로 **Samba** 서버 설정 지원

이번 업데이트를 통해 **IdM(Identity Management)** 도메인 멤버에 **Samba** 서버를 설정할 수 있습니다. 동일한 패키지에서 제공하는 새로운 **ipa-client-samba** 유틸리티는 **Samba**별 **Kerberos** 서비스 주체를 **IdM**에 추가하고 **IdM** 클라이언트를 준비합니다. 예를 들어 유틸리티는 **sss ID** 매핑 백엔드에 대한 **ID** 매핑 구성을 사용하여 **/etc/samba/smb.conf** 를 만듭니다. 결과적으로 관리자가 **IdM** 도메인 멤버에 **Samba**를 설정할 수 있습니다.

IdM Trust 컨트롤러가 글로벌 카탈로그 서비스를 지원하지 않기 때문에 **AD-Enrolled Windows** 호스

트는 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)

5.5.4. 고가용성 및 클러스터

Pacemaker podman 번들을 기술 프리뷰로 이용 가능

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

(BZ#1619620)

corosync-qdevice 의 추론을 기술 프리뷰로 사용 가능

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

(BZ#1784200)

새로운 fence-agents-heuristics-ping 펜스 에이전트

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

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

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

(BZ#1775847)

5.5.5. IdM (Identity Management)

ID 관리 JSON-RPC API를 기술 프리뷰로 사용 가능

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

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

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

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

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

(BZ#1664719)

IdM에서 DNSSEC 사용 가능

통합된 DNS가 있는 IdM(Identity Management) 서버는 DNS 프로토콜의 보안을 강화하는 DNS로의 확장 기능 세트인 DNSSEC(DNS Security Extensions)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)

공개 키 인프라의 전반적인 상태를 기술 프리뷰로 확인할 수 있습니다

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

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

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

(BZ#1303254)

5.5.6. 데스크탑

64비트 ARM 아키텍처용 GNOME을 기술 프리뷰로 사용 가능

이제 64비트 ARM 아키텍처에서 기술 프리뷰로 GNOME 데스크탑 환경을 사용할 수 있습니다. 이를 통해 관리자는 VNC 세션을 사용하여 원격으로 GUI(그래픽 사용자 인터페이스)에서 서버를 구성하고 관

리할 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#1667516, BZ#1667225, BZ#1724302)

5.5.7. 그래픽 인프라

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

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

(BZ#1698565)

5.5.8. Red Hat Enterprise Linux 시스템 역할

RHEL 시스템 역할의 postfix 역할을 기술 프리뷰로 사용 가능

Red Hat Enterprise Linux 시스템 역할은 Red Hat Enterprise Linux 하위 시스템에 대한 구성 인터페이스를 제공하므로 Ansible 역할을 포함하여 시스템 구성이 더 쉬워집니다. 이 인터페이스를 사용하면 여러 버전의 Red Hat Enterprise Linux에서 시스템 구성을 관리할 수 있을 뿐 아니라 새로운 주요 릴리스를 채택할 수 있습니다.

rhel-system-roles 패키지는 AppStream 리포지토리를 통해 배포됩니다.

postfix 역할은 기술 프리뷰로 사용할 수 있습니다.

다음 역할은 완전히 지원됩니다.

- kdump

- network
- selinux
- storage
- timesync

자세한 내용은 RHEL 시스템 역할에 대한 지식베이스 문서를 참조하십시오.

(BZ#1812552)

rhel-system-roles-sap 을 기술 프리뷰로 이용 가능

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

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

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

자세한 내용은 SAP용 Red Hat Enterprise Linux 시스템 역할을 참조하십시오.

참고: SAP 솔루션용 RHEL 8.2는 Intel 64 아키텍처 및 IBM POWER9에서 SAP HANA와 함께 사용할 수 있도록 검증될 예정입니다. SAP NetWeaver 및 SAP ASE와 같은 다른 SAP 애플리케이션 및 데이터

베이스 제품에 대한 지원은 GA 릴리스에 묶여 있으며, 고객은 GA에서 RHEL 8.2 기능을 사용할 수 있습니다. 검증된 릴리스 및 SAP 지원에 대한 최신 정보는 SAP Notes 2369910 및 2235581을 참조하십시오.

(BZ#1660832)

5.5.9. 가상화

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

Hyper-V 하이퍼바이저에서 실행되는 Red Hat Enterprise Linux 게스트 운영 체제는 이제 ixgbevf 및 i 40evf 드라이버에서 지원하는 Intel 네트워크 어댑터에 SR-IOV(Single-root I/O Virtualization) 기능을 사용할 수 있습니다. 이 기능은 다음 조건이 충족되면 활성화됩니다.

- NIC(네트워크 인터페이스 컨트롤러)에 SR-IOV 지원이 활성화됨
- 가상 NIC에 대해 SR-IOV 지원이 활성화됨
- 가상 스위치에 SR-IOV 지원이 활성화됨
- NIC의 VF(가상 기능)가 가상 머신에 연결되어 있습니다.

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

(BZ#1348508)

RHEL 8 Hyper-V 가상 머신에서 KVM 가상화 사용 가능

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

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

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

virtualization

(BZ#1519039)

KVM 가상 머신용 AMD SEV

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

단일 호스트에서 이 기능을 한 번에 사용할 수 있는 VM의 개수는 호스트 하드웨어에 의해 결정됩니다. 현재 AMD EPYC 프로세서는 SEV를 사용하여 최대 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 VM에 물리적 GPU를 할당하면 호스트가 GPU를 사용할 수 없으며 호스트의 그래픽 디스플레이 출력이 작동하지 않을 수 있습니다.

(BZ#1528684)

5.5.10. 컨테이너

Skopeo 컨테이너 이미지는 기술 프리뷰로 사용 가능

registry.redhat.io/rhel8/skopeo 컨테이너 이미지는 **skopeo** 패키지의 컨테이너화된 구현입니다. **skopeo** 는 컨테이너 이미지 및 이미지 리포지토리에서 다양한 작업을 수행하는 명령줄 툴 유틸리티입니다. 이 컨테이너 이미지를 사용하면 인증되지 않은 컨테이너 레지스트리에서 다른 컨테이너 레지스트리로 컨테이너 이미지를 검사하고 복사할 수 있습니다.

(BZ#1627900)

Buildah 컨테이너 이미지는 기술 프리뷰로 사용할 수 있습니다.

registry.redhat.io/rhel8/buildah 컨테이너 이미지는 **buildah** 패키지의 컨테이너화된 구현입니다. **buildah** 는 **OCI** 컨테이너 이미지를 쉽게 빌드할 수 있는 툴입니다. 이 컨테이너 이미지를 사용하면 시스템에 **buildah** 패키지를 설치할 필요 없이 컨테이너 이미지를 빌드할 수 있습니다. 사용 사례는 루트가 아닌 사용자로 이 이미지를 **rootless** 모드에서 실행하는 것을 다루지 않습니다.

(BZ#1627898)

5.6. 사용되지 않는 기능

이 부분에서는 **Red Hat Enterprise Linux 8.2**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 있지만 **RHEL 8**에서 *제거된* 기능에 관한 자세한 내용은 **RHEL 8** 채택 고려 사항을 참조하십시오.

5.6.1. 설치 프로그램 및 이미지 생성

몇 가지 **Kickstart** 명령 및 옵션이 더 이상 사용되지 않음

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

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

- ignoredisk --interactive
- 파티션 --active
- reboot --kexec

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

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

(BZ#1642765)

ignoredisk Kickstart 명령의 --interactive 옵션이 더 이상 사용되지 않음

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

(BZ#1637872)

5.6.2. 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)

5.6.3. 쉘 및 명령행 툴

curl에 대한 metalink 지원이 비활성화되었습니다

Metalink를 사용하여 다운로드한 콘텐츠와 자격 증명 및 파일 해시 불일치 처리 방식에 **curl** 기능에서 취약점이 발견되었습니다. 이 취약점으로 인해 호스팅 서버를 제어하는 악의적인 행위자가 다음을 수행할 수 있습니다.

- 악의적인 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)

5.6.4. 보안

NSS SEED 암호가 더 이상 사용되지 않음

Mozilla Network Security Services(NSS) 라이브러리는 향후 릴리스에서 **SEED** 암호를 사용하는 **TLS** 암호화 제품군을 지원하지 않습니다. **SEED** 암호를 사용하는 배포의 경우 **Red Hat**은 다른 암호화 제품군에 대한 지원을 활성화하는 것이 좋습니다. 이렇게 하면 **NSS**에 대한 지원이 제거될 때 원활한 전환을 보장합니다.

SEED 암호는 **RHEL;**에서 기본적으로 비활성화되어 있습니다.

(BZ#1817533)

TLS 1.0 및 **TLS 1.1**이 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 **NSS**에서 더 이상 사용되지 않음

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

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

(BZ#1645153)

TPM 1.2가 더 이상 사용되지 않음

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

(BZ#1657927)

5.6.5. 네트워킹

RHEL 8에서 네트워크 스크립트가 더 이상 사용되지 않음

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

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

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

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

ifup 및 **ifdown** 스크립트는 설치된 레거시 네트워크 스크립트에 연결됩니다.

레거시 네트워크 스크립트를 호출하면 사용 중단을 알리는 경고 메시지가 표시됩니다.

(BZ#1647725)

5.6.6. 커널

디스크리스 부팅을 사용하여 실시간 8용 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)

qla3xxx 드라이버가 더 이상 사용되지 않음

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

(BZ#1658840)

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

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

(BZ#1660627)

The rdma_rxe soft -RoCE 드라이버는 더 이상 사용되지 않습니다.

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

(BZ#1878207)

5.6.7. 파일 시스템 및 스토리지

종료된 커널 명령줄 매개변수는 더 이상 사용되지 않습니다.

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

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

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

자세한 내용은 디스크 스케줄러 설정을 참조하십시오.

(BZ#1665295)

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)

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)

5.6.8. 데스크탑

libgnome-keyring 라이브러리가 더 이상 사용되지 않음

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

(BZ#1607766)

5.6.9. 그래픽 인프라

AGP 그래픽 카드는 더 이상 지원되지 않습니다.

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

(BZ#1569610)

5.6.10. 웹 콘솔

웹 콘솔에서 더 이상 불완전한 번역을 지원하지 않습니다

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

(BZ#1666722)

5.6.11. 가상화

virt-manager가 더 이상 사용되지 않음

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

(JIRA:RHELPLAN-10304)

RHEL 8에서 가상 머신 스냅샷이 올바르게 지원되지 않음

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

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

(BZ#1686057)

Cirrus VGA 가상 GPU 유형이 더 이상 사용되지 않음

향후 **Red Hat Enterprise 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)

cpu64-rhel6 CPU 모델이 더 이상 사용되지 않으며 삭제되었습니다.

cpu64-rhel6 QEMU 가상 **CPU** 모델은 **RHEL 8.1**에서 더 이상 사용되지 않으며 **RHEL 8.2**에서 제거되었습니다. 호스트 시스템의 **CPU**에 따라 **QEMU** 및 **libvirt**에서 제공하는 다른 **CPU** 모델을 사용하는 것이 좋습니다.

(BZ#1741346)

5.6.12. 사용되지 않는 패키지

다음 패키지는 더 이상 사용되지 않으며 향후 **Red Hat Enterprise Linux** 주요 릴리스에 포함되지 않을 수 있습니다.

- **389-ds-base-legacy-tools**
- **authd**
- **custodia**
- 호스트 이름
- **libidn**

- net-tools
- network-scripts
- nss-pam-ldapd
- sendmail
- jp-tools
- ypbind
- ypserv

5.7. 확인된 문제

이 부분에서는 Red Hat Enterprise Linux 8.2에서 알려진 문제에 대해 설명합니다.

5.7.1. 설치 프로그램 및 이미지 생성

auth 및 authconfig Kickstart 명령에는 AppStream 리포지토리가 필요

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

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

(BZ#1640697)

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

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

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

(BZ#1697896)

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

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

(BZ#1696609)

reboot --kexec 명령을 사용하는 경우 설치 실패

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

(BZ#1672405)

RHEL 8 초기 설정은 SSH를 통해 수행할 수 없습니다.

현재 SSH를 사용하여 시스템에 로그인하면 RHEL 8 초기 설정 인터페이스가 표시되지 않습니다. 따라서 SSH를 통해 관리되는 RHEL 8 시스템에서는 초기 설정을 수행할 수 없습니다. 이 문제를 해결하려면 기본 시스템 콘솔(ttyS0)에서 초기 설정을 수행하고 나중에 SSH를 사용하여 로그인합니다.

(BZ#1676439)

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)

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)

바이너리 DVD ISO 이미지를 사용한 GUI 설치는 CDN 등록없이 진행되지 않는 경우가 있습니다.

바이너리 **DVD ISO** 이미지 파일을 사용하여 **GUI** 설치를 수행할 때 설치 프로그램의 경쟁 조건은 **Connect to Red Hat** 기능을 사용하여 시스템을 등록할 때까지 설치 진행을 방지할 수 있습니다. 이 문제를 해결하려면 다음 단계를 완료합니다.

1. **GUI** 설치의 **Installation Summary**(설치 요약) 창에서 **Installation Source** (설치 소스)를 선택합니다.
2. 자동 감지 설치 미디어가 선택되었는지 확인합니다.
3.

Done(완료 **)**을 클릭하여 선택을 확인하고 **Installation Summary(**설치 요약 **)** 창으로 돌아갑니다**.**

4. **Installation Summary (**설치 요약**)** 창에서 **Local Media (**로컬 미디어 **)** 상태가 **Installation Source(** 설치 소스**)**로 표시되는지 확인합니다**.**

결과적으로 **Connect to Red Hat** 기능을 사용하여 시스템을 등록하지 않고 설치를 진행할 수 있습니다**.**

(BZ#1823578)

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

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

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

(BZ#1687747)

Kickstart 설치에는 자체 서명 **HTTPS** 서버를 사용할 수 없습니다**.**

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

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

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

예를 들면 다음과 같습니다**.**

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

(BZ#1745064)

저장소 새로 고침을 완료하기 전에 CDN을 사용하여 등록 해제를 시도하면 GUI 설치에 실패할 수 있습니다.

RHEL 8.2에서는 시스템을 등록하고 CDN(Content Delivery Network)을 사용하여 서브스크립션을 연결할 때 GUI 설치 프로그램에 의해 리포지토리 메타데이터의 새로 고침이 시작됩니다. 새로 고침 프로세스는 등록 및 서브스크립션 프로세스의 일부가 아니며, 결과적으로 Connect to Red Hat 창에서 Unregister 버튼이 활성화됩니다. 네트워크 연결에 따라 새로 고침 프로세스를 완료하는 데 1분 이상이 걸릴 수 있습니다. 새로 고침 프로세스가 완료되기 전에 Unregister 단추를 클릭하면 unregister 프로세스가 CDN 리포지토리 파일과 CDN과 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 italics의 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 GUI를 설치하는 동안 시스템을 안전하게 등록 취소할 수 있습니다.

(BZ#1821192)

5.7.2. 서브스크립션 관리

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

Red Hat Enterprise Linux 8에서는 syspurpose 명령줄 툴의 4가지 속성(role,usage, service_level_agreement, addons)이 추가되었습니다. 현재는 role,usage 및 service_level_agreement 만

subscription-manager attach --auto 명령을 실행하는 출력에 영향을 미칩니다. **addons** 인수에 값을 설정하려는 사용자는 자동 연결된 서브스크립션에 어떤 영향을 미치지 않습니다.

(BZ#1687900)

Kickstart 파일을 사용하여 **RHEL**을 설치할 때 다중 경로 스토리지 장치의 데이터가 손실됩니다.

Kickstart 파일을 사용하여 **RHEL**을 설치할 때 호스트에 연결된 다중 경로 스토리지 장치의 데이터는 손실됩니다. 이 문제는 설치 프로그램이 **ignoredisk --drives** 명령을 사용하여 지정한 다중 경로 스토리지 장치를 무시하지 못하기 때문에 발생합니다. 따라서 장치의 데이터가 손실됩니다.

이 문제를 해결하려면 설치 전에 장치를 분리하거나 **ignoredisk --only-use** 명령을 사용하여 설치할 장치를 지정합니다.

(BZ#1862131)

5.7.3. 쉘 및 명령행 툴

Wayland 프로토콜을 사용하는 애플리케이션은 원격 디스플레이 서버로 전달할 수 없습니다.

Red Hat Enterprise Linux 8에서 대부분의 애플리케이션은 기본적으로 **X11** 프로토콜 대신 **Wayland** 프로토콜을 사용합니다. 결과적으로 **ssh** 서버는 **Wayland** 프로토콜을 사용하는 애플리케이션을 전달할 수 없지만 **X11** 프로토콜을 사용하는 애플리케이션을 원격 디스플레이 서버로 전달할 수 있습니다.

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

(BZ#1686892)

systemd-resolved.service 가 부팅 시 시작되지 않음

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

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

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

(BZ#1640802)

5.7.4. 보안

symlink의 감사 실행 파일이 작동하지 않음

w 옵션이 제공하는 파일 모니터링은 경로를 직접 추적할 수 없습니다. 실행된 프로그램을 비교하려면 장치와 **inode**의 경로를 확인해야 합니다. 실행 가능한 **symlink**를 모니터링하는 감시는 **symlink** 해상도에서 발견되는 메모리에서 실행되는 프로그램이 아닌 **symlink** 자체의 **inode**를 모니터링합니다. 감시에서 **symlink**를 확인하여 결과 실행 프로그램을 가져오더라도 규칙이 다른 **symlink**에서 호출된 **multi-call** 바이너리에 대해 트리거됩니다. 이로 인해 잘못된 양의 로그가 급증하게 됩니다. 결과적으로 **symlink**의 감사 실행 파일 감시가 작동하지 않습니다.

이 문제를 해결하려면 프로그램 실행 파일의 해결 경로를 감시하고 **comm=** 또는 **proctitle=** 필드에 나열된 마지막 구성 요소를 사용하여 결과 로그 메시지를 필터링합니다.

(BZ#1846345)

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

/etc/selinux/config 에서 **SELINUX=disabled** 옵션을 사용하여 **SELinux**를 비활성화하면 커널이 **SELinux**가 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 **SELinux**를 비활성화합니다.

(JIRA:RHELPLAN-34199)

libselinux-python 은 모듈을 통해서만 사용할 수 있습니다

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

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

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

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

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

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

(BZ#1666328)

udica 는 **--env container=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)

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

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

이 문제를 해결하려면 다음을 수행합니다.

1. **umount /sys/fs/selinux/** 명령을 입력합니다.
2. 누락된 **selinux-policy-targeted** 패키지를 수동으로 설치합니다.

3. 정책이 **SELINUX=enforcing** 과 같도록 **/etc/selinux/config** 파일을 편집합니다.

4. **load_policy -i** 명령을 입력합니다.

결과적으로 **SELinux**가 활성화되어 이전과 동일한 정책을 실행합니다.

(BZ#1641631)

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

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

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

(BZ#1746398)

SELinux는 **auditd** 가 시스템을 중단하거나 전원을 끄지 않도록 방지합니다.

SELinux 정책에는 감사 데몬이 **power_unit_file_t systemd** 장치를 시작할 수 있는 규칙이 포함되어 있지 않습니다. 결과적으로 **auditd** 는 로깅 디스크 파티션에 남은 공간 없음과 같은 경우 이를 수행하도록 구성된 경우에도 시스템을 중지하거나 전원을 끌 수 없습니다.

이 문제를 해결하려면 사용자 지정 **SELinux** 정책 모듈을 만듭니다. 결과적으로, **auditd** 는 해결 방법을 적용하는 경우에만 시스템을 올바르게 중지하거나 전원을 끌 수 있습니다.

(BZ#1826788)

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)

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)

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

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

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

(BZ#1659383)

특정 **rsyslog** 우선 순위 문자열이 올바르게 작동하지 않음

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

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

이 문제를 해결하려면 우선 순위 문자열이 올바르게 작동하는 경우에만 사용하십시오.

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

따라서 현재 구성을 올바르게 작동하는 문자열로 제한해야 합니다.

(BZ#1679512)

SHA-1 서명이 있는 서버에 대한 연결이 **GnuTLS**에서 작동하지 않음

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

(BZ#1628553)

TLS 1.3이 **FIPS** 모드에서 **NSS**에서 작동하지 않음

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

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

(BZ#1724250)

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

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

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

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

따라서 설명된 시나리오에서 TLS 연결을 설정할 수 있습니다.

(BZ#1685470)

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

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

(BZ#1749068)

ssh-keyscan 은 FIPS 모드에서 RSA 키를 검색할 수 없습니다

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

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

(BZ#1744108)

Libreswan 이 모든 설정에서 seccomp=enabled 에서 제대로 작동하지 않음

현재 Libreswan SECCOMP 지원 구현에서 허용되는 syscall 세트가 완료되지 않았습니다. 결과적으로 ipsec.conf 파일에서 SECCOMP를 활성화하면 syscall 필터링이 pluto 데몬이 제대로 작동하는 데 필요한 syscall도 거부합니다. 데몬이 종료되고 ipsec 서비스가 다시 시작됩니다.

이 문제를 해결하려면 seccomp= 옵션을 다시 disabled 상태로 설정합니다. ipsec 을 올바르게 실행하려면 SECCOMP 지원이 비활성화되어 있어야 합니다.

(BZ#1777474)

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)

SCAP Workbench가 사용자 정의 프로파일에서 결과를 기반으로 한 수정을 생성하지 못함

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

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

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

(BZ#1640715)

킥스타트에서는 **RHEL 8**에서 **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 7**과 이전 버전과의 호환성을 유지하기 위해 수행됩니다.

(BZ#1665082)

OSCAP Anaconda 애드온은 모든 패키지를 텍스트 모드에 설치하지 않음

OSCAP Anaconda Addon 플러그인은 설치가 텍스트 모드에서 실행 중인 경우 시스템 설치 프로그램에서 설치에 대해 선택한 패키지 목록을 수정할 수 없습니다. 결과적으로 **Kickstart**를 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)

Gnutls가 NSS 서버로 현재 세션을 다시 시작하지 못했습니다

TLS(Transport Layer Security) 1.3 세션을 다시 시작할 때 GnuTLS 클라이언트는 60밀리초 동안 서버에 세션 재개 데이터를 보낼 때까지 예상 왕복 시간을 기다립니다. 서버가 이 시간 내에 재사용 데이터를 전송하지 않으면 클라이언트는 현재 세션을 다시 시작하지 않고 새 세션을 만듭니다. 이로 인해 정기적인 세션 협상에 약간의 성능에 영향을 미치는 것을 제외하고는 심각한 부정적인 영향이 발생하지 않습니다.

(BZ#1677754)

oscap-ssh 유틸리티는 --sudo를 사용하여 원격 시스템을 스캔할 때 실패합니다.

oscap-ssh 툴을 --sudo 옵션과 함께 사용하여 원격 시스템을 SCAP(Security Content Automation Protocol) 스캔을 수행할 때 원격 시스템의 oscap 툴은 스캔 결과 파일을 저장하고 파일을 root 사용자로 임시 디렉터리에 보고합니다. 원격 시스템의 umask 설정이 변경되면 oscap-ssh 가 해당 파일에 액세스하지 못할 수 있습니다. 이 문제를 해결하려면 이 솔루션 "oscap -ssh --sudo"에 설명된 대로 oscap -ssh 툴을 수정하십시오. "scp: ...: 권한이 거부되었습니다" error. 결과적으로 oscap 은 파일을 대상 사용자로 저장하고 oscap-ssh 는 일반적으로 파일에 액세스합니다.

(BZ#1803116)

OpenSCAP은 YAML 여러 줄 문자열에서 빈 줄을 제거하여 발생하는 오탐을 생성합니다.

OpenSCAP에서 데이터 스트림에서 Ansible 해결을 생성하면 YAML 다중 줄 문자열에서 빈 행을 제거합니다. 일부 Ansible 수정에는 리터럴 구성 파일 내용이 포함되어 있으므로 빈 행을 제거하면 해당 수정 사항에 영향을 미칩니다. 이로 인해 openscap 유틸리티가 빈 줄에 영향을 미치지 않더라도 해당 OVAL(Open Vulnerability and Assessment Language) 검사에 실패합니다. 이 문제를 해결하려면 규칙 설명을 확인하고 빈 줄이 누락되어 실패한 스캔 결과를 건너뜁니다. 또는 Bash 수정으로 인해 잘못된 긍정적인 결과가 생성되지 않으므로 Ansible 해결 대신 Bash 수정을 사용하십시오.

(BZ#1795563)

OSPP 기반 프로필은 GUI 패키지 그룹과 호환되지 않습니다.

GUI 패키지 그룹과 함께 서버에서 설치한 GNOME 패키지에는 OSPP(Operating System Protection Profile)와 호환되지 않는 nfs-utils 패키지가 필요합니다. 결과적으로 OSPP 또는 OSPP 기반 프로필(예: STIG(Security Technical Implementation Guide))을 사용하여 시스템을 설치하는 동안 *GUI* 패키지 그룹이 포함된 서버를 선택하면 설치가 중단됩니다. OSPP 기반 프로필이 설치 후 적용되는 경우 시스템을 부팅할 수 없습니다. 이 문제를 해결하려면 *GUI* 패키지 그룹이나 OSPP 프로파일과 OSPP 기반 프로필을 사용할 때 GUI를 설치하는 다른 그룹을 사용하여 서버를 설치하지 마십시오. 대신 *Server* 또는 *Minimal Install* 패키지 그룹을 사용하는 경우 시스템이 문제 없이 설치되고 올바르게 작동합니다.

(BZ#1787156)

GUI 패키지 그룹이 포함된 RHEL 8 시스템은 e8 프로파일을 사용하여 수정할 수 없습니다.

OpenSCAP Anaconda 애드온을 사용하여 *Verify Integrity with RPM(RPM 그룹과 무결성 확인)에서 규칙을 선택하는 프로필이 있는 GUI 패키지 그룹과 함께* 서버에서 시스템을 강화하려면 시스템의 RAM 크기가 극도로 필요합니다. 이 문제는 OpenSCAP 스캐너로 인해 발생합니다. 자세한 내용은 OpenSCAP로 많은 파일 스캔을 통해 시스템에 메모리가 부족하게 됩니다. 결과적으로 RHEL8 Essential Eight(e8) 프로필을 사용하여 시스템 강화에 성공하지 못했습니다. 이 문제를 해결하려면 더 작은 패키지 그룹(예: Server)을 선택하고 설치 후 필요한 추가 패키지를 설치합니다. 결과적으로 시스템에 더 적은 수의 패키지가 생기므로 검사에 메모리가 적게 필요하므로 시스템을 자동으로 강화할 수 있습니다.

(BZ#1816199)

OpenSCAP로 많은 수의 파일을 스캔하면 시스템에 메모리가 부족합니다.

OpenSCAP 스캐너는 검사가 완료될 때까지 수집된 모든 결과를 메모리에 저장합니다. 그 결과 시스템에는 많은 수의 파일을 스캔할 때 RAM이 적은 시스템에서 메모리가 부족할 수 있습니다(예: *GUI 및 워크스테이션 을 사용한* 대규모 패키지 그룹). 이 문제를 해결하려면 더 작은 패키지 그룹(예: RAM이 제한된 시스템에 *Server* 및 *Minimal Install*)을 사용하십시오. 대규모 패키지 그룹을 사용해야 하는 경우 시스템에 가상 또는 스테이징 환경에서 메모리가 충분한지 테스트할 수 있습니다. 또는 전체 / 파일 시스템에 대한 재귀가 필요한 규칙을 선택 취소하도록 검사 프로필을 조정할 수 있습니다.

- rpm_verify_hashes
- rpm_verify_permissions
- rpm_verify_ownership
- file_permissions_unauthorized_world_writable
- no_files_unowned_by_user
- dir_perms_world_writable_system_owned
- file_permissions_unauthorized_suid
- file_permissions_unauthorized_sgid
- file_permissions_ungroupowned
- dir_perms_world_writable_sticky_bits

이렇게 하면 OpenSCAP 스캔으로 인해 시스템에 메모리가 부족해지는 것을 방지할 수 있습니다.

(BZ#1824152)

5.7.5. 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 GRO가 비활성화되면 IPsec 네트워크 트래픽이 실패합니다.

이 문제를 해결하려면 장치에서 **GRO**를 사용하도록 유지합니다.

(BZ#1649647)

iptables 는 지정된 체인 유형을 알 수 없는 경우 체인을 업데이트하는 명령에 대한 모듈 로드를 요청하지 않습니다.

참고: 이 문제로 인해 서비스 기본 구성을 사용하는 경우 **iptables systemd** 서비스를 중지할 때 기능이 작동하지 않는 잘못된 오류가 발생합니다.

iptables-nft 를 사용하여 체인의 정책을 설정할 때 관련 커널 모듈이 아직 로드되지 않은 경우 커널에 전송된 결과 **update chain** 명령이 실패합니다. 이 문제를 해결하려면 다음 명령을 사용하여 모듈이 로드되도록 합니다.

+

```
# iptables -t nat -n -L
# iptables -t mangle -n -L
```

(BZ#1812666)

nft_compat 모듈로 주소 제품군별 **LOG** 백엔드 모듈 자동 로드가 중단될 수 있습니다.

네트워크 네임스페이스(**netns**)에서의 작업이 병렬로 수행되는 동안 **nft_compat** 모듈이 제품군별 **LOG** 대상 백엔드를 로드하면 잠금 충돌이 발생할 수 있습니다. 결과적으로 주소 제품군별 **LOG** 대상 백엔드를 로드하는 것이 중단될 수 있습니다. 이 문제를 해결하려면 **iptables-restore** 유틸리티를 실행하기 전에 관련 **LOG** 대상 백엔드(예: **as nf_log_ipv4.ko** 및 **nf_log_ipv6.ko**)를 수동으로 로드합니다. 결과적으로 **LOG** 대상 백엔드를 로드해도 중단되지 않습니다. 그러나 시스템 부팅 중에 문제가 발생하면 해결 방법을 사용할 수 없습니다.

libvirtd 와 같은 다른 서비스도 **iptables** 명령을 실행하여 문제가 발생할 수 있습니다.

(BZ#1757933)

5.7.6. 커널

실수로 패치 제거로 인해 **huge_page_setup_helper.py** 가 오류가 표시됨

huge_page_setup_helper.py 스크립트를 업데이트하는 패치가 실수로 제거되었습니다. 결과적으로 **huge_page_setup_helper.py** 스크립트를 실행하면 다음과 같은 오류 메시지가 표시됩니다.

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

이 문제를 해결하려면 **RHEL 8.1**에서 **huge_page_setup_helper.py** 스크립트를 복사하여 **/usr/bin/** 디렉토리에 설치합니다.

1. **RHEL-8 .1.0** 설치 미디어 또는 **Red Hat** 고객 포털에서 **libhugetlbfs-utils-2.21-3.el8.x86_64.rpm** 패키지를 다운로드합니다.

2. **rpm2cpio** 명령을 실행합니다.

```
# rpm2cpio libhugetlbfs-utils-2.21-3.el8.x86_64.rpm | cpio -D / -iduv
'*/huge_page_setup_helper.py'
```

명령은 **RHEL 8.1 RPM**에서 **huge_page_setup_helper.py** 스크립트를 추출하여 **/usr/bin/** 디렉터리에 저장합니다.

결과적으로 **huge_page_setup_helper.py** 스크립트가 올바르게 작동합니다.

(BZ#1823398)

부팅 프로세스 중 많은 양의 영구 메모리 경험이 있는 시스템

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

(BZ#1666538)

KSM이 **NUMA** 메모리 정책을 무시하는 경우가 있음

merge_across_nodes=1 매개 변수를 사용하여 **KSM**(커널 공유 메모리) 기능을 활성화하면 **KSM**은 **mbind()** 함수에서 설정한 메모리 정책을 무시하고 일부 메모리 영역의 페이지를 정책과 일치하지 않는

NUMA(Non-Uniform Memory Access) 노드에 병합할 수 있습니다.

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

(BZ#1153521)

RHEL 8의 크래시 캡처 환경에서 커널을 부팅하지 못했습니다.

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

(BZ#1659609)

zlib 일부 압축 함수에서 vmcore 캡처 속도가 느려질 수 있습니다.

kdump 구성 파일은 기본적으로 lzo 압축 형식(makedumpfile -l)을 사용합니다. zlib 압축 형식(makedumpfile -c)을 사용하여 구성 파일을 수정할 때 vmcore 캡처 프로세스의 속도를 저하시키는 대신 압축 요인이 향상될 수 있습니다. 그 결과 lzo 에 비해 kdump 가 zlib 를 사용하여 vmcore 를 캡처하는 데 최대 4배 더 걸립니다.

따라서 속도가 주요 추진 요인인 경우에는 기본 lzo 를 사용하는 것이 좋습니다. 그러나 대상 시스템이 사용 가능한 공간이 부족한 경우 zlib 가 더 나은 옵션입니다.

(BZ#1790635)

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)

fadump 덤프 메커니즘은 네트워크 인터페이스의 이름을 **kdump-<interface-name>**으로 변경합니다.

펌웨어 지원 덤프(**fadump**)를 사용하여 **vmcore** 를 캡처하고 **SSH** 또는 **NFS** 프로토콜을 사용하여 원격 머신에 저장하는 경우 네트워크 인터페이스의 이름을 **kdump-<interface-name>** 으로 변경합니다. **<interface-name>** 이 일반인 경우 이름 변경이 발생합니다(예: ***eth#** 또는 **net#** 등). 이 문제는 초기 **RAM** 디스크(**initrd**)의 **vmcore** 캡처 스크립트를 네트워크 인터페이스 이름에 **kdump-** 접두사를 추가하여 영구적인 명명을 보안하기 때문에 발생합니다. 동일한 **initrd** 도 일반 부팅에 사용되므로 프로덕션 커널의 인터페이스 이름도 변경됩니다.

(BZ#1745507)

fadump 가 활성화된 경우 부팅 시 시스템이 긴급 모드로 전환됩니다.

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

(BZ#1750278)

irqpoll 을 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 파일의 KDUMP_COMMANDLINE_REMOVE 키에 irqpoll 을 추가합니다.

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

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

kdump 서비스는 상당한 양의 크래시 커널 메모리를 사용하여 vmcore 파일을 덤프할 수 있습니다. 캡처 커널에 kdump 서비스에 사용할 수 있는 메모리가 충분한지 확인합니다.

(BZ#1654962)

vPMEM 메모리를 덤프 대상으로 사용하면 커널 크래시 캡처 프로세스가 지연됩니다.

vPEM(가상 영구 메모리) 네임스페이스를 kdump 또는 fadump 대상으로 사용하는 경우 papr_scm 모듈은 vPMEM에서 지원하는 메모리를 매핑하고 다시 매핑하고 메모리를 선형 맵에 다시 추가해야 합니다. 결과적으로 이 동작으로 인해 하이퍼바이저 호출(HCalls)이 POWER Hypervisor로 트리거되고 총 시간이 걸리기 때문에 캡처 커널 부팅 속도가 상당히 느립니다. 따라서 vPMEM 네임스페이스를 kdump 또는 fadump의 덤프 대상으로 사용하지 않는 것이 좋습니다.

vPMEM을 사용해야 하는 경우 이 문제를 해결하려면 다음 명령을 실행합니다.

1. /etc/dracut.conf.d/99-pmem-workaround.conf 파일을 만들고 다음을 추가합니다.

```
add_drivers+="nd_pmem nd_btt libnvdimm papr_scm"
```

2. 초기 RAM 디스크(initrd) 파일 시스템을 다시 빌드합니다.

```
# touch /etc/kdump.conf
# systemctl restart kdump.service
```

(BZ#1792125)

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 **NMI**는 다음 두 가지 조건 중 하나로 시작됩니다.

1. **iLO(Integrated Lights-Out)** 서버 관리 소프트웨어에서 **Generate NMI** 버튼. 이 버튼은 사용자가 트리거합니다.

2. **hpwdt watchdog.** 만료는 기본적으로 서버로 **NMI**를 보냅니다.

두 시퀀스 모두 시스템이 응답하지 않는 경우 일반적으로 발생합니다. 정상적인 상황에서 이러한 두 상황에 대한 **NMI** 핸들러는 커널 **panic()** 함수를 호출하고 구성된 경우 **kdump** 서비스에서 **vmcore** 파일을 생성합니다.

그러나 누락된 **NMI**로 인해 **kernel panic()** 은 호출되지 않으며 **vmcore** 는 수집되지 않습니다.

첫 번째 사례(1.)에서 시스템이 응답하지 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)

cxgb4 드라이버로 인해 **kdump** 커널에서 충돌이 발생합니다.

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

(BZ#1708456)

모드 **5(밸런싱-tlb)** 본딩 마스터 인터페이스에 **ICE** 드라이버 **NIC** 포트를 추가하려고 하면 실패할 수 있습니다.

모드 **5(balance-tlb)** 본딩 마스터 인터페이스에 **ICE** 드라이버 **NIC** 포트를 추가하려고 하면 **Master 'bond0', Slave 'ens1f0'** 오류가 발생할 수 있습니다. 오류: **enslave failed.** 결과적으로 **NIC** 포트를 본딩 마스터 인터페이스에 추가하는 간헐적인 오류가 발생합니다. 이 문제를 해결하려면 인터페이스 추가를 다시 시도합니다.

(BZ#1791664)

인터페이스 **type='hostdev'**를 사용하여 가상 머신을 가상 머신에 연결하는 데 실패할 수 있습니다.

<interface type='hostdev'> 메서드를 사용하여 할당 후 **.XML** 파일을 사용하여 가상 머신에 **VF**(가상 기능)를 연결하는 데 실패할 수 있습니다. 이러한 문제는 **Assignment with <interface type='hostdev'>** 메서드를 사용하면 **VM**이 이 가상 머신에 표시되는 **VF NIC**에 연결할 수 없기 때문입니다. 이 문제를 해결하려면 **Assignment with <hostdev>** 메서드를 사용하여 **.XML** 파일을 사용하여 **VM**에 **VF**를 연결합니다. 결과적으로 **virsh attach-device** 명령이 오류 없이 성공합니다. **Assignment with <hostdev>** 및 **Assignment with < interface type='hostdev'> (SRIOV** 장치만 해당)의 차이점에 대한 자세한 내용은 호스트 네트워크 장치의 **PCI** 통과를 참조하십시오.

(BZ#1792691)

5.7.7. 파일 시스템 및 스토리지

/boot 파일 시스템을 **LVM**에 배치할 수 없습니다.

LVM 논리 볼륨에 **/boot** 파일 시스템을 배치할 수 없습니다. 이 제한은 다음과 같은 이유로 존재합니다.

- EFI 시스템에서 *EFI 시스템 파티션* 은 일반적으로 /boot 파일 시스템 역할을 합니다. uEFI 표준에는 이 파티션에 대한 특정 GPT 파티션 유형과 특정 파일 시스템 유형이 필요합니다.

- RHEL 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)

너무 많은 LUN이 연결되어 있을 때 DM Multipath를 시작하지 못할 수 있습니다.

multipathd 서비스는 시간이 초과될 수 있으며 너무 많은 LUN(논리 단위)이 시스템에 연결되어 있으면 시작되지 않을 수 있습니다. 문제를 유발하는 정확한 LUN 수는 장치 수, 스토리지 어레이의 응답 시간, 메모리 및 CPU 구성, 시스템 로드 등 여러 요인에 따라 달라집니다.

이 문제를 해결하려면 multipathd 유닛 파일에서 시간 초과 값을 늘립니다.

1. 장치 편집기에서 **multipathd** 유닛을 엽니다.

```
# systemctl edit multipathd
```

2. 시간 초과 값을 덮어쓰려면 다음 구성을 입력합니다.

```
[Service]
TimeoutSec=300
```

Red Hat은 기본 **90**에서 **300**으로 값을 늘리는 것을 권장하지만 **90** 이상의 다른 값을 테스트할 수도 있습니다.

3. 파일을 편집기에 저장합니다.

4. **systemd** 장치를 다시 로드하여 변경 사항을 적용합니다.

```
# systemctl daemon-reload
```

결과적으로 이제 다수의 **LUN**으로 **multipathd** 가 성공적으로 시작될 수 있습니다.

(BZ#1797660)

LVM writecache의 제한 사항

writecache LVM 캐싱 방법에는 캐시 방법에 없는 다음과 같은 제한 사항이 있습니다.

- 논리 볼륨이 **writecache** 를 사용하는 동안 논리 볼륨의 스냅샷을 만들 수 없습니다.
- 논리 볼륨이 활성화된 동안 **writecache** 를 연결하거나 분리할 수 없습니다.
- 비활성 논리 볼륨에 **writecache** 를 연결할 때 기존 파일 시스템 블록 크기와 일치하는 **writecache** 블록 크기를 사용해야 합니다.

자세한 내용은 **lvmcache(7)** 도움말 페이지를 참조하십시오.

- **writecache** 가 연결된 동안 논리 볼륨의 크기를 조정할 수 없습니다.
- **writecache** 와 함께 사용되는 장치에는 **pvmove** 명령을 사용할 수 없습니다.
- 씬 풀 또는 **VDO**와 함께 **writecache** 가 있는 논리 볼륨을 사용할 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)

5.7.8. 동적 프로그래밍 언어, 웹 서버 및 데이터베이스 서버

getpwnam() 은 32비트 애플리케이션에 의해 호출될 때 실패할 수 있습니다.

NIS 사용자가 **getpwnam()** 함수를 호출하는 32비트 애플리케이션을 사용하는 경우 **nss_nis.i686** 패키지가 누락된 경우 호출이 실패합니다. 이 문제를 해결하려면 **yum install nss_nis.i686** 명령을 사용하여 누락된 패키지를 수동으로 설치합니다.

(BZ#1803161)

Nginx 는 하드웨어 보안 토큰에서 서버 인증서를 로드할 수 없습니다.

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

(BZ#1668717)

php- opcache가 **PHP 7.2**와 함께 설치되면 **PHP- fpm** 으로 **SELinux AVC**가 거부됩니다.

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

```
opcache.huge_code_pages=0
```

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

(BZ#1670386)

종속성으로 설치할 때 **mod_wsgi** 패키지 이름이 누락되었습니다.

BZ#1779705 에 설명된 **mod_wsgi** 설치의 변경으로 **python3-mod_wsgi** 패키지는 더 이상 **mod_wsgi** 라는 이름을 제공하지 않습니다. **mod_wsgi** 모듈을 설치할 때 전체 패키지 이름을 지정해야 합니다. 이러한 변경으로 인해 타사 패키지의 종속성에 문제가 있습니다.

mod_wsgi 라는 종속성이 필요한 타사 패키지를 설치하려고 하면 다음과 유사한 오류가 반환됩니다.

```
Error:
 Problem: conflicting requests
  - nothing provides mod_wsgi needed by package-requires-mod_wsgi.el8.noarch
```

이 문제를 해결하려면 다음 중 하나를 선택하십시오.

a. 전체 패키지 이름 **python3-mod_wsgi** 를 요구하도록 패키지를 다시 빌드하거나 타사 벤더에게 새 빌드를 요청합니다.

b. 누락된 패키지 이름으로 메타 패키지를 생성합니다.

1. 이름이 **mod_wsgi** 인 고유한 빈 메타 패키지를 빌드합니다.
2. **meta** 패키지가 포함된 리포지토리의 **.repo** 구성 파일에 **module_hotfixes=True** 행을 추가합니다.
3. **python3-mod_wsgi** 를 수동으로 설치합니다.

(BZ#1829692)

5.7.9. 컴파일러 및 개발 도구

GCC에서 생성된 합성 함수가 SystemTap에 혼란 가중

GCC 최적화는 다른 함수의 부분 인라인 사본에 대해 합성 함수를 생성할 수 있습니다. **SystemTap** 및 **GDB**와 같은 도구는 이러한 온도 함수를 실제 함수와 구분할 수 없습니다. 결과적으로 **SystemTap**은 온도 및 실제 함수 진입점 모두에 프로브를 배치하므로 단일 실제 함수 호출에 대해 여러 개의 프로브 적중을 등록합니다.

이 문제를 해결하려면 **SystemTap** 스크립트를 수정하여 재귀를 감지하고 인라인 부분 함수와 관련된 프로브 배치를 방지합니다.

예제 스크립트

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

다음과 같은 방식으로 수정할 수 있습니다.

```
global in_can_nice%

probe kernel.function("can_nice").call {
  in_can_nice[tid()] ++;
  if (in_can_nice[tid()] > 1) { next }
  /* code for real probe handler */
}

probe kernel.function("can_nice").return {
  in_can_nice[tid()] --;
}
```

이 예제 스크립트는 **kprobes** 또는 **kretprobes** 누락 또는 의도된 재귀와 같은 가능한 모든 시나리오를 고려하지 않습니다.

(BZ#1169184)

5.7.10. IdM (Identity Management)

/etc/nsswitch.conf 를 변경하려면 수동 시스템 재부팅이 필요합니다

/etc/nsswitch.conf 파일을 변경하는 경우, 예를 들어 **authselect select profile_id** 명령을 실행하려면 모든 관련 프로세스에서 업데이트된 **/etc/nsswitch.conf** 파일을 사용하도록 시스템을 재부팅해야 합니다. 시스템 재부팅이 불가능한 경우 시스템을 **Active Directory(System Security Services Daemon)** 또는 **winbind** 에 조인하는 서비스를 다시 시작합니다.

(BZ#1657295)

파일 도메인이 활성화된 경우 **SSSD**에서 로컬 사용자에 대해 잘못된 **LDAP** 그룹 멤버십을 반환합니다.

SSSD(System Security Services Daemon)에서 로컬 파일 및 **sssd.conf** 파일의 **[domain/LDAP]** 섹션에 있는 **ldap_rfc2307_fallback_to_local_users** 속성에서 사용자를 제공하는 경우 파일 프로바이더에는 다른 도메인의 그룹 멤버십이 포함되지 않습니다. 그 결과 로컬 사용자가 **LDAP** 그룹의 멤버인 경우 **id local_user** 명령은 사용자의 **LDAP** 그룹 멤버십을 반환하지 않습니다. 이 문제를 해결하려면 암시적 파일 도메인을 추가하여 비활성화하십시오.

```
enable_files_domain=False
```

/etc/ sssd/sssd.conf 파일의 **[sssd]** 섹션에 추가합니다.

그 결과 **id local_user** 는 로컬 사용자에 대해 올바른 **LDAP** 그룹 멤버십을 반환합니다.

(BZ#1652562)

SSSD가 동일한 우선 순위로 여러 인증서 일치 규칙을 올바르게 처리하지 않음

지정된 인증서가 여러 인증서 일치 규칙과 동일한 우선 순위의 규칙과 일치하면 **SSSD(System Security Services Daemon)**는 규칙 중 하나만 사용합니다. 이 문제를 해결하려면 **LDAP** 필터가 | (또는) 운영자와 연결된 개별 규칙의 필터로 구성된 단일 인증서 일치 규칙을 사용합니다. 인증서 일치 규칙의 예는 **sss-certamp(5)** 도움말 페이지를 참조하십시오.

(BZ#1447945)

여러 도메인을 정의할 때 **auto_private_group = hybrid**로 프라이빗 그룹을 만들 수 없습니다.

여러 도메인이 정의되어 있고 첫 번째 도메인이 아닌 다른 도메인에서 하이브리드 옵션을 사용하는 경우 **auto_private_group =** 하이브리드 옵션을 사용하여 프라이빗 그룹을 만들 수 없습니다. 암시적 파일 도메인이 **sssd.conf** 파일의 **AD** 또는 **LDAP** 도메인과 함께 정의되어 있고 **MPG_HYBRID** 로 표시되지 않는 경우 **SSSD**는 **uid=gid**를 가진 사용자의 개인 그룹을 생성하지 못하고 이 **gid**가 있는 그룹이 **AD** 또는 **LDAP**에 존재하지 않습니다.

sssd_nss 응답자는 첫 번째 도메인에서만 **auto_private_groups** 옵션 값을 확인합니다. 결과적으로 **RHEL 8**의 기본 설정이 포함된 여러 도메인이 구성된 설정에서는 **auto_private_group** 옵션이 적용되지 않습니다.

이 문제를 해결하려면 **sssd. conf** 의 **sssd** 섹션에 **enable_files_domain = false** 를 설정합니다. 결과적으로 **enable_files_domain** 옵션이 **false**로 설정된 경우 **sssd**는 활성 도메인 목록을 시작할 때 **id_provider=files** 가 있는 도메인을 추가하지 않으므로 이 버그가 발생하지 않습니다.

(BZ#1754871)

python-ply 는 **FIPS**와 호환되지 않습니다

python-ply 패키지의 ✓**CC** 모듈은 **MD5** 해싱 알고리즘을 사용하여 **CC** 서명의 지문을 생성합니다. 그러나 **FIPS** 모드에서는 비보안 컨텍스트에서만 허용되는 **MD5** 사용을 차단합니다. 결과적으로 **python-ply**는 **FIPS**와 호환되지 않습니다. **FIPS** 모드의 시스템에서 **ply.yacc.yacc()** 에 대한 모든 호출이 실패하고 오류 메시지가 표시됩니다.

```
UnboundLocalError: local variable 'sig' referenced before assignment
```

이 문제는 **python-pycparser** 및 **python-cffi** 의 일부 사용 사례에 영향을 미칩니다. 이 문제를 해결하려면 **/usr/lib/python3.6/site-packages/ply/yacc.py** 파일의 **2966**행을 수정하고 **sig = md5()**를 **sig = md5 (usedforsecurity=False)** 로 바꿉니다. 결과적으로 **FIPS** 모드에서 **python-ply** 를 사용할 수 있습니다.

(BZ#1747490)

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)

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)

검색 필터에서 이러한 속성을 사용하는 경우 **Directory Server**에서 스키마에서 누락된 속성에 대해 경고합니다.

nsslapd-verify-filter-schema 매개변수를 **warn-invalid** 로 설정하면 **Directory Server**에서 스키마에 정의되지 않은 속성으로 검색 작업을 처리하고 경고를 기록합니다. 이 설정을 사용하면 속성이 스키마에 정의되어 있는지 여부에 관계없이 **Directory Server**에서 요청된 속성을 검색 결과에 반환합니다.

향후 **Directory Server** 버전에서는 더 엄격한 검사를 강제 적용하도록 **nsslapd-verify-filter-schema** 의 기본 설정을 변경합니다. 새 기본값은 스키마에서 누락된 속성에 대해 경고하며 요청을 거부하거나 부분적인 결과만 반환합니다.

(BZ#1790259)

ipa-healthcheck-0.4 이전 버전의 ipa-healthcheck가 사용되지 않음

Healthcheck 툴이 ipa- healthcheck 및 ipa-healthcheck- core 의 두 개의 하위 패키지로 나뉩니다. 그러나 ipa-healthcheck-core 하위 패키지만 사용되지 않는 이전 버전의 ipa-healthcheck 로 올바르게 설정됩니다. 결과적으로 Healthcheck 를 업데이트하면 ipa-healthcheck-core 만 설치되고 업데이트 후에도 ipa-healthcheck 명령이 작동하지 않습니다.

이 문제를 해결하려면 yum install ipa-healthcheck-0.4 를 사용하여 수동으로 ipa-healthcheck-0.4 하위 패키지를 설치하십시오.

(BZ#1852244)

5.7.11. 데스크탑

Wayland 세션의 제한 사항

Red Hat Enterprise Linux 8에서는 GNOME 환경과 GDM(GNOME Display Manager)이 이전 주요 RHEL에서 사용된 X11 세션 대신 Wayland 를 기본 세션 유형으로 사용합니다.

다음 기능은 현재 사용할 수 없거나 Wayland 에서 예상대로 작동하지 않습니다 :

- xrandr 과 같은 X11 구성 유틸리티는 해상도, 회전 및 레이아웃 처리에 대한 다양한 접근 방식으로 인해 Wayland 에서 작동하지 않습니다. GNOME 설정을 사용하여 디스플레이 기능을 구성할 수 있습니다.
- 화면 녹화 및 원격 데스크탑에서는 Wayland 에서 포털 API를 지원하는 애플리케이션이 필요합니다. 특정 레거시 애플리케이션은 포털 API를 지원하지 않습니다.
- Wayland 에서는 포인터 접근성을 사용할 수 없습니다.
- 클립보드 관리자는 사용할 수 없습니다.
- Wayland 의 GNOME Shell은 대부분의 레거시 X11 응용 프로그램에서 발행된 키보드 그랩을 무시합니다. /org/gnome/mutter/wayland/xwayland-grab-access-rules GSettings 키를 사

용하여 X11 애플리케이션에서 키보드 그랩을 발행할 수 있습니다. 기본적으로 Wayland 의 GNOME 쉘을 사용하면 다음 응용 프로그램이 키보드 그랩을 실행할 수 있습니다.

- GNOME 박스
- vinagre
- Xephyr
- virt-manager, virt-viewer, and remote-viewer
- vncviewer

- 게스트 VM(가상 시스템) 내의 Wayland 에는 안정성과 성능 문제가 있습니다. VM에서 실행되는 경우 RHEL은 자동으로 X11 세션으로 돌아갑니다.

X11 GNOME 세션을 사용한 RHEL 7 시스템에서 RHEL 8로 업그레이드하는 경우 시스템은 계속 X11 을 사용합니다. 다음 그래픽 드라이버를 사용하는 경우 시스템에서 X11 로 자동 대체합니다.

- 독점적 NVIDIA 드라이버
- cirrus 드라이버
- mga 드라이버
- aspeed 드라이버

Wayland 사용을 수동으로 비활성화할 수 있습니다.

- GDM에서 Wayland 를 비활성화하려면 /etc/gdm/custom.conf 파일에 WaylandEnable=false 옵션을 설정합니다.

- GNOME 세션에서 Wayland 를 비활성화하려면 로그인 이름을 입력한 후 로그인 화면의 메뉴로 legacy X11 옵션을 선택합니다.

Wayland에 관한 자세한 내용은 https://wayland.freedesktop.org/를 참조하십시오.

(BZ#1797409)

드래그 앤 드롭이 데스크탑과 응용 프로그램 간에 작동하지 않음

gnome-shell-extensions 패키지의 버그로 인해 현재 드래그 앤 드롭 기능이 데스크탑과 애플리케이션 간에 작동하지 않습니다. 이 기능에 대한 지원은 향후 릴리스에서 다시 추가될 예정입니다.

(BZ#1717947)

소프트웨어 리포지토리에서 flatpak 리포지토리를 비활성화할 수 없습니다.

현재 GNOME 소프트웨어 유틸리티의 Software Repositories(소프트웨어 리포지토리) 도구에서 flatpak 리포지토리를 비활성화하거나 제거할 수 없습니다.

(BZ#1668760)

Generation 2 RHEL 8 가상 머신이 Hyper-V Server 2016 호스트에서 부팅되지 않는 경우가 있습니다.

Microsoft Hyper-V Server 2016 호스트에서 실행되는 VM(가상 머신)에서 RHEL 8을 게스트 운영 체제로 사용하는 경우, 경우에 따라 VM이 부팅되지 않고 GRUB 부팅 메뉴로 돌아갑니다. 또한 Hyper-V 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)

시스템 충돌로 인해 fadump 설정이 손실될 수 있습니다.

이 문제는 펌웨어 지원 덤프(fadump)가 활성화된 시스템에서 확인되며 부팅 파티션은 XFS와 같은 저널링 파일 시스템에 있습니다. 시스템 충돌로 인해 부트 로더가 덤프 캡처 지원이 활성화되어 있지 않은 이전 initrd 를 로드할 수 있습니다. 결과적으로 시스템이 vmcore 파일을 캡처하지 않아 fadump 구성이 손실됩니다.

이 문제를 해결하려면 다음을 수행합니다.

- /boot 가 별도의 파티션인 경우 다음을 수행하십시오.

  1. kdump 서비스 다시 시작

  2. root 사용자로 다음 명령을 실행하거나 CAP_SYS_ADMIN 권한이 있는 사용자 계정을 사용합니다.

```
# fsfreeze -f
# fsfreeze -u
```

- /boot 가 별도의 파티션이 아닌 경우 시스템을 재부팅합니다.

(BZ#1723501)

5.7.12. 그래픽 인프라

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)

Radeon이 하드웨어를 올바르게 재설정하지 못했습니다

현재 **radeon** 커널 드라이버는 **kexec** 컨텍스트에서 하드웨어를 올바르게 재설정하지 않습니다. 대신, **radeon** 이 종료되어 나머지 **kdump** 서비스가 실패합니다.

이 문제를 해결하려면 **/etc/kdump.conf** 파일에 다음 행을 추가하여 **kdump** 의 **radeon** 을 블랙리스트로 지정합니다.

```
dracut_args --omit-drivers "radeon"
force_rebuild 1
```

시스템과 **kdump** 를 다시 시작합니다. **kdump** 를 시작한 후 **force_rebuild 1** 행이 구성 파일에서 제거될 수 있습니다.

이 시나리오에서는 **kdump** 중에 그래픽을 사용할 수 없지만 **kdump** 가 성공적으로 작동합니다.

(BZ#1694705)

단일 **MST** 토폴로지의 여러 디스플레이의 전원이 켜지지 않을 수 있습니다.

no 독립형 드라이버 와 함께 **NVIDIA rpming GPU**를 사용하는 시스템에서는 **DisplayPort hub**(예: 랩탑 부두)와 함께 여러 모니터가 연결되어 있어 이전 **RHEL** 릴리스에서는 모든 디스플레이가 표시되지 않을 수 있습니다. 이는 시스템이 모든 디스플레이를 지원하는 허브에 대역폭이 충분하지 않다고 잘못 생각하기 때문입니다.

(BZ#1812577)

5.7.13. 웹 콘솔

권한이 없는 사용자는 서브스크립션 페이지에 액세스할 수 있습니다.

관리자가 아닌 사용자가 웹 콘솔의 서브스크립션 페이지로 이동하면 웹 콘솔에 일반 오류 메시지 **Cockpit**에 예기치 않은 내부 오류가 표시되었습니다.

이 문제를 해결하려면 권한 있는 사용자로 웹 콘솔에 로그인하고 **Reuse my password for privileged tasks**(권한 있는 작업에 내 암호 재사용) 확인란을 선택해야 합니다.

(BZ#1674337)

5.7.14. 가상화

Windows Server 2019 호스트의 RHEL 8 가상 머신의 낮은 GUI 디스플레이 성능

Windows Server 2019 호스트에서 그래픽 모드에서 RHEL 8을 게스트 운영 체제로 사용하는 경우 GUI 디스플레이 성능이 낮고 현재 게스트의 콘솔 출력에 연결하는 데 예상보다 훨씬 오래 걸립니다.

이는 Windows 2019 호스트에서 알려진 문제이며 Microsoft가 수정 사항을 보류하고 있습니다. 이 문제를 해결하려면 SSH를 사용하여 게스트에 연결하거나 호스트로 Windows Server 2016을 사용합니다.

(BZ#1706541)

Wayland를 사용하는 가상 머신의 여러 모니터를 QXL에서는 표시할 수 없습니다.

remote-viewer 유틸리티를 사용하여 Wayland 디스플레이 서버를 사용하는 VM(가상 시스템)의 모니터를 두 개 이상 *표시하면 VM이 응답하지 않고 표시* 상태 메시지가 무기한 표시됩니다.

이 문제를 해결하려면 Wayland를 사용하는 VM의 GPU 장치로 qxl 대신 virtio-gpu 를 사용합니다.

(BZ#1642887)

virsh iface-* 명령이 일관되게 작동하지 않음

현재 virsh iface- start 및 virsh iface- destroy와 같은 virsh iface- * 명령은 구성 종속성으로 인해 실패하는 경우가 많습니다. 따라서 호스트 네트워크 연결을 구성하고 관리하는 데 virsh iface-* 명령을 사용하지 않는 것이 좋습니다. 대신 NetworkManager 프로그램과 관련 관리 애플리케이션을 사용합니다.

(BZ#1664592)

RHEL 8 가상 머신은 Witherspoon 호스트에서 부팅할 수 없는 경우가 있습니다.

경우에 따라 DD2.2 또는 DD2.3 CPU를 사용하는 *HPC 호스트(Witherspoon이라고도 함)용 Power9 S922LC* 에서 pseries-rhel7.6.0-sxxm 시스템 유형을 사용하는 RHEL 8 가상 머신(VM)에서 부팅되지 않는 경우가 있습니다.

이러한 VM을 부팅하려고 하면 다음과 같은 오류 메시지가 생성됩니다.

```
qemu-kvm: Requested safe indirect branch capability level not supported by kvm
```

이 문제를 해결하려면 다음과 같이 가상 머신의 **XML** 구성을 구성합니다.

```
<domain type='qemu' xmlns:qemu='http://libvirt.org/schemas/domain/qemu/1.0'>
  <qemu:commandline>
    <qemu:arg value='-machine'/>
    <qemu:arg value='cap-ibs=workaround'/>
  </qemu:commandline>
```

(BZ#1732726, BZ#1751054)

IBM POWER 가상 머신이 빈 **NUMA** 노드에서 제대로 작동하지 않음

현재 **RHEL 8** 호스트에서 실행 중인 **IBM POWER** 가상 머신(**VM**)이 제로메모리(**memory='0'**) 및 제로 **CPU**를 사용하는 **NUMA** 노드로 구성된 경우 **VM**을 시작할 수 없습니다. 따라서 **RHEL 8**에서 빈 **NUMA** 노드에서 **IBM POWER VM**을 사용하지 않는 것이 좋습니다.

(BZ#1651474)

AMD EPYC에서 호스트 패스스루 모드를 사용할 때 **VM**에서 **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 **VM**은 코어당 여러 스레드가 있는 가상 **CPU** 토폴로지를 탐지할 수 없습니다. 이 문제를 해결하려면 호스트 통과 대신 **EPYC CPU** 모델로 **VM**을 부팅합니다.

(BZ#1740002)

RHEL 8.2 VM의 디스크 식별자는 **VM** 재부팅 시 변경될 수 있습니다.

RHEL 8.2를 **Hyper-V** 하이퍼바이저에서 게스트 운영 체제로 사용하는 경우 **VM**(가상 머신)을 **Hyper-V** 하이퍼바이저에서 게스트 운영 체제로 사용하는 경우, **VM**이 재부팅될 때 **VM**의 가상 디스크의 장치 식별자가 변경될 수 있습니다. 예를 들어, 원래 **/dev/sda**로 식별된 디스크는 **/dev/ sdb** 가 될 수 있습니다. 결과적으로 **VM**이 부팅되지 않을 수 있으며 **VM** 디스크를 참조하는 스크립트가 작동을 중지할 수 있습니다.

이 문제를 방지하려면 **VM**의 디스크의 영구 이름을 설정하는 것이 좋습니다. 자세한 내용은 **Microsoft Azure** 설명서를 참조하십시오 . **https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-device-names-problems.**

(BZ#1777283)

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)

RHEL 7-ALT 호스트에서 RHEL 8로 POWER9 게스트 마이그레이션에 실패

현재 POWER9 가상 머신을 RHEL 7-ALT 호스트 시스템에서 RHEL 8로 마이그레이션하는 것은 "마이그레이션 상태: active" 상태로 응답하지 않습니다.

이 문제를 해결하려면 RHEL 7-ALT 호스트에서 THP(투명한 대규모 페이지)를 비활성화하여 마이그레이션을 성공적으로 완료할 수 있습니다.

(BZ#1741436)

5.7.15. 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)

5.7.16. 컨테이너

UDICA는 1.0의 안정적인 스트림을 사용할 것으로 예상되지 않습니다.

컨테이너에 대한 SELinux 정책을 생성하는 도구인 UDICA는 container-tools:1.0 모듈 스트림에서 podman 1.0.x를 통해 실행되는 컨테이너와 호환되지 않습니다.

(JIRA:RHELPLAN-25571)

Podman을 사용한 FIPS 지원에 대한 참고 사항

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

(BZ#1804193)

6장. 국제화

6.1. RED HAT ENTERPRISE LINUX 8 국제 언어

Red Hat Enterprise Linux 8은 사용자의 요구 사항에 따라 다양한 언어의 설치와 언어 변경을 지원합니다.

- **동아시아 언어 - 일본어, 한국어, 중국어 간체, 중국어 번체.**
- **유럽 언어 - 영어, 독일어, 스페인어, 프랑스어, 이탈리아어, 포르투갈어, 러시아어.**

다음 표에는 다양한 주요 언어에 제공되는 글꼴 및 입력 방법이 나열되어 있습니다.

언어	기본 글꼴 (Font Package)	입력 방법
영어	dejavu-sans-fonts	
프랑스어	dejavu-sans-fonts	
독일어	dejavu-sans-fonts	
이탈리아어	dejavu-sans-fonts	
러시아어	dejavu-sans-fonts	
스페인어	dejavu-sans-fonts	
포르투갈어	dejavu-sans-fonts	
중국어 간체	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libpinyin, libpinyin
중국어 번체	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-libzhuyin, libzhuyin
일본어	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	ibus-kkc, libkkc
한국어	google-noto-sans-cjk-ttc-fonts, google-noto-serif-cjk-ttc-fonts	IBus-hangul, libhangu

6.2. RHEL 8 국제화의 주요 변경 사항

RHEL 8에서는 RHEL 7에 비해 국제화에 다음과 같은 변경 사항이 추가되었습니다.

- 유니코드 11 컴퓨팅 업계 표준에 대한 지원이 추가되었습니다.
- 국제화는 여러 패키지로 배포되므로 설치 공간을 더 적게 설치할 수 있습니다. 자세한 내용은 langpacks 사용을 참조하십시오.
- 여러 로케일의 glibc 패키지 업데이트가 이제 CLDR(Common Locale Data Repository)과 동기화됩니다.

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#1715406, BZ#1748016, BZ#1790259, BZ#1748994, BZ#1739718
NetworkManager	BZ#1626348
anaconda	BZ#1747382, BZ#1637472, BZ#1748756, BZ#1649359, BZ#1715303, BZ#1696609, BZ#1672405, BZ#1687747, BZ#1745064, BZ#1659400, BZ#1821192, BZ#1822880, BZ#1823578, BZ#1748281, BZ#1746391
audit	BZ#1757986
authselect	BZ#1657295
bind	BZ#1564443, BZ#1664863, BZ#1704328
binutils	BZ#1777002, BZ#1618748
buildah-container	BZ#1627898
clevis	BZ#1766526, BZ#1564559, BZ#1436780, BZ#1784524
cloud-init	BZ#1641190, BZ#1666961
cockpit-appstream	BZ#1676506
cockpit	BZ#1678465, BZ#1754163, BZ#1666722
container-tools-rhel8-module	BZ#1784267
corosync-qdevice	BZ#1784200
createrepo_c	BZ#1743186
crypto-policies	BZ#1690565, BZ#1660839
device-mapper-multipath	BZ#1797660
dhcp	BZ#1729211

구성 요소	티켓
distribution	BZ#1657927
dnf	BZ#1676891, BZ#1754609
dnsmasq	BZ#1700916
edk2	BZ#1748180
elfutils	BZ#1744992
fapolicyd	BZ#1759895
fence-agents	BZ#1775847
firewalld	BZ#1737045, BZ#1740670, BZ#1733066
freeradius	BZ#1723362
gcc-toolset-9	BZ#1774118
gcc	BZ#1726641, BZ#1698607, BZ#1747157
gdb	BZ#1768593
gdm	BZ#1749960
glibc	BZ#1410154,BZ#1764214,BZ#1749439,BZ#1764235, BZ#1746928,BZ#1777241,BZ#1361965,BZ#1747502,BZ#1764218,BZ#1764238,BZ#1746933,BZ#1747453
gnome-shell-extensions	BZ#1717947
gnome-shell	BZ#1724302
gnome-software	BZ#1668760
gnutls	BZ#1628553, BZ#1677754
go-toolset	BZ#1747150
grafana-pcp	BZ#1685315
grafana	BZ#1725278

구성 요소	티켓
graphviz	BZ#1704875
grub2	BZ#1583445, BZ#1723501
httpd-2.4-module	BZ#1747923
httpd	BZ#1633224
initial-setup	BZ#1676439
ipa	BZ#1665051,BZ#1816784,BZ#1719767,BZ#1777564,BZ#1664719,BZ#1664718
ipcalc	BZ#1638834
java-11-openjdk	BZ#1746875
kernel-rt	BZ#1680161
kernel	BZ#1744397, BZ#1698297, BZ#1687094, BZ#1720227, BZ#1846345, BZ#1635295, BZ#1793389, BZ#1706541, BZ#1666538, BZ#1602962, BZ#1649647, BZ#1153521, BZ#1694705, BZ#1348508, BZ#1748451, BZ#1708456, BZ#1654962, BZ#1609288, BZ#1777283, BZ#1791664, BZ#1792125, BZ#1792691, BZ#1812666, BZ#1812577, BZ#1757933, BZ#1763661, BZ#1780432, BZ#1401552, BZ#1716002, BZ#1593711, BZ#1620349, BZ#1724969, BZ#1714330, BZ#1714486, BZ#1660368, BZ#1524687, BZ#1274406, BZ#1650518, BZ#1636572, BZ#1727369, BZ#1519039, BZ#1627455, BZ#1501618, BZ#1495358, BZ#1633143, BZ#1503672, BZ#1570255, BZ#1696451, BZ#1665295, BZ#1658840, BZ#1660627, BZ#1569610, BZ#1730502
kexec-tools	BZ#1750278, BZ#1690729
kmod-kvdo	BZ#1737639, BZ#1657301
krb5	BZ#1754690
libbpf	BZ#1759154
libdnf	BZ#1697472
libgnome-keyring	BZ#1607766
libndp	BZ#1697595
libpfm	BZ#1731019

구성 요소	티켓
libreswan	BZ#1777474
libselinux-python-2.8-module	BZ#1666328
libvirt	BZ#1749672, BZ#1664592, BZ#1528684
llvm-toolset	BZ#1747139
lorax	BZ#1754711
ltrace	BZ#1655368
lvm2	BZ#1600174, BZ#1496229, BZ#1768536
Make	BZ#1774790
Maven	BZ#1783926
mod_wsgi	BZ#1829692, BZ#1779705
mutter	BZ#1737553
nfs-utils	BZ#1719983, BZ#1592011
nftables	BZ#1778883, BZ#1643192
nginx	BZ#1668717
nmstate	BZ#1674456
nss_nis	BZ#1803161
nss	BZ#1724250, BZ#1817533, BZ#1645153
numactl	BZ#1730738
opencv	BZ#1694647
openscap	BZ#1636431, BZ#1618489, BZ#1646197, BZ#1803116, BZ#1795563, BZ#1824152, BZ#1642373
openssh	BZ#1744108
openssl-pkcs11	BZ#1705505, BZ#1664807, BZ#1745082

구성 요소	티켓
openssl	BZ#1685470, BZ#1749068
oscap-anaconda-addon	BZ#1665082, BZ#1674001, BZ#1691305, BZ#1787156, BZ#1816199
pacemaker	BZ#1712584, BZ#1700104
pam	BZ#1252859, BZ#1537242
pcp	BZ#1723598
pcs	BZ#1631519, BZ#1631514, BZ#1676431, BZ#1442116, BZ#1619620
perl-LDAP	BZ#1663063
php-7.2-module	BZ#1670386
php-pecl-xdebug	BZ#1769857
pki-core	BZ#1698084, BZ#1303254
podman	BZ#1804193, BZ#1645280
policycoreutils	BZ#1563742, BZ#1417455
postfix	BZ#1723950, BZ#1745321
powertop	BZ#1716721
pykickstart	BZ#1637872
python-ply	BZ#1747490
python38-3.8-module	BZ#1747329
qemu-kvm	BZ#1651474, BZ#1740002, BZ#1719687, BZ#1651994, BZ#1741346
교체	BZ#1729501
redhat-release	BZ#1817591
redhat-support-tool	BZ#1802026
rhel-system-roles-sap	BZ#1660832

구성 요소	티켓
rng-tools	BZ#1692435
rpm	BZ#1688849
rsyslog	JIRA:RHELPLAN-10431, BZ#1659383, BZ#1679512, BZ#1740683, BZ#1676559,BZ#1692073,BZ#1692072
rust-toolset	BZ#1776847
s390utils	BZ#1750326
samba	BZ#1754409, JIRA:RHELPLAN-13195
scap-security-guide	BZ#1755447, BZ#1754919, BZ#1750755, BZ#1755194
scap-workbench	BZ#1640715
selinux-policy	BZ#1641631, BZ#1746398, BZ#1826788, BZ#1727887, BZ#1726166, BZ#1726246
setools	BZ#1731519
setroubleshoot-plugins	BZ#1649842
setup	BZ#1730396, BZ#1663556
skopeo-container	BZ#1627900
skopeo	BZ#1810053
sscg	BZ#1717880
sssd	BZ#1669407, BZ#1652562, BZ#1447945, BZ#1754871
subscription-manager	BZ#1674337
sudo	BZ#1786990, BZ#1733961
systemd	BZ#1686892, BZ#1640802
systemtap	BZ#1744989
tpm2-tools	BZ#1725714
tuned	BZ#1738250

구성 요소	티켓
udica	BZ#1763210, BZ#1732704
vdo	BZ#1713749
virt-manager	BZ#1677019
Wayland	BZ#1673073
카나리아 제도	BZ#1734183
xorg-x11-drv-qxl	BZ#1642887
xorg-x11-server	BZ#1698565
zlib	BZ#1659433, BZ#1666798
기타	BZ#1640697, BZ#1659609, BZ#1687900, BZ#1697896, BZ#1797409, BZ#1790635, BZ#1823398, BZ#1745507, BZ#1732726, BZ#1757877, JIRA:RHELPLAN-25571, BZ#1777138, JIRA:RHELPLAN-27987, BZ#1797671, BZ#1780124, JIRA:RHELPLAN-2507, JIRA:RHELPLAN-37713, JIRA:RHELPLAN-37777, BZ#1841170, JIRA:RHELPLAN-13995, BZ#1785248, BZ#1755347, BZ#1784455, BZ#1784456, BZ#1789401, JIRA:RHELPLAN-41384, BZ#1690207, JIRA:RHELPLAN-1212, BZ#1559616, BZ#1812552, JIRA:RHELPLAN-14047, BZ#1769727, JIRA:RHELPLAN-27394, BZ#1642765, JIRA:RHELPLAN-10304, BZ#1646541, BZ#1647725, BZ#1686057, BZ#1748980, BZ#1827628

부록 B. 개정 내역

0.2-8

4월 29일, LRKKKKKKKK (lspackova@redhat.com)

- 더 이상 사용되지 않는 기능 소개가 업데이트되었습니다.
- BZ#1605216 의 고정 오타.
- 손상된 링크가 수정되었습니다.

0.2-7

2021년 12월 23일 목요일, 기니카 -파파산라(lspackova@redhat.com)

- soft-RoCE 드라이버인 rdma_rxe 에 대한 정보가 기술 프리뷰 BZ#1605216 및 더 이상 사용되지 않는 기능 BZ#1878207 (커널)에 추가되었습니다.

0.2-6

2021년 10월 5일 화요일, Lucie Maás¢(lmanasko@redhat.com)

- 더 이상 사용되지 않는 기능 BZ#1999620 (Shells 및 명령줄 툴)이 추가되었습니다.

0.2-5

2021년 8월 19일 목요일, Lucie Maás¢(lmanasko@redhat.com)

- YUM/DNF를 사용한 패키지 관리가 배포 장에 추가되었습니다.

0.2-4

2021년 7월 9일 금요일, Lucie Maásá(lmanasko@redhat.com)

- 업데이트된 JIRA:RHELPLAN-34199 (보안).

0.2-3

2021년 6월 23일 수요일, Lucie Maásá(lmanasko@redhat.com)

- 새 기능 섹션(설치자)을 업데이트했습니다.

0.2-2

2021년 5월 21일 금요일, 메카 -파파산라(lspackova@redhat.com)

- 개요 의 OS 변환에 대한 업데이트된 정보.

0.2-1

2021년 4월 6일 화요일, 메카 -파파산라(lspackova@redhat.com)

- 지원되는 아키텍처 목록 개선.

0.2-0

2021년 3월 11일 목요일, Lucie Maœás¢(lmanasko@redhat.com)

- 새 기능 섹션 업데이트(파일 시스템 및 스토리지).

0.1-9

2021년 2월 25일, 커널카 -파파산라(lspackova@redhat.com)

- 고정 CentOS Linux 이름.

0.1-8

2021년 2월 10일 수요일, Lucie Maásá(lmanasko@redhat.com)

- 알려진 문제(가상화) 추가.

0.1-7

2021년 1월 28일 목요일, Lucie Maás¢(lmanasko@redhat.com)

- 기술 프리뷰 장 업데이트.

0.1-6

2020년 12월 10일, Lenka pa¢á(lspackova@redhat.com)

- 새 기능(ID 관리)에 SSSD의 AD GPO 처리에 대한 정보가 추가되었습니다.

0.1-5

2020년 12월 01일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- fapolicyd (Security)와 관련된 버그 수정을 추가했습니다.
- 알려진 문제(설치자)가 추가되었습니다.

0.1-4

2020년 11월 24일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- 새 기능 섹션(네트워킹)을 업데이트했습니다.

0.1-3

2020년 10월 30일 금요일, Barbka pa¢á(lspackova@redhat.com)

- Repositories(리포지토리) 섹션에 업데이트된 애플리케이션 스트림 설명.

0.1-2

2020년 10월 5일, Lucie Maásá(lmanasko@redhat.com)

- 버그 수정(네트워킹)이 추가되었습니다.

0.1-1

2020년 9월 29일 화요일, 기니카 -파파산라(lspackova@redhat.com)

- RHEL 7.9 릴리스로 내부 업그레이드 경로가 업데이트되었습니다.

0.1-0

2020년 8월 27일 목요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- 버그 수정(Kernel)이 추가되었습니다.

0.0-9

2020년 8월 10일, Lucie Maásá(lmanasko@redhat.com)

- 알려진 문제(ID 관리) 추가.

0.0-8

2020년 7월 21일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- Red Hat Enterprise Linux 8.2.1 릴리스 노트 릴리스.

0.0-7

2020년 7월 16일 목요일, Lucie Maás¢(lmanasko@redhat.com)

- 기술 프리뷰(네트워킹) 추가.

- 새 기능 섹션 업데이트.

0.0-6

2020년 6월 25일, Jaroslav Klech(jklech@redhat.com)

- 커널 매개 변수 장을 평가합니다.
- 장치 드라이버 장에 다양한 개선 사항이 추가되었습니다.

0.0-5

2020년 6월 19일 금요일, Lucie Maásá(lmanasko@redhat.com)

- 알려진 새로운 문제가 추가되었습니다.
- 기타 릴리스 노트에 대한 여러 업데이트.

0.0-4

2020년 6월 4일 목요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- 새 기능 섹션 업데이트.
- 알려진 문제(컨테이너)가 추가되었습니다.

0.0-3

2020년 5월 20일, 종료될 예정인 카나리아파파산라(lspackova@redhat.com)

- 알려진 문제(동적 프로그래밍 언어, 웹 및 데이터베이스 서버) 추가.
- 버그 수정(Compilers 및 개발 툴)을 추가했습니다.

- 기타 릴리스 노트에 대한 여러 업데이트.

0.0-2

2020년 4월 28일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- **Red Hat Enterprise Linux 8.2** 릴리스 노트.

0.0-1

2020년 3월 9일, Jaroslav Klech(jklech@redhat.com)

- 외부 커널 매개 변수 및 새 드라이버에 중요한 변경 사항 제공.

0.0-0

2020년 1월 21일 화요일, Lucie Ma¢ás¢(lmanasko@redhat.com)

- **Red Hat Enterprise Linux 8.2** 베타 릴리스 노트 릴리스.