Red Hat Enterprise Linux 7

7.4 릴리스 노트

Red Hat Enterprise Linux 7.4 릴리스 정보

Last Updated: 2023-07-22

Red Hat Enterprise Linux 7 7.4 릴리스 노트

Red Hat Enterprise Linux 7.4 릴리스 정보

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

법적 공지

초록

릴리스 노트에서는 Red Hat Enterprise Linux 7.4에서 구현된 개선 사항 및 추가 기능에 대한 높은 수준과 이 릴리스의 알려진 문제, 주요 버그 수정, 기술 프리뷰, 사용되지 않는 기능 및 기타 세부 사항을 설명합니다.

차례

머리말

Red Hat Enterprise Linux 마이너 릴리스는 개별 보안, 개선 사항 및 버그 수정 에라타의 집계입니다. *Red Hat Enterprise Linux 7.4 릴리스 노트* 문서에서는 Red Hat Enterprise Linux 7 운영 체제의 주요 변경 사항과 이 마이너 릴리스에서 제공되는 애플리케이션, 알려진 문제 및 현재 사용 중인 모든 기술 프리뷰의 전체 목록을 설명합니다.

다른 버전의 시스템에 비해 Red Hat Enterprise Linux 7의 기능 및 제한사항은 https://access.redhat.com/articles/rhel-limits 에서 확인할 수 있습니다.

이 릴리스와 함께 배포된 패키지는 Red Hat Enterprise Linux 7 패키지 매니페스트에 나열되어 있습니다 . Red Hat Enterprise Linux 6에서 마이그레이션하는 방법에 대한 자세한 내용은 마이그레이션 플래닝 가이드에 설명되어 있습니다.

Red Hat Enterprise Linux 라이프 사이클에 대한 자세한 내용은 https://access.redhat.com/support/policy/updates/errata/ 를 참조하십시오.

1장. 개요

보안

- Red Hat Enterprise Linux 7.4에서는 시스템 관리자가 시스템을 재부팅할 때 암호를 수동으로 입력하지 않고도 베어 메탈 시스템에서 하드 드라이브의 루트 볼륨을 암호화할 수 있는 Network Bound Disk Encryption(NBDE) 지원을 제공합니다.

- **USBGuard** 소프트웨어 프레임워크는 장치 속성을 기반으로 기본 화이트리스트 및 블랙리스트 기능을 구현하여 침입형 USB 장치에 대한 시스템 보호 기능을 제공합니다.

- **OpenSSH** 라이브러리 업데이트에는 SFTP(Secure File Transfer Protocol)에서 중단된 업로드를 다시 시작하고 SHA-256 알고리즘을 사용하는 새로운 지문 유형에 대한 지원이 추가되었습니다. 이 **OpenSSH** 버전은 SSH-1 프로토콜에 대한 서버 측 지원도 제거합니다.

- 보다 쉽게 관리할 수 있도록 새로운 Linux 감사 기능이 추가되어 감사 시스템에서 기록된 이벤트를 필터링하고 중요한 이벤트에서 더 많은 정보를 수집하고, 많은 수의 레코드를 해석합니다.

- **OpenSC** 세트의 라이브러리 및 유틸리티에는CAC(Common Access Card) 카드에 대한 지원이 추가되어 이제 **CoolKey** recommendations 기능도 제공합니다.

- **OpenSSL** 업데이트에는 DTLS(Datagram Transport Layer Security) 버전 1.2 프로토콜 및 ALPN(Application-Layer Protocol Negotiation)에 대한 지원과 같은 여러 개선 사항이 포함되어 있습니다.

- **OpenSCAP** 툴은 NIST 인증을 통해 규제된 환경에서 보다 쉽게 채택할 수 있습니다.

- 안전하지 않은 암호화 프로토콜 및 알고리즘은 더 이상 사용되지 않습니다. 그러나 이 버전에서는 다른 많은 암호화 관련 개선 사항도 도입되었습니다. 자세한 내용은 V 부. 지원되지 않는 기능 및 Red Hat 고객 포털의 Red Hat Enterprise Linux 7.4 지식 베이스에서 Cryptography 변경 사항을 사용하여 운영 체제 보안 강화 문서를 참조하십시오.

보안 강화에 대한 자세한 내용은 15장. *보안* 를 참조하십시오.

IdM (Identity Management)

- 컨테이너의 SSSD(System Security Services Daemon)가 완전히 지원됩니다. IdM(Identity Management) 서버 컨테이너는 기술 프리뷰 기능으로 사용할 수 있습니다.

- 이제 사용자가 FIPS 모드가 활성화된 시스템에 새 ID 관리 서버, 복제본 및 클라이언트를 설치할 수 있습니다.

- 스마트 카드 인증과 관련된 몇 가지 개선 사항이 도입되었습니다.

IdM 변경 사항에 대한 자세한 내용은 5장. *인증 및 상호 운용성* 을 참조하십시오. IdM과 관련된 더 이상 사용되지 않는 기능에 대한 자세한 내용은 V 부. 지원되지 않는 기능 을 참조하십시오.

네트워킹

- **NetworkManager** 는 라우팅을 위한 추가 기능을 지원하며 MACsec(Media Access Control Security) 기술을 활성화하여 관리되지 않는 장치를 처리할 수 있습니다.

- 커널 GRE(Generic Routing Encapsulation) 터널링이 향상되었습니다.

자세한 네트워킹 기능은 14장. *네트워킹* 에서 참조하십시오.

커널

- NVM-Express 커널 드라이버에 NVMe-Express 커널 드라이버에 대한 지원이 추가되어 이더넷 또는 Infiniband 패브릭 인프라의 데이터 센터에 있는 고성능 NVMe 스토리지 장치에 액세스할 때 유연성이 향상됩니다.

커널 관련 추가 변경 사항은 12장. *커널* 에서 참조하십시오.

스토리지 및 파일 시스템

- LVM은 RAID 인수에 대한 전체 지원을 제공하여 RAID 논리 볼륨을 하나의 RAID 수준에서 다른 RAID 수준으로 변환하고 RAID reshaping을 위해 사용자가 RAID 알고리즘, 스트라이프 크기 또는 이미지 수와 같은 속성을 다시 수행할 수 있습니다.

- Docker에서 OverlayFS를 사용할 때 컨테이너에 대한 SELinux 지원을 활성화할 수 있습니다.

- Red Hat Enterprise Linux 클라이언트에서 액세스하는 경우 NFS(NFSoRDMA) 서버가 완전히 지원됩니다.

파일 시스템 개선 사항은 17장. *스토리지* 에서 추가 스토리지 관련 기능 및 9장. *파일 시스템* 를 참조하십시오.

툴

- **Performance Co-** dpdk(PCP) 애플리케이션은 **pcp2infDegradeddb ,pcp -mpstat** 및 **pcp-pidstat** 와 같은 새로운 클라이언트 툴을 지원하도록 개선되었습니다. 또한 여러 하위 시스템의 새로운 PCP 성능 지표는 다양한 Performance Co-octets 분석 툴에서 사용할 수 있습니다.

다양한 툴 업데이트에 대한 자세한 내용은 7장. *컴파일러 및 도구* 을 참조하십시오.

고가용성

- Red Hat Enterprise Linux 7.4에서는 다음 기능을 완벽하게 지원합니다.
  - **Clufter** - 클러스터 구성 형식을 변환하고 분석하기 위한 툴
  - 확장 클러스터를 관리하기 위한 Pacemaker 클러스터의 쿼럼 장치(QDevice)
  - **booth** 클러스터 티켓 관리자

이 릴리스에 도입된 고가용성 기능에 대한 자세한 내용은 6장. *클러스터링* 을 참조하십시오.

가상화

- Red Hat Enterprise Linux 7 게스트 가상 머신은 이제 ENA(Elastic Network Adapter)를 지원하므로 AWS(Amazon Web Services) 클라우드에서 실행되는 경우 향상된 네트워킹 기능을 제공합니다.

가상화에 대한 추가 개선 사항은 19장. *가상화* 에서 참조하십시오.

관리 및 자동화

- Red Hat Enterprise Linux 7.4에는 **Red Hat Enterprise Linux 배포의 관리 및 유지 관리를 간소화하는 구성 인터페이스인 Ansible 을 기반으로 하는 Red Hat Enterprise Linux 시스템**역할이 포함되어 있습니다. 이 기능은 기술 프리뷰로 사용할 수 있습니다.

자세한 내용은 47장. *Ansible에서 지원하는 Red Hat Enterprise Linux 시스템 역할* 의 내용을 참조하십시오.

Red Hat Insights

Red Hat Enterprise Linux 7.2부터는 *Red Hat Insights* 서비스를 사용할 수 있습니다. Red Hat Insights는 배포에 영향을 미치기 전에 알려진 기술 문제를 식별, 검사 및 해결할 수 있도록 설계된 적극적인 서비스입니다. Insights는 Red Hat 지원 엔지니어에 대한 지식, 문서화된 솔루션, 해결된 문제를 활용하여 시스템 관리자에게 실행 가능한 관련 정보를 제공합니다.

이 서비스는 at https://access.redhat.com/insights/ 또는 Red Hat Satellite를 통해 고객 포털을 통해 호스팅 및 제공됩니다. 시스템을 등록하려면 Insights 시작하기 가이드를 따르십시오. 자세한 내용은 의 내용을 https://access.redhat.com/insights/splash/ 참조하십시오.

Red Hat Customer Portal 랩

Red Hat 고객 포털 랩 은 다음 주소에 있는 고객 포털 https://access.redhat.com/labs/ 섹션의 툴 세트입니다. Red Hat 고객 포털 랩의 애플리케이션은 성능을 개선하고, 문제를 신속하게 해결하고, 보안 문제를 식별하며, 복잡한 애플리케이션을 신속하게 배포 및 구성하는 데 도움이 될 수 있습니다. 가장 인기있는 애플리케이션 중 일부는 다음과 같습니다.

- registration Assistant
- 코드 브라우저
- Red Hat 제품 인증서
- Red Hat Network (RHN) 시스템 목록 내보내기
- Kickstart 생성
- 로그 리퍼
- 로드 밸런서 구성 도구
- 다중 경로 도움말기

2장. 아키텍처

Red Hat Enterprise Linux 7.4는 다음 아키텍처에 대한 지원을 제공하는 커널 버전 3.10.0-693과 함께 배포됩니다. [1]

- 64비트 AMD
- 64비트 Intel
- IBM POWER7+ 및 POWER8 (big endian) [2]
- IBM POWER8 (little endian) [3]
- IBM z Systems [4]

---

[1] Red Hat Enterprise Linux 7.4 설치는 64비트 하드웨어에서만 지원됩니다. Red Hat Enterprise Linux 7.4는 이전 버전의 Red Hat Enterprise Linux를 가상 머신으로 포함하여 32비트 운영 체제를 실행할 수 있습니다.

[2] Red Hat Enterprise Linux 7.4(big endian)는 현재 Red Hat Enterprise Virtualization for Power 및 PowerVM에서 KVM 게스트로 지원됩니다.

[3] Red Hat Enterprise Linux 7.4(little endian)는 현재 Red Hat Enterprise Virtualization for Power, on PowerVM 및 PowerNV(bare metal)에서 KVM 게스트로 지원됩니다.

[4] Red Hat Enterprise Linux 7.4는 IBM zEnterprise 196 하드웨어 이상을 지원합니다. IBM z10 Systemsmem 시스템은 더 이상 지원되지 않으며 Red Hat Enterprise Linux 7.4를 부팅하지 않습니다.

3장. 외부 커널 매개 변수의 중요한 변경 사항

이 장에서는 시스템 관리자에게 Red Hat Enterprise Linux 7.4와 함께 제공되는 커널의 중요한 변경 사항에 대한 요약을 제공합니다. 이러한 변경 사항에는 추가 또는 업데이트된 **proc** 항목, **sysctl**, **sysfs** 기본 값, 부팅 매개 변수, 커널 구성 옵션 또는 눈에 띄는 동작 변경이 포함됩니다.

업데이트된 /PROC/SYS/KERNEL 항목

hung_task_panic

응답하지 않는 작업이 감지되면 커널의 동작을 제어합니다. 이 파일은 **CONFIG_DETECT_HUNG_TASK** 가 활성화된 경우 발생합니다.

형식: { "0" | "1" }

0 - 계속 작동합니다. 기본 동작.

1 - 즉시 패닉이 발생합니다.

hung_task_check_count

확인한 작업 수에 상한을 제공합니다. 이 파일은 **CONFIG_DETECT_HUNG_TASK** 가 활성화된 경우 발생합니다.

hung_task_timeout_secs

점검 간격. D 상태의 작업이 이 값보다 장기간 예약되지 않은 경우 경고를 보고합니다. 이 파일은 **CONFIG_DETECT_HUNG_TASK** 가 활성화된 경우 발생합니다.

0 - 무한 시간 - 확인하지 않음

hung_task_warning

점검 간격 동안 보고할 최대 경고 수를 제공합니다. 이 값에 도달하면 더 이상 경고가 보고되지 않습니다. 이 파일은 **CONFIG_DETECT_HUNG_TASK** 가 활성화된 경우 발생합니다.

-1 - 무한한 경고 수를 보고합니다.

panic_on_rcu_stall

1로 설정하면 Rcu stall detection 메시지 후 panic() 함수를 호출합니다. 이는 vmcore를 사용하여 Rcu stalls의 근본 원인을 정의하는 데 유용합니다.

0 - Rcu stall이 발생할 때 패닉을 하지 않습니다. 기본 동작.

1 - Rcu stall 메시지를 출력한 후 패닉

업데이트된 /PROC/SYS/USER 항목

/proc/sys/user 디렉터리의 파일을 사용하여 사용자 네임스페이스 제한당 네임스페이스 및 기타 오브젝트 수에 대한 기본 제한을 덮어쓸 수 있습니다. 이러한 제한의 목적은 많은 수의 오브젝트를 만들려고 시도하는 프로그램을 중단하는 것입니다. 이러한 제한의 기본값을 조정하여 정상적인 작업에서 모든 프로그램이 해당 프로그램에 도달할 수 없도록 합니다.

사용자 네임스페이스당 오브젝트 생성은 오브젝트를 생성한 사용자 네임스페이스에서 사용자에게 부과되며, 해당 사용자 네임스페이스의 사용자 제한 아래에 있는 사용자 네임스페이스의 사용자가 확인됩니다. 이러한 오브젝트 생성은 사용자 네임스페이스에서 발생하며 사용자 네임스페이스를 생성한 모든 사용자에게도 부과됩니다.

생성된 오브젝트의 재귀적 계산을 통해 사용자 네임스페이스를 생성하면 사용자가 현재 제한을 초과할 수 없습니다.

/proc/sys/user 에서 업데이트된 파일은 다음과 같습니다.

max_cgroup_namespaces

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

max_ipc_namespaces

현재 사용자 네임스페이스의 모든 사용자가 생성할 수 있는 최대 프로세스 간 통신 네임스페이스 수입니다.

max_mnt_namespaces

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

max_net_namespaces

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

max_pid_namespaces

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

max_user_namespaces

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

max_uts_namespaces

현재 사용자 네임스페이스의 모든 사용자가 생성할 수 있는 최대 UNIX 시계열 시스템(UTS) 네임스페이스 수입니다.

커널 매개변수

acpi_force_table_verification [HW,ACPI]

초기 단계에서 테이블 체크섬 확인을 활성화합니다. 초기 매핑 크기 제한으로 인해 32비트 AMD 및 Intel 아키텍처에서 기본적으로 비활성화되어 있습니다.

acpi_no_auto_ssdt [HW,ACPI]

SSDT(Secondary System Description Table)의 자동 로드를 비활성화합니다.

acpi_no_static_ssdt [HW,ACPI]

초기 부팅 시 정적 SSDT 설치를 비활성화합니다. 기본적으로 Root System Description Table (RSDT) 또는 eXtended System Descriptor Table (XSDT)에 포함된 SSDT는 자동으로 설치되고 **/sys/firmware/acpi/tables** 디렉터리에 나타납니다.

이 옵션은 이 기능을 비활성화합니다. 이 옵션을 지정하면 SSDT 테이블을 **/sys/firmware/acpi/tables/dynamic** 디렉터리에 설치하는 동적 테이블 설치에 영향을 미치지 않습니다.

irqaffinity= [SMP]

기본 irq 선호도 마스크를 다음 형식으로 설정합니다.

형식: <cpu number>,.., <cpu 번호>

또는

<CPU 번호>-<cpu 번호>

오름차순 또는 조합을 사용하여 양수 범위를 사용할 수 있습니다.

<cpu number>,...,<cpu number>-<cpu number>

nokaslr [KNL]]

초기 부팅 시 정적 SSDT 설치를 비활성화합니다. 기본적으로 RSDT 또는 XSDT에 포함된 SSDT는 자동으로 설치되고 **/sys/firmware/acpi/tables** 디렉터리에 나타납니다.

CONFIG_RANDOMIZE_BASE 가 설정된 경우 커널 및 모듈 기본 오프셋 주소 공간 레이아웃 Randomization (ASLR)을 비활성화합니다.

nohibernate

hibernation 및 resume를 비활성화합니다.

crash_kexec_post_notifiers

panic-notifiers 및 dumping kmsg를 실행한 후 **kdump** 를 실행합니다.

[PCI] hpbussize=nn

핫 플러그 브리지 아래에 버스를 위해 예약된 최소의 추가 버스 번호를 제공합니다. 기본값은 1입니다.

pcie_port_pm=[PCIE]

PCIe 포트 전원 관리 처리:

형식: { "off" | "force" }

off - 모든 PCIe 포트의 전원 관리를 비활성화합니다.

1 - 모든 PCIe 포트의 전원 관리를 활성화합니다.

sunrpc.svc_rpc_per_connection_limit=[NFS,SUNRPC]

단일 연결에서 병렬로 처리할 서버의 요청 수를 제한합니다. 기본값은 0(제한 없음)입니다.

I 부. 새로운 기능

이 부분에서는 Red Hat Enterprise Linux 7.4에 도입된 새로운 기능 및 주요 개선 사항을 설명합니다.

4장. 일반 업데이트

Red Hat Enterprise Linux 6에서 Red Hat Enterprise Linux 7로 인플레이스 업그레이드

즉각적 업그레이드는 기존 운영 체제를 교체하여 시스템을 Red Hat Enterprise Linux의 새로운 주요 릴리스로 업그레이드하는 방법을 제공합니다. 즉각적 업그레이드를 수행하려면 실제 업그레이드를 실행하기 전에 시스템 업그레이드 문제를 확인하는 유틸리티인 **Preupgrade Assistant** 를 사용하고 **Red Hat Upgrade Tool** 에 대한 추가 스크립트도 제공합니다. **Preupgrade Assistant** 에서 보고한 모든 문제를 해결했으면 **Red Hat Upgrade Tool** 을 사용하여 시스템을 업그레이드하십시오.

절차 및 지원되는 시나리오에 대한 자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Migration_Planning_Guide/chap-Red_Hat_Enterprise_Linux-Migration_Planning_Guide-Upgrading.html 및 https://access.redhat.com/solutions/637583 를 참조하십시오.

Red Hat Enterprise Linux 6 Extras 채널에서 **Preupgrade Assistant** 및 **Red Hat Upgrade Tool** 을 사용할 수 있습니다. https://access.redhat.com/support/policy/updates/extras 를 참조하십시오. (BZ#1432080)

cloud-init Base 채널로 이동합니다.

Red Hat Enterprise Linux 7.4에서 cloud-init 패키지와 해당 종속 항목은 Red Hat Common 채널에서 Base 채널로 이동되었습니다. **cloud-init** 는 환경에서 제공하는 메타데이터를 사용하여 시스템의 초기 초기화를 처리하는 툴입니다. 일반적으로 OpenStack 또는 Amazon Web Services와 같은 클라우드 환경에서 부팅하는 서버를 구성하는 데 사용됩니다. Red Hat Common 채널을 통해 제공되는 최신 버전에서는 cloud-init 패키지가 업데이트되지 않았습니다. (BZ#1427280)

5장. 인증 및 상호 운용성

컨테이너에서 SSSD가 완전히 지원됨

SSSD(System Security Services Daemon)를 제공하는 rhel7/sssd 컨테이너 이미지는 더 이상 기술 프리뷰 기능이 아닙니다. 이제 이미지가 완전히 지원됩니다. **rhel7/ipa-server** 컨테이너 이미지는 여전히 기술 프리뷰 기능입니다.

자세한 내용은 https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/using_containerized_identity_management_services 을 참조하십시오. (BZ#1467260)

Identity Management에서 FIPS 지원

이번 개선된 기능을 통해 IdM(Identity Management)은 연방 정보 처리 표준(FIPS)을 지원합니다. 이를 통해 FIPS 기준을 충족해야 하는 환경에서 IdM을 실행할 수 있습니다. FIPS 모드가 활성화된 상태에서 IdM을 실행하려면 FIPS 모드가 활성화된 Red Hat Enterprise Linux 7.4를 사용하여 IdM 환경의 모든 서버를 설정해야 합니다.

다음을 수행할 수 없다는 점에 유의하십시오.

- FIPS 모드가 비활성화된 상태로 이전에 설치된 기존 IdM 서버에서 FIPS 모드를 활성화합니다.
- FIPS 모드가 비활성화된 기존 IdM 서버를 사용할 때 FIPS 모드에서 복제본을 설치합니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html#prerequisites 을 참조하십시오. (BZ#1125174)

SSSD는 사용자가 스마트 카드로 인증할 때 Kerberos 티켓을 얻을 수 있도록 지원합니다.

SSSD(System Security Services Daemon)에서 Kerberos PKINIT 사전 인증 메커니즘을 지원합니다. IdM(Identity Management) 도메인에 등록된 데스크탑 클라이언트 시스템에 스마트 카드를 인증할 때 인증에 성공한 경우 유효한 Kerberos 티켓 생성 티켓(TGT)이 표시됩니다. 그런 다음 사용자는 클라이언트 시스템에서 추가 SSO(Single Sign-On) 인증을 위해 TGT를 사용할 수 있습니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/sc-pkinit-auth.html 을 참조하십시오. (BZ#1200767, BZ#1405075)

SSSD를 사용하면 동일한 스마트 카드 인증서를 사용하여 다른 사용자 계정에 로그인할 수 있습니다.

이전에는 SSSD(System Security Services Daemon)에서 모든 인증서를 단일 사용자에게 고유하게 매핑해야 했습니다. 스마트 카드 인증을 사용할 때 여러 계정이 있는 사용자는 동일한 스마트 카드 인증서를 사용하여 이러한 모든 계정에 로그인할 수 없었습니다. 예를 들어 개인 계정을 보유한 사용자 및 기능 계정(예: 데이터베이스 관리자 계정)이 개인 계정에만 로그인할 수 있었습니다.

이번 업데이트를 통해 SSSD를 더 이상 단일 사용자에게 고유하게 매핑할 필요가 없습니다. 결과적으로 사용자는 단일 스마트 카드 인증서를 사용하여 다른 계정에 로그인할 수 있습니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/smart-cards.html 을 참조하십시오. (BZ#1340711, BZ#1402959)

IdM 웹 UI를 사용하면 스마트 카드 로그인 활성화

Identity Management 웹 UI를 사용하면 스마트 카드를 사용하여 로그인할 수 있습니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/sc-web-ui-auth.html 을 참조하십시오. (BZ#1366572)

새 패키지: keycloak-httpd-client-install

keycloak-httpd-client-install 패키지는 Red Hat Single Sign-On(RH-SSO)으로 등록할 때 Apache **httpd** 인증 모듈의 구성을 자동화하고 단순화할 수 있는 다양한 라이브러리 및 툴을 제공합니다. Keycloak(Identity Provider) 클라이언트라고도 합니다.

RH-SSO에 대한 자세한 내용은 https://access.redhat.com/products/red-hat-single-sign-on 를 참조하십시오.

이번 업데이트의 일환으로 Red Hat Enterprise Linux에 새로운 종속 항목이 추가되었습니다.

- python-requests-oauthlib 패키지: 이 패키지는 python-requests 패키지에 대한 OAuth 라이브러리 지원을 제공합니다. 이 라이브러리는 인증에 OAuth를 사용할 수 있습니다. python-requests
- python-oauthlib 패키지: 이 패키지는 OAuth 인증 메시지 생성 및 사용을 제공하는 Python 라이브러리입니다. 메시지 전송을 제공하는 도구와 함께 사용됩니다. (BZ#1401781, BZ#1401783, BZ#1401784)

새로운 Kerberos 인증 정보 캐시 유형: KCM

이번 업데이트에서는 이름이 **kcm** 인 새 SSSD 서비스가 추가되었습니다. 서비스는 sssd-kcm 하위 패키지에 포함되어 있습니다.

kcm 서비스가 설치되면 **KCM** 이라는 새로운 인증 정보 캐시 유형을 사용하도록 Kerberos 라이브러리를 구성할 수 있습니다. KCM 인증 정보 캐시 유형이 구성된 경우 **sssd-kcm** 서비스는 인증 정보를 관리합니다.

컨테이너화된 환경에는 KCM 인증 정보 캐시 유형이 적합합니다.

- KCM을 사용하면 **kcm** 서비스가 수신 대기하는 UNIX 소켓 마운트에 따라 필요에 따라 컨테이너 간에 인증 정보 캐시를 공유할 수 있습니다.
- **kcm** 서비스는 RHEL이 기본적으로 사용하는 KEYRING 인증 정보 캐시 유형과 달리 커널 외부의 사용자 공간에서 실행됩니다. KCM을 사용하면 선택한 컨테이너에서만 **kcm** 서비스를 실행할 수 있습니다. KEYRING을 사용하면 모든 컨테이너가 커널을 공유하므로 인증 정보 캐시를 공유합니다.

또한 KCM 인증 정보 캐시 유형은 filesystem ccache 유형과 달리 캐시 컬렉션을 지원합니다.

자세한 내용은 sssd-kcm(8) 매뉴얼 페이지를 참조하십시오. (BZ#1396012)

AD 사용자가 웹 UI에 로그인하여 셀프 서비스 페이지에 액세스할 수 있습니다.

이전에는 AD(Active Directory) 사용자가 명령줄에서 **kinit** 유틸리티를 사용하여 인증할 수 있었습니다. 이번 업데이트를 통해 AD 사용자는 IdM(Identity Management) 웹 UI에 로그인할 수도 있습니다. IdM 관리자는 사용자가 로그인하기 전에 AD 사용자에 대한 ID 재정의를 생성해야 합니다.

따라서 AD 사용자는 IdM 웹 UI를 통해 셀프 서비스 페이지에 액세스할 수 있습니다. 셀프 서비스 페이지에 AD 사용자 ID 재정의의 정보가 표시됩니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/using-the-ui.html#ad-users-idm-web-ui 을 참조하십시오. (BZ#872671)

SSSD를 사용하면 SSSD 서버 모드에서 AD 하위 도메인을 설정할 수 있습니다.

이전에는 SSSD(System Security Services Daemon)에서 신뢰할 수 있는 AD(Active Directory) 도메인을 자동으로 구성했습니다. 이번 업데이트를 통해 SSSD는 결합된 도메인과 동일한 방식으로 신뢰할 수 있는 AD 도메인의 특정 매개 변수 구성을 지원합니다.

결과적으로 SSSD가 통신하는 도메인 컨트롤러와 같은 신뢰할 수 있는 도메인에 대한 개별 설정을 설정할 수 있습니다. 이렇게 하려면 이 템플릿의 이름을 사용하여 **/etc/sssd/sssd.conf** 파일에 섹션을 만듭니다.

```
[domain/main_domain/trusted_domain]
```

예를 들어, 기본 IdM 도메인 이름이 ipa.com이고 신뢰할 수 있는 AD 도메인 이름이 ad.com인 경우 해당 섹션 이름은 다음과 같습니다.

```
[domain/ipa.com/ad.com]
```

(BZ#1214491)

SSSD는 AD 환경에서 짧은 이름으로 사용자 및 그룹 조회 및 인증을 지원합니다.

이전 버전에서는 SSSD(System Security Services Daemon)에서 도메인 구성 요소 없이 데몬을 독립 실행형 도메인에 조인된 경우에만 사용자 및 그룹 확인 및 인증이라는 짧은 이름이라는 사용자 이름을 지원했습니다. 이제 이러한 환경의 모든 SSSD 도메인에서 짧은 이름을 사용할 수 있습니다.

- AD(Active Directory)에 연결된 클라이언트의 경우
- AD forest와의 신뢰 관계가 있는 IdM(Identity Management) 배포

짧은 이름을 사용하는 경우에도 모든 명령의 출력 형식은 항상 완전히 정규화됩니다. 이 기능은 다음 방법 중 하나로 도메인 확인 순서 목록을 설정한 후 기본적으로 활성화됩니다(기본 설정 순서로 나열됨).

- 로컬에서 **/etc/sssd/sssd.conf** 파일의 **[sssd]** 섹션에서 **domain_resolution_order** 옵션을 사용하여 목록을 구성합니다.
- ID 보기 사용
- 전역적으로 IdM 구성

기능을 비활성화하려면 **/etc/sssd/sssd.conf** 파일의 **[domain/example.com]** 섹션에서 **use_fully_qualified_names** 옵션을 **True** 로 설정합니다. (BZ#1330196)

SSSD는 UID 또는 FlexVolumes 없이 설정 시 사용자 및 그룹 해상도, 인증 및 권한 부여 지원

기존 SSSD(System Security Services Daemon) 배포에서는 POSIX 속성이 설정되거나 SSSD가 Windows SID(Security identifiers)를 기반으로 사용자와 그룹을 확인할 수 있습니다.

이번 업데이트를 통해 ID 공급자로 LDAP를 사용하는 설정에서 SSSD는 이제 LDAP 디렉터리에 UID 또는 InstallPlans가 없는 경우에도 다음과 같은 기능을 지원합니다.

- D-Bus 인터페이스를 통한 사용자 및 그룹 확인
- Pluga=< 인증 모듈 (PAM) 인터페이스 (BZ#1425891)를 통한 인증 및 권한 부여

SSSD에서는 ssctl user-checks 명령을 도입하여 단일 작업에서 기본 SSSD 기능을 확인합니다.

sssctl 유틸리티에는 이제 **user-checks** 라는 새 명령이 포함되어 있습니다. **sssctl user-checks** 명령은 SSSD(System Security Services Daemon)를 사용자 조회, 인증 및 권한 부여의 백엔드로 사용하는 애플리케이션의 문제를 디버깅하는 데 도움이 됩니다.

- **sssctl user-checks [USER_NAME]** 명령은 NS(Name Service Switch) 및 D-Bus 인터페이스의 InfoPipe 응답자를 통해 사용 가능한 사용자 데이터를 표시합니다. 표시된 데이터는 사용자가 **system-auth** pluggable 인증 모듈(PAM) 서비스를 사용하여 로그인할 수 있는 권한이 있는지 여부를 표시합니다.

- **sssctl user-checks** 에서 허용한 추가 옵션은 인증 또는 다른 PAM 서비스를 확인합니다.

sssctl user-checks 에 대한 자세한 내용은 **sssctl user-checks --help** 명령을 사용합니다. (BZ#1414023)

서비스로서 보안 지원

이번 업데이트에서는 SSSD(System Security Services Daemon)에 **시크릿** 이라는 응답자가 추가되었습니다. 이 응답기를 통해 애플리케이션은 Custodia API를 사용하여 UNIX 소켓을 통해 SSSD와 통신할 수 있습니다. 이를 통해 SSSD는 로컬 데이터베이스에 시크릿을 저장하거나 원격 Custodia 서버로 전달할 수 있습니다. (BZ#1311056)

IdM을 사용하면 외부 DNS 서버에서 IdM DNS 레코드의 반자동 업그레이드를 활성화합니다.

외부 DNS 서버의 IdM(Identity Management) DNS 레코드를 업데이트하기 위해 IdM에 **ipa dns-update-system- records --dry-run --out [file]** 명령이 도입되었습니다. 이 명령은 **nsupdate** 유틸리티에서 허용한 형식으로 레코드 목록을 생성합니다.

생성된 파일을 사용하여 TSIG(Transaction Signature) 프로토콜 또는 GSS(GSS-TSIG) 알고리즘으로 보호되는 표준 동적 DNS 업데이트 메커니즘을 사용하여 외부 DNS 서버의 레코드를 업데이트할 수 있습니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/dns-updates-external.html 을 참조하십시오. (BZ#1409628)

IdM에서 SHA-256 인증서 및 공개 키 지문 생성

이전에는 IdM(Identity Management)에서 인증서 및 공개 키의 지문을 생성할 때 MD5 해시 알고리즘을 사용했습니다. 보안 강화를 위해 IdM은 이제 언급한 시나리오에서 SHA-256 알고리즘을 사용합니다. (BZ#1444937)

IdM은 스마트 카드 인증서를 사용자 계정에 연결하기 위한 유연한 매핑 메커니즘 지원

이전에는 IdM(Identity Management)에서 특정 스마트 카드에 해당하는 사용자 계정을 찾을 수 있는 유일한 방법은 전체 스마트 카드 인증서를 Base64로 인코딩된 DER 문자열로 제공하는 것이었습니다. 이번 업데이트를 통해 인증서 문자열 자체뿐만 아니라 스마트 카드 인증서의 속성을 지정하여 사용자 계정을 찾을 수 있습니다. 예를 들어 관리자는 일치 및 매핑 규칙을 정의하여 특정 CA(인증 기관)에서 발급한 스마트 카드 인증서를 IdM의 사용자 계정에 연결할 수 있습니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/smart-cards.html#sc-one-card-multiple-accounts-links 을 참조하십시오. (BZ#1402959)

새로운 사용자 공간 도구를 사용하면 더 편리한 LMDB 디버깅을 사용할 수 있습니다.

이번 업데이트에서는 **mdb_copy**,**mdb_dump**,**mdb_load**, **mdb_stat** 툴을 **/usr/libexec/openldap/** 디렉터리에 도입합니다. 또한 **man/man1** 하위 디렉터리에 있는 관련 도움말 페이지가 포함되어 있습니다. 새로운 툴은 Lightning Memory-Mapped Database(LMDB) 백엔드와 관련된 문제를 디버깅하는 데만 사용합니다. (BZ#1428740)

openldap 버전 2.4.44로 다시 시작

openldap 패키지가 업스트림 버전 2.4.44로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 이 새 버전에서는 많은 복제 및 Lightning Memory-Mapped Database(LMDB) 버그가 수정되었습니다. (BZ#1386365)

ID 관리에서 DNS 조회 보안 및 서비스 주체 조회 기능 개선

Kerberos 클라이언트 라이브러리는 티켓 생성 서버(TGS) 요청을 발행할 때 더 이상 호스트 이름을 표준화하지 않습니다. 이 기능은 다음과 같은 이점을 제공합니다.

- 보안은 이전에 표준화 중 이전에 필요한 DNS 조회가 더 이상 수행되지 않기 때문에 보안을 유지하지 않습니다.

- 클라우드 또는 컨테이너화된 애플리케이션과 같은 더 복잡한 DNS 환경에서 서비스 주체 조회성

호스트 및 서비스 주체에서 올바른 FQDN(정규화된 도메인 이름)을 지정해야 합니다. 이러한 동작 변경으로 인해 Kerberos는 보안 주체의 다른 유형의 이름(예: 짧은 이름)을 해결하려고 시도하지 않습니다. (BZ#1404750)

samba 버전 4.6.2로 업데이트

samba 패키지는 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공하는 버전 4.6.2로 업그레이드되었습니다.

- Samba는 이제 **winbindd** 서비스가 시작되기 전에 ID 매핑 구성을 확인합니다. 구성이 유효하지 않으면 **winbindd** 가 시작되지 않습니다. **testparm** 유틸리티를 사용하여 **/etc/hiera/hiera.conf** 파일을 확인합니다. 자세한 내용은1.8.0 **.conf** 매뉴얼 페이지의 RuntimeClass **MAPPING CONSIDERATIONS** 섹션을 참조하십시오.

- 이제 Windows 10에서 프린터 드라이버를 업로드하는 것이 올바르게 작동합니다.

- 이전에는 RuntimeClass **서버 동적 포트 범위** 매개 변수의 기본값은 **1024-1300** 이었습니다. 이번 업데이트에서는 기본값이 **49152-65535** 로 변경되었으며 이제 Windows Server 2008 이상에서 사용되는 범위와 일치합니다. 필요한 경우 방화벽 규칙을 업데이트합니다.

- **net advertising unregister** 명령은 이제 도메인을 나가면 Active Directory DNS 영역에서 호스트의 DNS 항목을 삭제할 수 있습니다.

- 이제 xfs **2 리스 매개변수에서 SMB 2.1 리스가** 기본적으로 활성화됩니다. SMB는 클라이언트가 적극적으로 파일을 캐시할 수 있도록 지원합니다.

- 보안을 강화하기 위해 NT LAN 관리자 버전 1(NTLMv1) 프로토콜은 기본적으로 비활성화되어 있습니다. 비보안 RuntimeClassv1 프로토콜이 필요한 경우 **/etc/hiera/hiera.conf 파일의 ntlm auth 매개변수를 yes 로 설정합니다.**

- **이벤트** 하위 명령이 이벤트 스크립트와 상호 작용하기 위해 **ctdb** 유틸리티에 추가되었습니다.

- **idmap_hash** ID 매핑 백엔드는 더 이상 사용되지 않는 것으로 표시되고 향후 Samba 버전에서 제거됩니다.

- 더 이상 사용되지 않는 사용자와 **사용자 이름 매개변수만** 제거되었습니다.

Samba는 LABELd ,**nmbd** 또는 **winbind** 데몬이 시작될 때 tdb 데이터베이스 파일을 자동으로 업데이트합니다. **Samba를 시작하기 전에 데이터베이스 파일을 백업하십시오. Red Hat은 downgrading tdb 데이터베이스 파일을 지원하지 않습니다.**

주요 변경 사항에 대한 자세한 내용은 업데이트 전에 업스트림 릴리스 노트를 참조하십시오. (BZ#1391954)

authconfig 를 사용하면 SSSD 에서 스마트 카드로 사용자를 인증할 수 있습니다.

이 새로운 기능을 통해 authconfig 명령은 SSSD(System Security Services Daemon)를 구성하여 스마트 카드로 사용자를 인증할 수 있습니다.

```
# authconfig --enablesssd --enablesssdauth --enablesmartcard --smartcardmodule=sssd --
smartcardaction=0 --updateall
```

이번 업데이트를 통해 이제 **pam_pkcs11** 이 설치되지 않은 시스템에서 스마트 카드 인증을 수행할 수 있습니다. 그러나 **pam_pkcs11** 이 설치된 경우**--smartcardmodule=sssd** 옵션이 무시됩니다. 대신 **/etc/pam_pkcs11/pam_pkcs11.conf** 에 정의된 첫 번째 pkcs11_module이 기본값으로 사용됩니다.

자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/aut idm-client-sc.html 을 참조하십시오. (BZ#1378943)

authconfig 를 사용하여 계정 잠금을 활성화할 수 있습니다.

이번 업데이트에서는 **authconfig** 명령에 **--enable** octets 옵션이 추가되었습니다. 옵션을 활성화하면 15분 간격 내에 4번 연속 로그인 시도에 실패한 로그인 시도 후 20분 동안 구성된 계정이 잠깁니다. (BZ#1334449)

IdM 서버 성능 개선

IdM(Identity Management) 서버는 많은 공통 워크플로우 및 설정에서 성능이 향상되었습니다. 이러한 개선 사항은 다음과 같습니다.

- IdM 서버 관리 프레임워크 내 왕복을 줄임으로써 Vault 성능이 향상되었습니다.
- IdM 서버 관리 프레임워크가 내부 통신 및 인증에 소요되는 시간을 단축하도록 조정되었습니다.
- Directory Server 연결 관리는 **nunc-stans** 프레임워크를 사용하여 보다 확장 가능합니다.
- 새로운 설치에서 Directory Server는 이제 서버의 하드웨어 리소스에 따라 데이터베이스 항목 캐시 및 스레드 수를 자동으로 조정합니다.
- 대용량 또는 중첩 그룹으로 작업할 때 **memberOf** 플러그인 성능이 향상되었습니다. (BZ#1395940, BZ#1425906, BZ#1400653)

IdM 웹 UI의 기본 세션 만료 기간이 변경되었습니다.

이전에는 사용자가 사용자 이름과 암호를 사용하여 IdM(Identity Management) 웹 UI에 로그인하면 웹 UI에서 20분 동안 비활성 후 자동으로 사용자를 기록했습니다. 이번 업데이트를 통해 기본 세션 길이는 로그인 작업 중에 얻은 Kerberos 티켓의 만료 기간과 동일합니다. 기본 세션 길이를 변경하려면 **/etc/ipa/default.conf** 파일에서 **kinit_lifetime** 옵션을 사용하고 **httpd** 서비스를 다시 시작합니다. (BZ#1459153)

dbmon.sh 스크립트는 인스턴스 이름을 사용하여 Directory Server 인스턴스에 연결합니다.

dbmon.sh 쉘 스크립트를 사용하면 Directory Server 데이터베이스 및 항목 캐시 사용을 모니터링할 수 있습니다. 이번 업데이트를 통해 스크립트는 더 이상 **HOST** 및 **PORT** 환경 변수를 사용하지 않습니다. 보안 바인딩을 지원하기 위해 스크립트에서 **SERVID** 환경 변수에서 Directory Server 인스턴스 이름을 읽고 이를 사용하여 서버에 보안 연결이 필요한 경우 호스트 이름, 포트 및 정보를 검색합니다. 예를 들어 **slapd-localhost** 인스턴스를 모니터링하려면 다음을 입력합니다.

```
SERVID=slapd-localhost INCR=1 BINDDN="cn=Directory Manager" BINDPW="password" dbmon.sh
```

(BZ#1394000)

Directory Server에서 **SSHA_512** 암호 스토리지 스키마를 기본값으로 사용합니다.

이전 버전에서는 Directory Server는 **cn=config** 항목의 **passwordStorageScheme** 및 **nsslapd-rootpwstoragescheme** 매개변수에 설정된 기본 암호 스토리지 체계로 약한160 비트 솔라이크(Secure hashed secure hash algorithm)를 사용했습니다. 보안을 강화하기 위해 두 매개 변수의 기본값이 강력한 512비트 SSHA 스키마(SSHA_512)로 변경되었습니다.

새 기본값이 사용됩니다.

- 새 Directory Server 설치를 수행할 때
- **passwordStorageScheme** 매개변수가 설정되지 않고**userPassword** 속성에 저장된 암호를 업데이트하는 것입니다.
- **nsslapd-rootpwstoragescheme** 매개변수가 설정되지 않고**nsslapd-rootpw** 특성에 설정된 Directory Server 관리자 암호를 업데이트 중입니다. (BZ#1425907)

Directory Server에서 tcmalloc 메모리 allocator 사용

Red Hat Directory Server에서 **tcmalloc** 메모리 할당기를 사용합니다. 이전에 사용된 표준**glibc** 할당기에는 더 많은 메모리가 필요했고, 경우에 따라 서버가 메모리가 부족해질 수 있었습니다. **tcmalloc** 메모리 할당기를 사용하면 Directory Server에서 더 적은 메모리가 필요하며 성능이 향상되었습니다. (BZ#1426275)

Directory Server에서 nunc-stans 프레임워크 사용

nunc-stans 이벤트 기반 프레임워크가 Directory Server에 통합되었습니다. 이전에는 Directory Server에 동시 들어오는 연결 수가 설정되었을 때 성능이 느려질 수 있었습니다. 이번 업데이트를 통해 서버는 성능 저하 없이 훨씬 더 많은 수의 연결을 처리할 수 있습니다. (BZ#1426278, BZ#1206301, BZ#1425906)

Directory Server memberOf 플러그인의 성능 개선

이전에는 대규모 또는 중첩된 그룹을 사용하여 작업할 때 플러그인 작업에 시간이 오래 걸릴 수 있었습니다. 이번 업데이트를 통해 Red Hat Directory Server **memberOf** 플러그인의 성능이 향상되었습니다. 결과적으로 **memberOf** 플러그인은 이제 그룹에서 사용자를 더 빠르게 추가하고 제거합니다. (BZ#1426283)

Directory Server에서 오류 로그 파일에 심각도 수준을 기록합니다.

Directory Server는 이제 **/var/log/dirsrv/slapd-instance_name/errors** 로그 파일에 심각도 수준을 기록합니다. 이전에는 오류 로그 파일에서 항목의 심각도를 구분하기 어려웠습니다. 이 향상된 기능을 통해 관리자는 심각도 수준을 사용하여 오류 로그를 필터링할 수 있습니다.

자세한 내용은 Red Hat Directory Server 구성, 명령 및 파일 참조의 해당 섹션을 참조하십시오.
https://access.redhat.com/documentation/en-US/Red_Hat_Directory_Server/10/html/Configuration_Command_and_File_Reference/error-logs.html#error-logs-content (BZ#1426289)

Directory Server에서 PBKDF2_SHA256 암호 스토리지 스키마 지원

보안을 강화하기 위해 이 업데이트는 256비트 암호 기반 키 파생 기능 2(PBKDF2_SHA256)를 Directory Server에서 지원되는 암호 저장소 스키마 목록에 추가합니다. 이 스키마는 30,000회 반복을 사용하여 256비트 보안 해시 알고리즘(SHA256)을 적용합니다.

7.4 버전 이전의 Red Hat Enterprise Linux의 네트워크 보안 서비스(NSS) 데이터베이스는 PBKDF2를 지원하지 않습니다. 따라서 이전 Directory Server 버전의 복제 토폴로지에서는 이 암호 스키마를 사용할 수 없습니다. (BZ#1436973)

Directory Server의 자동 조정 지원 개선

이전에는 데이터베이스를 모니터링하고 설정을 수동으로 튜닝하여 성능을 개선해야 했습니다. 이번 업데이트를 통해 Directory Server는 다음 사항에 맞게 최적화된 자동 조정 기능을 지원합니다.

- 데이터베이스 및 항목 캐시
- 생성된 스레드 수

Directory Server는 서버의 하드웨어 리소스에 따라 이러한 설정을 조정합니다.

새 Directory Server 인스턴스를 설치하는 경우 자동 조정이 기본적으로 자동으로 활성화됩니다. 이전 버전에서 업그레이드한 인스턴스에서는 자동 튜닝을 활성화하는 것이 좋습니다. 자세한 내용은 다음을 참조하십시오.

- 데이터베이스 및 항목 캐시: https://access.redhat.com/documentation/en-US/Red_Hat_Directory_Server/10/html/Performance_Tuning_Guide/memoryusage.html#DB
- 디렉터리 서버 스레드: https://access.redhat.com/documentation/en-US/Red_Hat_Directory_Server/10/html/Performance_Tuning_Guide/ds-threads (BZ#1426286)

새로운 PKI 구성 매개변수를 사용하면 TCP keepalive 옵션을 제어할 수 있습니다.

이번 업데이트에서는 tcp.keepAlive 매개변수가 CS.cfg 구성 파일에 추가되었습니다. 이 매개변수는 부울 값을 허용하며 기본적으로 true 로 설정됩니다. PKI 하위 시스템에서 생성한 모든 LDAP 연결에 대한 TCP keepalive 옵션을 구성하려면 이 매개변수를 사용합니다. 이 옵션은 인증서 발급이 매우 오랜 시간이 걸리는 경우 유용하며 너무 오래 유휴 상태가 된 후 연결이 자동으로 닫힙니다. (BZ#1413132)

PKI 서버에서 강력한 암호화를 사용하여 PKCS #12 파일을 생성

PKCS #12 파일을 생성할 때 이전에는 PKCS #12에서 더 이상 사용되지 않는 키 파생 기능(KDF) 및 트리플 DES(3DES) 알고리즘을 사용했습니다. 이번 업데이트를 통해 이제 명령에서 암호 기반 암호화 표준 2(PBES2) 스키마를 암호 기반 키 파생 함수 2(PBKDF2)와 함께 사용하고 Advanced Encryption Standard(AES) 알고리즘을 사용하여 개인 키를 암호화합니다. 결과적으로 이러한 기능 향상을 통해 보안이 강화되고 Common criteria 인증 요구 사항을 준수할 수 있습니다. (BZ#1426754)

암호화 작업에 사용할 수 있는 CC 호환 알고리즘

공통 기준은 승인된 알고리즘을 사용하여 암호화 및 키 줄 바꿈 작업을 수행해야 합니다. 이러한 알고리즘은 인증 기관의 보호 프로파일의 FCS_COP.1.1(1) 섹션에 명시되어 있습니다. 이번 업데이트에서는 KRA의 암호화 및 암호 해독을 수정하여 승인된 AES 암호화를 사용하고 보안 및 키의 전송 및 저장 알고리즘을 래핑합니다. 이번 업데이트에서는 서버 및 클라이언트 소프트웨어 변경 사항이 필요합니다. (BZ#1445535)

TPS 인터페이스에서 메뉴 항목의 가시성을 구성할 수 있는 새로운 옵션

이전에는 TPS(Token Processing System) 사용자 인터페이스의 시스템 메뉴에 그룹화된 메뉴 항목이 사용자 역할에 따라 정적으로 결정되었습니다. 특정 상황에서는 표시된 메뉴 항목이 사용자가 실제로 액세스할 수 있는 구성 요소와 일치하지 않았습니다. 이번 업데이트를 통해 TPS 사용자 인터페이스의 시스템 메뉴에는 TPS 관리자의 target.configure.list 매개 변수 및 TPS 에이전트의target.agent_approve.list 매개 변수만 표시됩니다. 이러한 매개변수는 액세스 가능한 구성 요소와 일치하도록 인스턴스 CS.cfg 파일에서 수정할 수 있습니다. (BZ#1391737)

주체 일반 이름 확장에 인증서 주체 일반 이름을 복사하는 프로필 구성 요소 추가

일부 TLS 라이브러리는 DNS 이름이 주체 일반 이름(CN) 필드에만 표시될 때 DNS 이름 확인에 대해 경고하거나 거부하고, 이는 RFC 2818에서 더 이상 사용되지 않는 관행입니다. 이번 업데이트에서는 제목 Common Name을 SAN(Subject Alternative Name) 확장에 복사하고 인증서가 현재 표준을 준수하도록 하는 CommonNameToSANDefault 프로필 구성 요소가 추가되었습니다. (BZ#1305993)

LDIF 가져오기 전에 LDAP 항목을 제거하는 새로운 옵션

CA를 마이그레이션할 때 LDIF 가져오기 전에 LDAP 항목이 존재하면 LDAP 가져오기에서 항목이 다시 생성되지 않아 일부 필드가 누락됩니다. 결과적으로 요청 ID가 정의되지 않은 것으로 표시되었습니다. 이번 업데이트에서는 pkispawn 프로세스 끝에 서명 인증서에 대한 LDAP 항목을 제거하는 옵션이 추가되었습니다. 이 항목은 이후 LDIF 가져오기에 다시 생성됩니다. 이제 서명 항목이 제거되고 LDIF 가져오기에 다시 추가되면 요청 ID 및 기타 필드가 올바르게 표시됩니다. 추가할 올바른 매개변수는 (X) 가져오는 서명 인증서의 일련번호를 10진수로 나타냅니다.

```
pki_ca_signing_record_create=False
pki_ca_signing_serial_number=X
```

(BZ#1409946)

인증서 시스템에서 외부 인증 사용자를 지원

이전에는 인증서 시스템에서 사용자 및 역할을 생성해야 했습니다. 이번 개선된 기능을 통해 외부 ID 공급자

가 인증된 사용자를 허용하도록 인증서 시스템을 구성할 수 있습니다. 또한 영역별 권한 부여 ACL(액세스 제어 목록)을 사용할 수 있습니다. 결과적으로 더 이상 인증서 시스템에서 사용자를 만들 필요가 없습니다. (BZ#1303683)

인증서 시스템에서 인증서 및 CRL 게시 활성화 및 비활성화 지원

이번 업데이트 이전에는 CA(인증 기관)에서 게시가 활성화된 경우 인증서 시스템에서는 CRL(인증서 취소 목록) 및 인증서 게시를 자동으로 활성화했습니다. 결과적으로 인증서 게시가 활성화되지 않은 서버에서 오류 메시지가 기록되었습니다. 인증서 시스템이 향상되었으며 이제 **/var/lib/pki/<instance>/ca/conf/CS.cfg** 파일에서 독립적으로 인증서 및 CRL 게시를 지원하고 있습니다.

인증서 및 CRL 게시를 모두 활성화하거나 비활성화하려면 다음을 설정합니다.

```
ca.publish.enable = True|False
```

CRL 게시만 활성화하려면 다음을 설정합니다.

```
ca.publish.enable = True
ca.publish.cert.enable = False
```

인증서 게시만 활성화하려면 다음을 설정합니다.

```
ca.publish.enable = True
ca.publish.crl.enable = False
```

(BZ#1325071)

searchBase 구성 옵션이 DirAclAuthz PKI 서버 플러그인에 추가되었습니다.

다양한 권한 부여 ACL(액세스 제어 목록) 읽기를 지원하기 위해 **searchBase** 구성 옵션이 **DirAclAuthz** PKI Server 플러그인에 추가되었습니다. 결과적으로 플러그인이 ACL을 로드하는 하위 트리를 설정할 수 있습니다. (BZ#1388622)

성능 향상을 위해 인증서 시스템에서 이제 임시 지원

이번 업데이트 이전에는 KRA(인증서 시스템 키 복구 에이전트) 인스턴스는 항상 LDAP 백엔드에 시크릿의 복구 및 스토리지 요청을 저장합니다. 여러 에이전트가 요청을 승인해야 하는 경우 상태를 저장하는 데 필요합니다. 그러나 요청이 즉시 처리되고 하나의 에이전트만 요청을 승인해야 하는 경우 상태를 저장할 필요가 없습니다. 성능을 개선하기 위해 이제 **/var/lib/pki/<instance>/kra/conf/CS.cfg** 파일에서 **kra.ephemeralRequests=true** 옵션을 설정하여 더 이상 LDAP 백엔드에 요청을 저장하지 않도록 할 수 있습니다. (BZ#1392068)

PKI 배포 구성 파일의 섹션 헤더는 더 이상 대소문자를 구분하지 않습니다.

PKI 배포 구성 파일의 섹션 헤더(예: **[Tomcat]**)는 이전에는 대소문자를 구분하지 않았습니다. 이 동작은 어떠한 이점도 제공하지 않는 동안 오류 발생 가능성을 높였습니다. 이번 릴리스부터 구성 파일의 섹션 헤더는 대소문자를 구분하지 않으므로 오류가 발생할 가능성이 줄어듭니다. (BZ#1447144)

인증서 시스템에서 FIPS 지원 Red Hat Enterprise Linux에서 HSM을 사용하여 CA 설치를 지원합니다.

CA(Certificate System Certificate Authority) 인스턴스를 설치하는 동안 설치 프로그램에서 인스턴스를 다시 시작해야 합니다. 이 재시작 중에 FIPS(Federal Information Processing Standard) 모드가 활성화되어 있고 HSM(하드웨어 보안 모듈)을 사용하는 운영 체제의 인스턴스는 HTTPS 포트 대신 비보안 HTTP 포트에 연결해야 합니다. 이번 업데이트를 통해 HSM을 사용하여 FIPS 지원 Red Hat Enterprise Linux에 Certificate System 인스턴스를 설치할 수 있습니다. (BZ#1450143)

CMC 요청은 이제 AES 및 3DES 암호화에 임의의 IV를 사용합니다.

이번 업데이트를 통해 PKI(Certificate Management over CMS) 요청에서는 보관할 키를 암호화할 때 임

의로 생성된 초기화 벡터(IV)를 사용합니다. 이전에는 클라이언트 및 서버 코드에서 이 시나리오에서 고정 IV를 사용했습니다. CMC 클라이언트 코드가 향상되었으며 결과적으로 Advanced Encryption Standard (AES) 및 Triple Data Encryption Algorithm (3DES)에 대한 암호화를 수행할 때 임의의 IV를 사용하면 보안을 강화합니다. (BZ#1458055)

6장. 클러스터링

clufter 버전 0.76.0으로 다시 시작하고 완전히 지원됩니다.

clufter 패키지는 클러스터 구성 형식을 변환하고 분석하기 위한 툴을 제공합니다. 이전 스택 구성에서 Pacemaker를 활용하는 최신 구성으로의 마이그레이션을 지원하는 데 사용할 수 있습니다. 기술 프리뷰로 이전에 사용 가능한 **clufter** 툴이 이제 완전히 지원됩니다. clufter의 기능에 대한 자세한 내용은 **clufter (1)** 도움말 페이지 또는 **clufter -h** 명령의 출력을 참조하십시오. **clufter** 사용법의 예는 다음 Red Hat Knowledgebase 문서 https://access.redhat.com/articles/2810031 에서 참조하십시오.

clufter 패키지가 업스트림 버전 0.76.0으로 업그레이드되어 여러 버그 수정 및 새 기능을 제공합니다. 주요 업데이트 중 하나는 다음과 같습니다.

- **ccs2pcs*** 명령 제품군으로 CMAN + RGManager 스택 특정 구성을 해당 Pacemaker 구성(또는 **pcs** 명령 시퀀스)로 변환하는 경우 **clufter** 툴에서 더 이상 완전히 유효한 lvm 리소스 에이전트 구성을 변환하지 않습니다.

- CMAN 기반 구성을 **ccs2pcs** 명령 제품군으로 Pacemaker 스택의 유사한 구성으로 변환할 때 이전에 처리 중 손실된 일부 리소스 관련 구성 비트(예: maximum number of failures before returning a failure to a status check)가 올바르게 전파됩니다.

- **clufter** 명령의 **cib2 pcs** 및 **pcs2pcscmd** 제품군으로 pcs 명령을 생성할 때 이제 구성 변경 사항의 단일 단계 푸시(기본값) 동작을 수행하는 경고 핸들러 정의에 적절한 최종 구문이 사용됩니다.

- **pcs** 명령을 생성할 때 **clufter** 툴에서는 전체 구성 업데이트를 푸시하는 대신 중간 업데이트를 통해 구성의 수정 사항만 업데이트할 수 있는 pcs 명령을 생성하는 기본 기능을 지원합니다. 적용 가능한 경우 **clufter** 툴은 이제 사용자 권한(ACL)을 구성하도록 **pcs** 툴에 지시하는 기능을 지원합니다. 이를 위해 문서 스키마의 다양한 주요 버전의 인스턴스에서 작동하도록 Clu fter 는 내부 주문형 형식 업그레이드의 개념을 확보하여 **pacemaker** 의 내부 메커니즘을 미러링합니다. 마찬가지로 **Clufter** 는 이제 번들 기능을 구성할 수 있습니다.

- **clufter** 명령의 **ccs2pcscmd** 및 **pcs2pcscmd** 제품군에 의해 생성된 스크립트와 같은 출력 시퀀스에서 이제 의도한 쉘 인터프리터가 이제 단순한 POSIX 쉘이 아닌 특정 위치에 대해 명확히 하기 위해 운영 체제에서 직접 이해한 첫 번째 줄로 출력됩니다. 이것은 과거의 어떤 상황에서 잘못 일 수 있습니다.

- = 문자가 완료되는 순서로 옵션의 값을 지정하는 경우 **clufter** 의 Bash 완료 파일이 더 이상 제대로 작동하지 않습니다.

- 이제 **Clufter** 툴은 터미널의 대화형 사용을 적절하게 감지하여 출력을 보다 편리하게 표현할 수 있도록 하고, 이전에 무시된 오류 조건에 대해 더 나은 진단을 제공합니다. (BZ#1387424, BZ#1381522, BZ#1440876, BZ#1381531, BZ#1381565)

Pacemaker 클러스터에서 쿼럼 장치 지원

Red Hat Enterprise Linux 7.4는 이전에 기술 프리뷰로 사용 가능한 쿼럼 장치에 대한 전체 지원을 제공합니다. 이 기능은 클러스터의 타사 중재 장치 역할을 하는 별도의 쿼럼 장치(QDevice)를 구성할 수 있습니다. 기본 용도는 클러스터가 표준 쿼럼 규칙에서 허용하는 표준 쿼럼 규칙보다 많은 노드 오류를 유지할 수 있도록 하는 것입니다. 노드 수가 짝수이고 2개 노드 클러스터에 사용하는 경우 쿼럼 장치가 권장됩니다. 쿼럼 장치 구성에 대한 자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/ 을 참조하십시오. (BZ#1158805)

Booth 클러스터 티켓 관리자 지원

Red Hat Enterprise Linux 7.4는 Booth 클러스터 티켓 관리자에 대한 전체 지원을 제공합니다. 이전에 기술 프리뷰로 사용 가능한 이 기능을 사용하면 분산 서비스를 통해 통신하여 리소스 관리를 조정하는 별도의 사이트에서 여러 고가용성 클러스터를 구성할 수 있습니다. Booth 티켓 관리자는 티켓이 부여된 한 번에 하나의 사이트에서만 특정 리소스를 실행하도록 개별 티켓에 대한 합의 기반 결정 프로세스를 용이하게 합니

다. Booth 티켓 관리자를 사용하여 다중 사이트 클러스터를 구성하는 방법에 대한 자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/ (BZ#302087, BZ#1305049)을 참조하십시오.

SBD 데몬과 함께 공유 스토리지를 사용하기 위한 지원 추가

Red Hat Enterprise Linux 7.4는 공유 블록 장치와 SBD(Storage-Based Death) 데몬 사용에 대한 지원을 제공합니다. 이를 통해 이전에 지원했던 워치독 장치를 통해 펜싱 외에도 공유 블록 장치를 사용하여 펜싱을 활성화할 수 있습니다. 이제 **fence-agents** 패키지에서 RHCS 스타일 펜스 에이전트를 통해 실제 펜싱을 트리거하고 제어하는 데 필요한 **fence_sbd** 펜스 에이전트를 제공합니다. Pacemaker 원격 노드에서 SBD가 지원되지 않습니다. (BZ#1413951)

RuntimeClass 리소스 에이전트에 대한 완전한 지원

Samba 배포를 구현하는 데 사용되는 RuntimeClass 리소스 에이전트가 이제 Red Hat Enterprise Linux에서 지원됩니다. (BZ#1077888)

이제 IBM POWER, little endian에서 고가용성 및 복구 스토리지 애드온을 사용할 수 있습니다.

Red Hat Enterprise Linux 7.4에는 IBM POWER, little endian 아키텍처를 위한 고가용성 및 복구 스토리지 애드온 지원이 추가되었습니다. 이 지원은 POWER8 서버의 PowerVM에서 실행되는 클러스터 노드에 대해서만 제공됩니다. (BZ#1289662, BZ#1426651)

pcs에서 암호화된 corosync 통신으로 클러스터를 설정하는 기능 제공

pcs cluster setup 명령에서는 클러스터에서 corosync 암호화 설정을 제어하는 새로운 **--encryption** 플래그를 지원합니다. 이를 통해 사용자는 완전히 신뢰할 수 없는 환경에서 암호화된 corosync 통신으로 클러스터를 설정할 수 있습니다. (BZ#1165821)

원격 및 게스트 노드 지원 및 제거를 위한 새로운 명령

Red Hat Enterprise Linux 7.4는 원격 및 게스트 노드를 생성하고 제거하기 위해 다음과 같은 새로운 명령을 제공합니다.

- pcs cluster node add-guest
- pcs cluster node remove-guest
- pcs cluster node add-remote
- pcs cluster node remove-remote

이러한 명령은 더 이상 사용되지 않는 **pcs cluster remote-node add** 및 **pcs cluster remote-node remove** 명령을 교체합니다. (BZ#1176018, BZ#1386512)

pcsd bind 주소 구성

이제 **/etc/sysconfig/ pcsd** 파일에서 **pcsd** bind 주소를 구성할 수 있습니다. 이전 릴리스에서**pcsd** 는 일부 사용자에게 적합하지 않은 상황인 모든 인터페이스에 바인딩할 수 있었습니다. 기본적으로 **pcsd** 는 모든 인터페이스에 바인딩됩니다. (BZ#1373614)

모니터링 작업을 비활성화하기 위해 pcs resource unmanage 명령에 대한 새로운 옵션

리소스가 관리되지 않는 모드인 경우에도 클러스터에서 모니터 작업을 계속 실행합니다. 이로 인해 리소스가 관리되지 않는 경우 이러한 오류가 발생할 수 있으므로 클러스터에 오류가 보고되지 않을 수 있습니다. **pcs resource unmanage** 명령에서 **--monitor** 옵션을 지원하여 리소스를 관리되지 않는 모드로 배치할 때 모니터링 작업을 비활성화합니다. 또한 **pcs resource manage** 명령은 **--monitor** 옵션을 지원하므로 리소스를 관리 모드로 다시 배치할 때 모니터 작업을 수행할 수 있습니다. (BZ#1303969)

위치 제약 조건을 구성할 때 pcs 명령줄에서 정규식 지원

pcs 는 이제 명령줄의 위치 제약 조건에서 정규식을 지원합니다. 이러한 제약 조건은 일치하는 리소스 이름에 따라 여러 리소스에 적용됩니다. 이는 이전에 여러 개가 필요한 경우 한 가지 제약 조건을 사용할 수 있으므로 클러스터 관리를 단순화합니다. (BZ#1362493)

정규식 또는 노드 속성 및 해당 값으로 펜싱 토폴로지에서 노드 지정

이제 노드 이름에 적용된 정규식과 노드 속성 및 해당 값으로 펜싱 토폴로지에서 노드를 지정할 수 있습니다.

예를 들어 다음 명령은 노드 **node1**, node2 ,**node2** 및 **node3** 을 구성하여 **apc1** 및 **apc2**, **node4**,**node5**, **node6** 노드를 사용하여 펜싱 장치**apc3** 및 **apc4** 를 사용합니다.

```
pcs stonith level add 1 "regexp%node[1-3]" apc1,apc2
pcs stonith level add 1 "regexp%node[4-6]" apc3,apc4
```

다음 명령은 노드 속성 일치를 사용하여 동일한 결과를 제공합니다.

```
pcs node attribute node1 rack=1
pcs node attribute node2 rack=1
pcs node attribute node3 rack=1
pcs node attribute node4 rack=2
pcs node attribute node5 rack=2
pcs node attribute node6 rack=2
pcs stonith level add 1 attrib%rack=1 apc1,apc2
pcs stonith level add 1 attrib%rack=2 apc3,apc4
```

(BZ#1261116)

리소스 에이전트 Oracle 및 OraLsnr에 대한 Oracle 11g 지원

Red Hat Enterprise Linux 7.4는 Pacemaker와 함께 사용되는 **Oracle** Database 11g 및 Oracle Database 11 **snr** 리소스 에이전트를 지원합니다. (BZ#1336847)

공유 스토리지와 함께 SBD 사용 지원

pcs 명령을 사용하여 공유 스토리지로 구성된 SBD(Storage-Based Death)에 대한 지원이 추가되었습니다. SBD fending에 대한 자세한 내용은 https://access.redhat.com/articles/2943361 을 참조하십시오. (BZ#1413958)

NodeUtilization 리소스 에이전트 지원

Red Hat Enterprise Linux 7.4는 **NodeUtilization** 리소스 에이전트를 지원합니다. **NodeUtilization** 에이전트는 사용 가능한 CPU, 호스트 메모리 가용성 및 하이퍼 바이저 메모리 가용성의 시스템 매개변수를 감지하고 이러한 매개변수를 CIB에 추가할 수 있습니다. 에이전트를 복제 리소스로 실행하여 각 노드에서 이러한 매개변수를 자동으로 채울 수 있습니다. **NodeUtilization** 리소스 에이전트 및 이 에이전트의 리소스 옵션에 대한 자세한 내용은 **pcs resource describe NodeUtilization** 명령을 실행합니다. Pacemaker의 사용률 및 배치 전략에 대한 자세한 내용은 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/High_Availability_Add-On_Reference/s1-utilization-HAAR.html 를 참조하십시오. (BZ#1430304)

7장. 컴파일러 및 도구

pcp 버전 3.11.8을 다시 시작

PCP(**Performance Co-** dpdk 애플리케이션)가 업스트림 버전 3.11.81로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 개선 사항은 다음과 같습니다.

- 새로운 클라이언트 도구 **pcp2infDegradeddb** 가 추가되어 성능 지표 값을 infDegradeddb 데이터베이스로 내보낼 수 있습니다.
- 새 클라이언트 툴 **pcp-mpstat** 및 **pcp-pidstat** 이 추가되었습니다.MPstat 및 pidstat 값의 역추적 분석을 수행할 수 있습니다.
- 장치 매퍼, **Ceph** 장치, cpusched cgroups, per-processor soft IRQs,**buddyinfo**,**zoneinfo**, shared memory, **libvirt**, same-page- share, **lio**,**Redis**, **Docker** 용으로 새로운 성능 지표가 추가되었습니다.
- 이제 여러 하위 시스템의 추가 성능 지표를 다양한 PCP 분석 툴에 사용할 수 있습니다. (BZ#1423020)

systemtap 버전 3.1로 업데이트

systemtap 패키지가 업스트림 버전 3.1로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 시스템 호출에 대한 프로브는 더 이상 **debuginfo** 정보를 기반으로 하는 기본 상태가 아닙니다.
- **Python** 기능에 대한 지원이 추가되었습니다.
- **Java** 함수 매개 변수에 대한 액세스도 더 균일하게 설정되었습니다.
- 통계 집계 변수의 성능이 향상되었습니다.
- 새로운 통계 연산자 **@variance** 가 추가되었습니다.
- 사용자 공간 값 가져오기 및 설정에 대한 더 많은 옵션이 추가되었습니다.
- 샘플로 NFS 모니터링 개선

스크립트 및 탭 호환성 수정 (BZ#1398393, BZ#1416204, BZ#1433391)

valgrind 버전 3.12로 업데이트

valgrind 패키지가 업스트림 버전 3.12로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 새 옵션 **--ignore-range-below-sp** 가 memcheck 도구에 추가되어 스택 포인터 아래의 메모리 액세스를 무시합니다. 이는 현재 더 이상 사용되지 않는 옵션 **--workaround-gcc296-bugs=yes** 를 일반적으로 대체합니다.
- **--gen-suppressions=yes** 옵션에 의해 생성된 억제 항목의 최대 호출자는**--num-callers** 옵션에서 지정한 값과 동일합니다.
- 가장 일반적인 사용 사례에 맞는 코드 블록, AMD64 및 Intel 64 아키텍처의 **memcheck** 도구의 비용이 감소되었습니다.
- 8KB 이하의 명령 주소 범위를 많이 삭제하는 디버깅 프로그램에 대해 성능이 향상되었습니다.
- IBM Power 9 (ISA 3.0) 아키텍처에 대한 지원이 추가되었습니다.

- AMD FMA4 지침에 대한 부분적인 지원이 추가되었습니다.
- 64비트 ARM 아키텍처 버전 8에서 암호화 및 CRC 명령 지원이 추가되었습니다. (BZ#1391217)

새 패키지: unitsofmeasurement

unitsofmeasurement 패키지를 사용하면 Java 코드에서 측정 단위를 표시할 수 있습니다. 측정 단위를 위한 새로운 API를 사용하면 물리적 수량 처리가 쉬워지고 오류가 발생하기 쉽습니다. 패키지의 API는 메모리 및 리소스를 사용하는 데 효율적입니다. (BZ#1422263)

HTTP 클라이언트에 대한 SSL/TLS 인증서 확인은 이제 Python 표준 라이브러리에서 기본적으로 활성화되어 있습니다.

HTTP 클라이언트의 기본 글로벌 설정은 기본적으로 SSL/TLS 인증서를 확인하기 위해 Python 표준 라이브러리에서 변경되었습니다. 파일 기반 구성을 사용하는 고객은 영향을 받지 않습니다. 자세한 내용은 https://access.redhat.com/articles/2039753 을 참조하십시오. (BZ#1219110)

%gemspec_add_dep 및 %gemspec_remove_dep 에 대한 지원이 추가되었습니다.

이번 업데이트에서는 %gemspec_add_dep 및 %gemspec_remove_dep 매크로에 대한 지원이 추가되었습니다. 이러한 매크로를 사용하면 rubygem-* 패키지 종속성을 보다 쉽게 조정할 수 있습니다. 또한 모든 현재 매크로는 시험판 버전의 패키지 지원을 개선하도록 확장되었습니다. (BZ#1397390)

ipmitool 버전 1.8.18로 업데이트

ipmitool 패키지가 업스트림 버전 1.8.18로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- PEF 사용자 인터페이스가 재설계되었습니다.
- IP 버전 6 로컬 영역 네트워크 매개 변수에 대해 새 하위 명령 lan6 이 추가되었습니다.
- VITA 관련 센서 유형 및 이벤트 지원이 추가되었습니다.
- SHA_MD5 및SHA_SHA256 암호화 지원이 추가되었습니다.
- etcdctlCMG 확장 기능 5.x 검사에 대한 지원이 추가되었습니다.
- 새로운 통신 인터페이스로 USB 매체에 대한 지원이 추가되었습니다.
- GNU Linux 시스템(BZ#1398658)에 대해 USB 드라이버가 기본적으로 활성화되어 있습니다.

lshw IBM Power의 little-endian 변형 업데이트

머신의 하드웨어 구성에 대한 자세한 정보를 제공하는 lshw 패키지가 IBM Power System의 little-endian 변형에 대해 업데이트되었습니다. (BZ#1368704)

Intel Xeon v5에서 코어 수 없는 이벤트 지원

이번 업데이트를 통해 Intel Xeon v5 서버 CPU에서 점수가 없는 이벤트를 지원하도록 Linux(perf)용 성능 분석 도구가 업데이트되었습니다. 이러한 이벤트는 고급 사용자를 위한 추가 성능 모니터링 정보를 제공합니다. (BZ#1355919)

dmidecode updated

dmidecode 패키지가 최신 버전으로 업데이트되어 여러 버그 수정 및 하드웨어 지원 개선 사항이 추가되었습니다. (BZ#1385884)

이제 iSCSI에서 skopeo를 사용하여 ALUA 작업 구성을 지원합니다 .

이니시에이터에서 대상으로 여러 경로를 사용하면 기본적이지 않은 방식으로 경로를 사용하는 방법에 대한 기본 설정을 구성하려면 **Asymmetric Logical Unit Assignment (ALUA)**를 사용할 수 있습니다. **Linux-IO(Linux-IO)** 커널 대상은 항상 이 기능을 지원합니다. 이번 업데이트를 통해 **opm** 명령 쉘 을 사용하여 **ALUA** 작업을 구성할 수 있습니다. **(BZ#1243410)**

jansson 버전 **2.10**으로 다시 시작

jansson 라이브러리가 버전 **2.10**으로 업데이트되어 이전 버전에 대해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 **clevis,tang** 및 **jose** 애플리케이션을 지원하기 위해 인터페이스가 추가되었습니다. **(BZ#1389805)**

Egrep 및 **fgrep**의 새로운 호환성 환경 변수

이전 **grep** 기반에서 **egrep** 및 **fgrep** 명령은 각각 **grep -E** 및 **grep -F** 로 교체되었습니다. 이러한 변경은 **ps** 명령의 외부에만 **grep** 만 표시되었기 때문에 고객 스크립트에 영향을 미칠 수 있습니다. 이러한 문제를 방지하기 위해 이 업데이트에는 새로운 호환성 환경 변수인 **GREP_LEGACY_EGREP_PS** 가 도입되었습니다. **ps** 출력에 **egrep** 및 **fgrep** 표시를 유지하려면 변수를 **1**로 설정합니다.

```
GREP_LEGACY_EGREP_FGREP_PS=1
```

(BZ#1297441)

lastcomm 에서 **--pid** 옵션 지원

lastcomm 명령은 이제 **--pid** 옵션을 지원합니다. 이 옵션은 커널에서 지원하는 경우 각 레코드에 대한 프로세스 **ID(PID)** 및 상위 프로세스 **ID(PPID)**를 표시합니다. **(BZ#1255183)**

새 패키지: **perl-Perl4-CoreLibs**

새로운 **perl-Perl4-CoreLibs** 패키지는 이제 **Red Hat Enterprise Linux 7**의 기본 채널에서 사용할 수 있습니다. 이 패키지에는 **Perl 4**에서 이전에 사용할 수 있었지만 **Red Hat Enterprise Linux 7**과 함께 배포되는 **Perl 5.16**에서 제거된 라이브러리가 포함되어 있습니다. 이전 릴리스에서 이러한 라이브러리는 선택적 채널을 통해 **Perl** 하위 패키지로 제공되었습니다. **(BZ#1366724)**

tar 은 아카이브에서 추출할 때 심볼릭 링크를 따릅니다.

이번 업데이트에서는 **tar** 명령에 **--keep-directory-symlink** 옵션이 추가되었습니다. 이 옵션은 추출하려는 디렉터리와 이름이 동일한 **symlink**가 표시되면 **tar** 의 동작을 변경합니다. 기본적으로 **tar** 은 먼저 심볼릭 링크를 제거한 다음 디렉터리 추출을 진행합니다. **--keep-directory-symlink** 옵션은 이 동작을 비활성화하고 아카이브에서 추출할 때 **tar** 에 **symlink**를 디렉터리에 따르도록 지시합니다. **(BZ#1350640)**

IO::Socket::SSL Perl 모듈이 **TLS** 버전 제한 지원

보안을 개선하기 위해 **Net:SSLeay Perl** 모듈이 **TLS** 프로토콜 버전 **1.1** 또는 **1.2**의 명시적 사양을 지원하도록 업데이트되었으며 **IO::Socket::SSL** 모듈이 적절하게 업데이트되었습니다. 새 **IO::Socket::SSL**

오브젝트가 생성되면 이제 SSL_version 옵션을 TLSv1_1 또는 TLSv1_2 로 설정하여 TLS 버전을 1.1 또는 1.2로 제한할 수 있습니다. 또는 TLSv11 및 TLSv12 를 사용할 수 있습니다. 이러한 값은 대/소문자를 구분합니다.These values are case-sensitive. (BZ#1335035)

Net:SSLeay Perl 모듈에서 이제 TLS 버전 제한 지원

Net:SSLeay Perl 모듈이 업데이트되어 보안 개선에 사용할 수 있는 TLS 프로토콜 버전의 명시적 사양을 지원합니다. TLS 버전을 1.1 또는 1.2로 제한하려면 Net::SSLeay::ssl_version 변수를 각각 11 또는 12 로 설정합니다. (BZ#1335028)

wget 은 TLS 프로토콜 버전의 사양 지원

이전에는 wget 유틸리티에서 원격 서버에 연결할 때 기본적으로 가장 높은 TLS 프로토콜 버전 1.2를 사용했습니다. 이번 업데이트를 통해 사용자가 --secure-protocol=TLSv1_1 또는 --secure-protocol=TLSv1_2 명령줄 옵션을 wget 명령에 추가하여 TLS 프로토콜 마이너 버전을 명시적으로 선택할 수 있도록 wget 이 개선되었습니다. (BZ#1439811)

tcpdump 버전 4.9.0으로 업데이트

tcpdump 패키지가 업스트림 버전 4.9.0으로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 많은 보안 취약점이 수정되었습니다.
- 인기 있는 네트워크 프로토콜의 dissection에서 많은 개선이 이루어졌습니다.
- 기본 snaplen 기능이 262144 바이트로 증가했습니다.
- 캡처 버퍼는 4MiB로 확대되었습니다(BZ#1422473)

tcpdump 에 대한 캡처 방향을 -P 에서 -Q로 설정하는 옵션

이전에는 Red Hat Enterprise Linux의 tcpdump 유틸리티에서 -P 옵션을 사용하여 캡처 방향을 설정했지만 업스트림 버전은 -Q 를 사용했습니다. -Q 옵션이 구현되어 현재 선호됩니다. -P 옵션은 이전 함수를 -Q 의 별칭으로 유지하지만 경고가 표시됩니다. (BZ#1292056)

OpenJDK 는 64비트 ARM 아키텍처에서 SystemTap 지원

OpenJDK 플랫폼은 이제 64비트 ARM 아키텍처에서 SystemTap 계측 툴을 사용한 인트로스펙션을 지원합니다. (BZ#1373986)

sos 버전 3.4로 다시 기반

sos 패키지가 업스트림 버전 **3.4**로 업데이트되어 다음과 같은 여러 개선 사항, 새로운 기능 및 버그 수정이 제공됩니다.

- **ceph_ansible,collectd,crypto,dracut,gnocchi,jars,nfsganesha, nodejs ,nodejs,openstack_ansible,openstack_instack,openstack_manila, snippet , Salt , Salt , Salt , , Saltmaster, storage console**에 대한 새로운 플러그인이 추가되었습니다.

- **API** 플러그인 개선 사항

- 국제화 업데이트

- 네트워크 이름에 단일 견적 문자가 포함된 경우 네트워킹 플러그인이 더 이상 충돌하지 않습니다 .

- **foreman-debug** 플러그인이 이제 더 긴 시간 초과로 실행되어**eman-debug** 정보가 완료되지 않음

- 특정 개인 **SSL** 인증서 파일이 더 이상 수집되지 않습니다 **(BZ#1414879)**

targetd 버전 다시 시작 0.8.6

targetd 패키지가 업스트림 버전 **0.8.6**으로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 **targetd** 서비스는 이제 **Python 2** 또는 **Python 3** 런타임 시간에 실행되며 다음 **API**가 추가되었습니다. **initiator_list,access_group_list,access_group_create,access_group_destroy,access_group_init_add,access_group_init_del,access_group_map_list,access_group_map_create, access_group_map_destroy.**

주요 버그 수정 사항은 다음과 같습니다.

- **targetd** 는 이제 **JSON-RPC** 응답 버전 **2.0**을 준수합니다.

- 이제 **export_create API**를 사용하여 동일한 **LUN**을 여러 이니시에이터에 매핑할 수 있습니다.

- 이제 targetd 에서 시작 시 SSL 인증서가 있는지 확인합니다. (BZ#1162381)

shim 버전 12-1로 다시 시작

이번 업데이트를 통해 shim 패키지가 업스트림 버전 12-1로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 32비트 UEFI 펌웨어 및 EFI(Extensible Firmware Interface) 유틸리티에 대한 지원이 추가되었습니다. (BZ#1310766)

rubygem-abrt 버전 0.3.0으로 다시 시작

rubygem-abrt 패키지는 이전 버전에 대해 여러 버그 수정 및 개선 사항을 제공하는 버전 0.3.0을 다시 시작했습니다. 주요 사항:

- Ruby ABRT 핸들러는 이제 uReports, 자동 익명 마이크로 보고를 지원합니다. uReports 를 사용하면 개발자는 애플리케이션 문제에 대해 신속하게 알림을 받고 버그를 수정하고 문제를 더 빠르게 해결할 수 있습니다.

- 이전에는 Ruby 애플리케이션이 Bundler 를 사용하여 종속성을 관리하고 오류가 발생한 경우 Ruby ABRT 처리기의 구성 요소를 로드하는 데 잘못된 논리가 사용되었습니다. 결과적으로 예기치 않은 LoadReport 오류가 적절한 ABRT 보고서 대신 사용자에게 보고되었습니다. 로드 논리가 수정되었으며 Ruby 애플리케이션 오류가 이제 ABRT 를 사용하여 올바르게 처리 및 보고됩니다. (BZ#1418750)

새 패키지: http-parser

새로운 http-parser 패키지는 HTTP 메시지를 구문 분석하기 위한 유틸리티를 제공합니다. 요청과 응답을 모두 구문 분석합니다. parser는 HTTP 성능을 관리하는 애플리케이션에서 사용하도록 설계되었습니다. syscall이나 할당을 생성하지 않으며, 데이터를 버퍼링하지 않으며, 언제든지 중단될 수 있습니다. 아키텍처에 따라 메시지 스트림당 약 40바이트의 데이터만 필요합니다. (BZ#1393819)

모든 기본 POSIX 뮤텍스에 대한 Intel 및 IBM POWER 트랜잭션 메모리 지원

기본 POSIX 뮤텍스는 Intel 및 IBM POWER 트랜잭션 메모리 지원으로 투명하게 대체할 수 있어 잠금 취득 비용을 크게 줄일 수 있습니다. 모든 기본 POSIX 뮤텍스에 대한 트랜잭션 메모리 지원을 활성화하려면 RHEL_GLIBC_TUNABLES=glibc.elision.enable 환경 변수를 1 로 설정합니다. 따라서 일부 애플리케이션의 성능이 향상될 수 있습니다.

개발자는 프로파일링을 사용하여 이 기능을 활성화할지 여부를 결정하여 애플리케이션의 성능을 향상시키는 것이 좋습니다. (BZ#841653, BZ#731835)

glibc 에서 그룹 병합 지원

다른 이름 서비스 모듈의 그룹 멤버를 병합하는 기능이 glibc 에 추가되었습니다. 결과적으로 여러 호스

트에서 중앙 집중식 사용자 액세스 제어 및 그룹 멤버십을 보다 쉽게 관리할 수 있습니다. (BZ#1298975)

glibc 는 IBM POWER9 아키텍처에서 최적화된 문자열 비교 함수 지원

glibc 라이브러리의 문자열 비교 함수 strcmp 및 strncmp 는 IBM POWER9 아키텍처에 최적화되어 있습니다. (BZ#1320947)

Intel SSE, AVX 및 AVX512 기능을 사용하여 동적으로 로드된 라이브러리의 성능 개선

Intel SSE, AVX 및 AVX512 기능을 사용하는 라이브러리용 동적 라이브러리 로드가 업데이트되었습니다. 결과적으로 이러한 라이브러리를 로드하는 동안 성능이 향상되었습니다. 또한 LD_AUDIT 스타일 감사 지원이 추가되었습니다. (BZ#1421155)

elfutils 버전 0.168로 업데이트

elfutils 패키지가 업스트림 버전 0.168로 업그레이드되어 여러 버그 수정 및 개선 사항이 추가되었습니다.

- 이제 eu-readelf 유틸리티의 --symbols 옵션을 사용하면 기호를 표시하는 섹션을 선택할 수 있습니다.
- ELF/DWARF 문자열 테이블 생성을 위한 새로운 함수가 libdw 라이브러리에 추가되었습니다.
- DW_LANG_PL1 상수가 DW_LANG_PLI 로 변경되었습니다. 이전 이름은 계속 사용할 수 있습니다.
- libelf 라이브러리의 gelf_newehdr 및 gelf_newphdr 함수의 반환 유형이 다른 libelf 구현과의 소스 호환성을 위해 void* 로 변경되었습니다. 이러한 변경으로 인해 Red Hat Enterprise Linux에서 지원하는 모든 플랫폼에서 바이너리 호환성이 유지됩니다. (BZ#1400302)

bison 버전 3.0.4로 업데이트

bison 패키지가 업스트림 버전 3.0.4로 업그레이드되어 여러 버그 수정 및 개선 사항이 추가되었습니다.

- 캐럿 오류로 인한 무한한 진단이 수정되었습니다.
- 지정된 경고를 오류로 처리하기 위해 -Werror=CATEGORY 옵션이 추가되었습니다. 경고는 -W 옵션을 사용하여 명시적으로 활성화할 필요가 없습니다.

- 선행 규칙 및 쓸모없는 규칙을 처리하는 데 많은 기능이 개선되었습니다.

또한 이전 버전과의 호환성을 분리하는 다음과 같은 변경 사항이 추가되었습니다.

- YYFAIL,YYLEX_PARAM,YYPARSE_PARAM,yystype, YYLEX_PARAM

- 작업 종료 시 별칭이 누락되면 더 이상 자동으로 추가되지 않습니다.

- autoconf 유틸리티 버전 2.69 및 이전 버전과 함께 Vison 확장을 사용하려면 -Wno-yacc 옵션을 (AM_)YFLAGS 로 전달합니다. (BZ#1306000)

시스템 기본 CA 번들은 Mutt의 컴파일된 기본 설정 또는 구성에서 기본값으로 설정되어 있습니다.

이전에는 TLS/SSL을 통해 새 시스템에 연결할 때 Mutt 이메일 클라이언트에 사용자가 인증서를 저장해야 했습니다. 이번 업데이트를 통해 기본적으로 시스템 CA(인증 기관) 번들이 Mutt 에 설정되어 있습니다. 그 결과 Mutt 은 이제 사용자가 인증서를 승인하거나 거부하도록 요청하지 않고 SSL/TLS를 통해 유효한 인증서가 있는 호스트에 연결합니다. (BZ#1388511)

objdump 혼합 목록 속도

이전에는 DWARF 디버그 정보를 구문 분석하기 위한 BFD 라이브러리가 매우 느렸습니다. BFD 라이브러리는 objdump 툴에서 사용합니다. 그 결과 소스 코드의 혼합 목록을 생성하는 경우 objdump 가 상당히 느려졌습니다. BFD 라이브러리 성능이 향상되었습니다. 결과적으로 objdump 와 혼합된 목록을 생성하는 것이 더 빠릅니다. (BZ#1366052)

fjes 드라이버에서 사람이 읽을 수 있는 출력에 대한 ethtool 지원

fjes 드라이버에서 사람이 읽을 수 있는 레지스터 덤프 출력 형식을 제공하도록 ethtool 유틸리티가 개선되었습니다. 결과적으로 ethtool 사용자는 Fujitsu Extended Socket Network Device 드라이버를 보다 쉽게 검사할 수 있습니다. (BZ#1402701)

ecj 버전 4.5.2로 다시 기반

ecj 패키지가 업스트림 버전 4.5.2로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 버전 8에서 Java 언어에 추가된 기능에 대한 지원이 완료되었습니다. 그 결과 Java 8 기능을 사용한 Java 코드 컴파일이 더 이상 실패하지 않습니다. 여기에는 Java 런타임 환경에서 제공하는 시스템 클래스와 같이 이러한 기능을 사용하여 Java 8 기능을 사용하지 않는 코드가 이러한 기능을 사용하여 참조되는 경우가 포함됩니다. (BZ#1379855)

rhino 버전 1.7R5로 업데이트

rhino 패키지가 업스트림 버전 **1.7R5**로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 정규식을 구문 분석하는 동안 무한 루프의 이전 문제가 수정되었습니다.**Notably, the former problem with an infinite loop while parsing regular expressions has been fixed.** 이전에 이 버그가 발생했을 때 이 버그가 올바르게 작동하는 **applications. (BZ#1350331)**

scap-security-guide oscap-docker 에서 컨테이너 지원

이제 사용자가 **oscap-docker** 유틸리티 및 **SCAP** 보안 가이드를 사용하여 잘못된 양의 결과가 발생하지 않고 컨테이너 또는 컨테이너 이미지의 규정 준수를 평가할 수 있습니다. 파티셔닝과 같은 컨테이너 컨텍스트에서 의미가 없는 테스트(예: 파티션)가 적용되지 않는 값으로 설정되어 있으며 선택한 보안 정책을 사용하여 컨테이너를 스캔할 수 있습니다. **(BZ#1404392)**

8장. 데스크탑

GNOME rebased to 버전 3.22.3

GNOME 데스크탑이 업스트림 버전 3.22.3으로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 반복된 데스크탑 알림
- 세계 시계 및 미디어 플레이어와 내장된 통합
- 화면 밝기 자동 조정 (통합 광 센서가 있는 시스템용)
- 많은 애플리케이션에서는 키보드 바로 가기를 문서화하는 표준 대화 상자를 지원합니다.
- 여러 설정 패널의 개선 사항(서식, 마우스, 터치패드, 키보드 바로 가기)
- 한 번에 여러 파일의 이름을 변경할 수 있는 옵션
- 압축 파일 및 Google 드라이브에 대한 기본 제공 지원
- 휴지통에 대한 실행 취소 지원 (BZ#1383353)

Xorg -x11-drv-libinput 드라이버가 X.Org 입력 드라이버에 추가되었습니다.

xorg-x11-drv-libinput X.Org 드라이버는 낮은 수준의 libinput 라이브러리를 위한 래퍼 드라이버입니다. 이번 업데이트에서는 X.Org 입력 드라이버에 드라이버가 추가되었습니다. xorg-x11-drv-libinput 을 설치한 후 xorg-x11-drv-synaptics 드라이버를 제거하고 libinput 에서 제공하는 개선된 입력 장치 처리에 대한 액세스를 얻을 수 있습니다. (BZ#1413811)

일부 Intel 및 nVidia 하드웨어의 기본 드라이버 변경

이 변경 사항은 다음과 같습니다.

- 4th Generation Intel Core Processors 이상
- NVIDIA GeForce 8 하드웨어 이상

기본 DDX 드라이버가 xf86-video-modesetting 으로 변경되었습니다.

이전에는 nVidia 및 Intel 하드웨어에서 각각 xf86-video-nouveau 및 xf86-video-intel 이 있었습니다. (BZ#1404868)

dconf-editor 가 이제 별도의 패키지로 제공됨

업스트림 dconf 팀에는 dconf-editor 를 자체 패키지로 분할했습니다. 이 릴리스에는 이러한 변경 사항이 반영되어 있습니다.

또한 사용자 인터페이스는 버전 3.22에서 재설계되었습니다.

- 왼쪽의 트리 보기가 제거되었습니다.
- 이제 키와 디렉터리가 동일한 창에 표시됩니다.
- 계층 구조로 돌아가는 기능은 header-bar에 표시된 경로로 이동했습니다. (BZ#1388931)

9장. 파일 시스템

OverlayFS 파일 시스템에서 SELinux 보안 레이블이 지원됨

이번 업데이트를 통해 OverlayFS 파일 시스템에서 SELinux 보안 레이블을 지원합니다. OverlayFS 스토리지 드라이버와 함께 Docker 컨테이너를 사용하는 경우 더 이상 컨테이너에 대한 SELinux 지원을 비활성화하도록 Docker를 구성할 필요가 없습니다. (BZ#1297929)

NFSoRDMA 서버가 완전히 지원됩니다.

이전에 기술 프리뷰로 제공된 NFS(NFSoRDMA) 서버가 Red Hat Enterprise Linux 클라이언트에서 액세스하는 경우 완전히 지원됩니다. NFSoRDMA에 대한 자세한 내용은 Red Hat Enterprise Linux 7 스토리지 관리 가이드의 다음 섹션을 참조하십시오. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Storage_Administration_Guide/index.html#nfs-rdma (BZ#1400501)

E gressIP에서 amd 형식 맵의 찾아보기 옵션 지원

Sun 형식 맵의 찾아보기 기능을 사용하면 자동 마운트를 마운트할 수 있는 자동 마운트 지점을 사용할 수 있으며 이제 EgressIP amd 형식 맵에서도 사용할 수 있습니다.

이제 마스터 맵에 해당 항목을 추가하지 않고도 자동 마운트 지점을 amd.md에서 구성하는 것과 동일한 방식으로 amd 형식 마운트에 대한 mount point(마운트) 구성에 마운트 지점 섹션을 추가할 수 있습니다. 결과적으로 공유 멀티 벤더 환경 내에서 EgressIP 마스터 맵에서 호환되지 않는 마스터 맵 항목이 없는 것을 방지할 수 있습니다.

browsable_dirs 옵션은 EgressIP [amd] 설정 섹션에서 또는 amd 마운트 지점 섹션에 사용할 수 있습니다. amd 유형 자동 맵 항목의 browsable 및 utimeout 맵 옵션도 사용할 수 있습니다.

browsable_dirs 옵션은 yes 또는 no 로만 설정할 수 있습니다. (BZ#1367576)

로그를 더 쉽게 검색하기 위해 이제 EgressIP 에서 마운트 요청 로그 항목의 식별자를 제공합니다.

사용량이 많은 사이트의 경우 마운트 문제를 검사할 때 특정 마운트 시도에 대한 로그 항목을 식별하기 어려울 수 있습니다. 로그에서 많은 활동을 기록한 경우 항목을 다른 동시 마운트 요청 및 활동과 혼합하는 경우가 많습니다. 이제 EgressIP 구성에 요청 로그 항목을 마운트하기 위해 마운트 요청 로그 식별자를 추가할 경우 특정 마운트 요청에 대한 항목을 빠르게 필터링할 수 있습니다. 새 로깅은 기본적으로 꺼져 있으며 EgressIP .conf 파일에 설명된 대로 use_mount_request_log_id 옵션으로 제어됩니다. (BZ#1382093)

IBM z Systems의 GFS2가 SSI 환경에서 지원됨

Red Hat Enterprise Linux 7.4부터 IBM z Systems의 GFS2(silient Storage on the s390x add-on)는 여러 중앙 전자기(CEC) 환경에서 z/VM 단일 시스템 이미지(SSI) 환경에서 지원됩니다. 이를 통해 LPAR(Logical partitions) 또는 CEC를 다시 시작할 때에도 클러스터를 가동할 수 있습니다. HA(고가용

성) 클러스터링의 실시간 요구 사항으로 인해 실시간 마이그레이션이 지원되지 않습니다. IBM z Systems의 노드 4개 노드의 최대 노드 제한은 여전히 적용됩니다. IBM z 시스템의 고가용성 및 탄력적 스토리지 구성에 대한 자세한 내용은 https://access.redhat.com/articles/1543363 을 참조하십시오. (BZ#1273401)

gfs2-utils 버전 3.1.10으로 다시 시작

gfs2-utils 패키지가 업스트림 버전 3.1.10으로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 이 업데이트는 다음을 제공합니다.

- fsck.gfs2 명령의 다양한 검사 및 성능 개선
- mkfs.gfs2 명령에서 odd block device geometry를 더 잘 처리합니다.
- gfs2_edit savemeta leaf chain block handling 버그 수정
- 사용자 지정 함수 대신 libuuid 라이브러리로 UUID를 처리합니다.
- 프로파일링을 위해 새로운 --enable-gprof 구성 옵션입니다.
- 설명서 개선 사항. (BZ#1413684)

FUSE는 이제 lseek 호출에서 SEEK_HOLE 및 SEEK_DATA 지원

이번 업데이트에서는 FUSE(사용자 공간) lseek 시스템 호출에 대한 SEEK_HOLE 및 SEEK_DATA 기능을 제공합니다. 이제 FUSE lseek 를 사용하여 SEEK_DATA 또는 SEEK_HOLE 을 사용하여 데이터가 포함된 파일의 다음 위치로 파일 오프셋을 조정할 수 있습니다. (BZ#1306396)

NFS 서버에서 제한된 copy-offload 지원

NFS 서버 측 복사 기능을 사용하면 NFS 클라이언트에서 NFS 클라이언트를 통해 네트워크를 통해 데이터를 다시 전송할 필요 없이 동일한 NFS 서버의 동일한 파일 시스템에 있는 두 파일 간에 파일 데이터를 복사할 수 있습니다. NFS 프로토콜은 여러 파일 시스템 또는 서버 간에도 복사할 수 있지만 Red Hat Enterprise Linux 구현에서는 현재 이러한 작업을 지원하지 않습니다. (BZ#1356122)

SELinux는 GFS2 파일 시스템과 함께 사용할 수 있도록 지원됩니다.

이제 GFS2 파일 시스템과 함께 사용할 수 있도록 SELinux(Security Enhanced Linux)가 지원됩니다. SELinux를 GFS2와 함께 사용하면 성능이 저하될 수 있으므로 SELinux가 강제 모드에서도 시스템에서 GFS2와 함께 SELinux를 사용하지 않도록 선택할 수 있습니다. 이 구성 방법에 대한 자세한 내용은

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Global_File_System_2/index.html 을 참조하십시오. (BZ#437984)

NFSoRDMA 클라이언트 및 서버에서 Kerberos 인증 지원

이번 업데이트에서는 NFS over RDMA(NFSORDMA) 클라이언트 및 서버에 대한 Kerberos 인증 지원이 추가되어 NFSoRDMA 기능을 사용하여 KnativeServing5i 및 KnativeServing5p 인증을 사용할 수 있습니다. 이제 NFSoRDMA와 Kerberos를 사용하여 각 RPC(Remote Procedure call) 트랜잭션의 보안 인증을 사용할 수 있습니다. NFSoRDMA에서 Kerberos를 사용하려면 nfs-utils 패키지 버전 1.3.0-0.36 이상이 설치되어 있어야 합니다. (BZ#1401797)

RPC.idmapd 는 이제 DNS에서 NFSv4 ID 도메인 가져오기 지원

ID 매핑에 사용되는 NFS 도메인 이름을 이제 DNS에서 검색할 수 있습니다. 도메인 변수가 /etc/idmapd.conf 파일에 설정되지 않은 경우 DNS가 _nfsv4idmapdomain 텍스트 레코드를 검색하도록 쿼리됩니다. 값을 찾으면 NFS 도메인으로 사용됩니다. (BZ#980925)

NFSv4.1은 이제 기본 NFS 마운트 프로토콜입니다.

이번 업데이트 이전에는 NFSv4.0이 기본 NFS 마운트 프로토콜이었습니다. NFSv4.1에서는 세션, pNFS, 병렬 OPEN 및 세션 트렁크와 같은 NFSv4.0에 비해 상당한 기능 개선을 제공합니다. 이번 업데이트를 통해 NFSv4.1은 기본 NFS 마운트 프로토콜입니다.

이미 마운트 프로토콜 마이너 버전을 지정한 경우 이 업데이트로 인해 동작이 변경되지 않습니다. 이 업데이트에서는 서버가 NFSv4.1을 지원하는 경우 특정 마이너 버전 없이 NFSv4를 지정한 경우 동작이 변경됩니다. 서버가 NFSv4.0만 지원하는 경우 마운트는 NFSv4.0 마운트로 유지됩니다. 0 을 마이너 버전으로 지정하여 원래 동작을 유지할 수 있습니다.

- 마운트 명령줄에서,
- /etc/fstab 파일에서
- 또는 /etc/nfsmount.conf 파일에서 다음을 수행합니다. (BZ#1375259)

nfs-utils 구성 옵션은 nfs.conf에서 중앙 집중화되었습니다.

이번 업데이트를 통해 nfs-utils 는 nfs.conf 파일에서 중앙 집중화된 구성을 사용하며, 이는 각 nfs-utils 프로그램의 스탠자로 구성됩니다. 각 nfs-utils 프로그램은 파일에서 직접 구성을 읽을 수 있으므로 systemctl restart nfs-config.service 명령을 더 이상 사용할 필요가 없지만 특정 프로그램만 다시 시작합니다. 자세한 내용은 nfs.conf(5) 매뉴얼 페이지를 참조하십시오.

이전 릴리스와의 호환성을 위해 이전 /etc/sysconfig/nfs 구성 방법을 계속 사용할 수 있습니다. 그러나 /etc/sysconfig/nfs 및 /etc/nfs.conf 파일에서 구성 설정을 지정하지 않는 것이 좋습니다. (BZ#1418041)

NFSv4.1 마운트의 잠금 성능이 특정 워크로드의 경우 향상되었습니다.

NFSv4 클라이언트는 서버를 간격으로 폴링하여 경합에서 잠금을 확보합니다. 따라서 NFSv4의 컨텐츠 잠금 성능이 NFSv3의 성능보다 느립니다.

CB_NOTIFY_LOCK 작업이 NFS 클라이언트 및 서버에 추가되어 NFSv4.1 이상에서는 서버가 잠금에서 대기 중인 클라이언트로 다시 호출할 수 있습니다.

이번 업데이트에서는 특정 워크로드에 대해 NFSv4.1 마운트의 콘텐츠 잠금 성능이 향상되었습니다. 더 긴 잠금 경합 시간에 대해 성능이 향상되지 않을 수 있습니다. (BZ#1377710)

Red Hat Ceph Storage 3에서 CephFS 커널 클라이언트가 완전히 지원됩니다.

Ceph File System(CephFS) 커널 모듈을 사용하면 Red Hat Enterprise Linux 노드에서 Red Hat Ceph Storage 클러스터에서 Ceph 파일 시스템을 마운트할 수 있습니다. Red Hat Enterprise Linux의 커널 클라이언트는 Red Hat Ceph Storage에 포함된 Filesystem in Userspace(FUSE) 클라이언트에 대한 보다 효율적인 대안입니다. 현재 커널 클라이언트는 CephFS 할당량을 지원하지 않습니다.

CephFS 커널 클라이언트는 Red Hat Enterprise Linux 7.3에서 기술 프리뷰로 소개되었으며 Red Hat Ceph Storage 3 릴리스부터 CephFS가 완전히 지원됩니다.

자세한 내용은 Red Hat Ceph Storage 3: https://access.redhat.com/documentation/en-us/red_hat_ceph_storage/3/html/ceph_file_system_guide/ 의 Ceph 파일 시스템 가이드를 참조하십시오. (BZ#1626527)

10장. 하드웨어 활성화

하드웨어 유틸리티 도구가 최근 릴리스된 하드웨어 식별

이번 업데이트 이전에는 사용되지 않는 ID 파일로 인해 최근에 컴퓨터에 연결된 하드웨어가 알 수 없는 것으로 보고되었습니다. 이 버그를 해결하기 위해 PCI, USB 및 벤더 장치 식별 파일이 업데이트되었습니다. 그 결과 하드웨어 유틸리티 도구가 최근에 릴리스된 하드웨어를 올바르게 식별합니다. (BZ#1386133)

새로운 Wacom 드라이버를 사용하여 향후 버전 지원

이번 업데이트를 통해 최근 출시 날짜 및 출시 예정인 알바티스를 지원하기 위해 새로운 Wacom 드라이버가 도입되었으며, 현재 드라이버는 이전에 출시된 알약을 계속 지원하고 있습니다.

주요 기능:

- Wacom 27QHT (Wacom 27QHT)가 지원됩니다.
- ExpressKey Remote(BZ#1385026)

Wacom 커널 드라이버에서 이제 bookinfoPad X1 Yoga 연락처 화면 지원

이번 업데이트에서는 Wacom 커널 드라이버에 대해 thinkPad X1 Yoga contact 화면에 대한 지원이 추가되었습니다. 따라서 이러한 시스템에서 Red Hat Enterprise Linux 7을 실행할 때 해당 화면을 올바르게 사용할 수 있습니다. (BZ#1388646)

Wacom Cintiq 27 QHDT 알리브레이션 (Wacom Cintiq 27 QHDT 알)에 연락처가 추가되었습니다.

이번 업데이트에서는 Wacom Cintiq 27 QHDT 알약 기능을 지원하는 기능이 추가되어 시스템에서 Red Hat Enterprise Linux 7을 실행할 때 해당 화면을 올바르게 사용할 수 있습니다. (BZ#1391668)

AMDGPU 는 이제 남아메리카 주,볼카 니티스 및 북아메리카 칩셋을 지원합니다.

남아프리카 공화국,시 우 오카 라우 (Row canic company s) 및 북아메리카 칩셋에 대한 지원이 추가되었습니다. AMDGPU 그래픽 드라이버는 최신 AMD/ATI Radeon 그래픽 카드를 위한 차세대 오픈 소스 그래픽 드라이버입니다. 이는 남부의 제도(남아시아 주), 볼카니아 주, 북아메리카의 칩셋을 기반으로 합니다. linux-firmware 패키지에서 제공하는 카드의 적절한 펌웨어 또는 마이크로 코드를 설치해야 합니다. (BZ#1385757)

AMD 모바일 그래픽에 대한 지원 추가

Polaris 아키텍처를 기반으로 하는 AMD 모바일 그래픽 지원이 추가되었습니다. 파라 리스 아키텍처는 북아메리카 칩셋 을 기반으로 합니다. linux-firmware 패키지에서 제공하는 카드의 적절한 펌웨어 또는

마이크로 코드를 설치해야 합니다. (BZ#1339127)

Netronome NFP 장치가 지원됩니다.

이번 업데이트를 통해 **nfp** 드라이버가 **Linux** 커널에 추가되었습니다. 그 결과 **Netronome Network Flow Processor (Netronome NFP 4000/6000 VF)** 장치가 이제 **Red Hat Enterprise Linux 7**에서 지원됩니다. (BZ#1377767)

nvme-cli 버전 **1.3**으로 다시 시작

nvme-cli 유틸리티는 **NVMe(Nonvolatile Memory Express)** 지원을 포함하는 버전 **1.3**으로 업데이트되었습니다. **NVMe**에 대한 지원을 통해 **RDMA(Remote Direct Memory Access)**를 통해 대상을 찾고 이러한 대상에 연결할 수 있습니다. (BZ#1382119)

대기 중인 스핀 잠금이 **Linux** 커널에 구현됨

이번 업데이트에서는 커널의 스핀 잠금이 **AMD64** 및 **Intel 64** 아키텍처의 대기 중인 스핀 잠금으로 변경되었습니다. 대기 중인 스핀 클래시는 티켓 회전보다 더 확장 가능합니다. 그 결과 특히 많은 **CPU**가 많은 **SMP(Symmetric Multi Processing)** 시스템에서 시스템 성능이 향상되었습니다. **CPU** 수가 늘어남에 따라 성능이 더 선형으로 향상되었습니다. 이러한 변경으로 인해 **Red Hat Enterprise Linux 7**에 빌드된 커널 모듈이 이전 릴리스의 커널에서 로드되지 않을 수 있습니다. **7.4** 미만의 **RHEL(Red Hat Enterprise Linux)** 버전에서 릴리스된 커널 모듈은 **RHEL 7.4**에서 릴리스된 커널에서 로드될 수 있습니다. (BZ#1241990)

Intel Xeon v2 서버 지원

Intel Xeon v2 서버를 지원하도록 **Intel rapl** 드라이버가 업데이트되었습니다. (BZ#1379590)

Intel Platform Controller Hub [PCH] 장치에 대한 추가 지원

Intel Xeon Processor E3 v6 Family CPU에서 새로운 **Intel PCH** 하드웨어에 대한 지원을 활성화하도록 커널이 업데이트되었습니다. (BZ#1391219)

IBM Power 및 **s390x**에서 하드웨어 가속 **zLib**를 사용할 수 있도록 **genwqe-tools** 포함

genwqe-tools 패키지를 사용하면 **IBM Power** 및 **s390x** 하드웨어 사용자가 **zLib** 압축 및 압축 해제 프로세스에 **RuntimeClass** 기반 **PCIe** 카드를 사용할 수 있습니다.

이러한 도구는 **RFC1950, RFC1951** 및 **RFC1952** 준수 하드웨어를 사용하여 성능을 향상시킬 수 있습니다. (BZ#1275663)

librtas 버전 **2.0.1**로 업데이트

librtas 패키지가 업스트림 버전 **2.0.1**로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 이 업데이트에서는 제공된 라이브러리의 **soname**을 변경합니다. **librtas.so.1**

은 librtas.so.2 로 변경되고 librtasevent.so.1 이 librtasevent.so.2 로 변경됩니다. (BZ#1380656)

NFP 드라이버

NFP(Network Flow Processor) 드라이버가 Linux 커널 버전 4.11에서 백포트되었습니다. 이 드라이버는 Netronome NFP4000 및 고급 이더넷 NIC로 작동하는 NFP6000 기반 카드를 지원합니다. 드라이버는 SR-IOV 물리적 및 가상 함수 모두에서 작동합니다. (BZ#1406197)

Nouveau에서 최신 NVIDIA 카드 활성화

이번 업데이트에는 Pascal 플랫폼을 기반으로 하는 고급 NVIDIA 카드가 올바르게 작동하도록 하는 지원 코드가 포함되어 있습니다. (BZ#1330457)

Wacom ExpressKey Remote 지원

이제 Red Hat Enterprise Linux 7에서 Wacom ExpressKey Remote(EKR)가 지원됩니다. EKR은 바로 가기, 메뉴 및 명령에 액세스할 수 있는 외부 장치입니다. (BZ#1346348)

Wacom Cintiq 27 QHD에서 ExpressKey Remote 지원

이번 업데이트를 통해 Wacom Cintiq 27 QHD 알약은 ExpressKey Remote (EKR)를 지원합니다. EKR은 바로 가기, 메뉴 및 명령에 액세스할 수 있는 외부 장치입니다. (BZ#1342990)

11장. 설치 및 부팅

Anaconda 를 사용하면 **RAID** 청크 크기를 설정할 수 있습니다.

이번 업데이트를 통해 사용자는 **kickstart** 파일에서 **raid** 유틸리티의 **--chunksize** 매개변수를 설정하여 **RAID** 스토리지의 청크 크기를 **KiB**로 지정할 수 있습니다. **--chunksize** 매개변수를 사용하면 기본 값이 재정의됩니다. 결과적으로 새 청크 크기에서 음수 성능이 기본값이 영향을 미칠 수 있습니다. **(BZ#1332316)**

Anaconda 텍스트 모드에서 **IPoIB** 인터페이스 지원

이번 업데이트에서는 텍스트 모드에서 수동 설치 중에 **IP over InfiniBand (IPoIB)** 네트워크 인터페이스에 대한 지원이 추가되었습니다. **IPoIB** 인터페이스 상태 정보를 보고 인터페이스 구성을 변경할 수 있습니다. **(BZ#1366935)**

inst.debug 를 사용하면 **Anaconda** 설치 문제를 보다 편리하게 디버깅할 수 있습니다.

이번 업데이트에서는 **inst.debug** 부팅 옵션을 사용하여 **Anaconda** 설치를 시작하여 시스템의 초기 상태와 관련된 로그를 저장할 수 있는 기능이 추가되었습니다. 이 옵션은 **/tmp/pre-anaconda-logs/** 디렉터리에 **lsblk,dmesg** 및 **lvmdump** 인 **3**개의 추가 로그를 저장하여 설치 중에 발생한 문제를 보다 편리하게 디버깅할 수 있습니다. **(BZ#1255659)**

Kickstart 설치 실패에서 **%onerror** 스크립트가 자동으로 트리거

이번 개선된 기능을 통해 **Anaconda** 설치에 실패하면 **Kickstart** 파일의 **%onerror** 섹션이 실행됩니다. 스크립트는 추가 검사를 위해 자동으로 로그를 수집하는 데 사용할 수 있습니다. 이 업데이트의 결과 설치 중에 역추적 또는 다른 치명적인 오류가 발생하면 설치 프로그램에서 **%onerror** 스크립트 및 **%traceback** 스크립트에서 오류가 **traceback**으로 발생했는지 확인합니다. **(BZ#1412538)**

이제 설치를 시작하기 전에 **Anaconda** 에서 네트워크를 사용할 수 있을 때까지 기다릴 수 있습니다.

일부 환경에서는 첫 번째 **DHCP** 요청이 실패할 것으로 예상됩니다. 이전 버전에서는 첫 번째 **DHCP** 오류로 인해 **Anaconda** 에서 설치를 진행하여 특히 연결을 수동으로 설정할 수 없는 자동 설치 문제가 발생할 수 있었습니다. 이번 업데이트에서는 새로운 **Anaconda** 부팅 옵션인 **inst.waitfornet=X** 가 도입되어 설치 프로그램이 네트워크 연결을 진행하기 전에 **X** 초 동안 대기하도록 강제 적용합니다. 연결이 설정된 후 또는 지정된 시간 간격이 경과한 후에 설치가 계속됩니다. **(BZ#1315160)**

설치 실패를 방지하기 위해 **stage2** 또는 **Kickstart** 파일의 여러 네트워크 위치를 지정할 수 있습니다.

이번 업데이트에서는 **stage2** 및 **Kickstart** 파일의 네트워크 위치와 함께 여러 **inst.stage2** 및 **inst.ks** 부팅 옵션을 지정할 수 있습니다. 이렇게 하면 요청된 파일에 도달할 수 없는 상황이 발생하지 않으며 **stage2** 또는 **Kickstart** 파일이 있는 연결된 서버에 액세스할 수 없기 때문에 설치에 실패합니다.

새 업데이트를 사용하면 여러 위치를 지정하면 설치 실패를 방지할 수 있습니다. 정의된 모든 위치가 **URL**, 즉 **HTTP,HTTPS** 또는 **FTP** 인 경우 요청된 파일을 성공적으로 가져올 때까지 순차적으로 시도됩니

다. URL이 아닌 위치가 있는 경우 마지막으로 지정된 위치만 시도합니다. 나머지 위치는 무시됩니다. (BZ#1391724)

Kickstart 파일의 autopart --nohome 은 자동 파티션에서 /home/ 생성을 비활성화합니다.

이번 업데이트에서는 kickstart 파일의 autopart 명령에 --nohome 옵션이 추가되어 /home/ 파티션의 자동 생성을 비활성화합니다. 이번 개선된 기능을 통해 /home/ 파티션을 되돌려야 하는 경우 수동 파티셔닝을 수행할 필요가 없습니다. 업데이트 결과 파티셔닝이 자동으로 완료되면 /home 파티션이 생성되지 않습니다. (BZ#663099)

하드 디스크 드라이브 및 USB가 활성화된 드라이버 디스크 로드

이번 업데이트를 통해 네트워크 또는 initrd에서 드라이버 디스크를 로드하는 대신 하드 디스크 드라이브 또는 유사한 장치에서 드라이버 디스크를 로드할 수 있습니다. 설치는 kickstart 또는 부팅 옵션을 사용하여 진행할 수 있습니다.

절차는 다음과 같습니다.

1. 하드 디스크 드라이브, USB 또는 유사한 장치에 드라이버 디스크를 로드합니다.

2. 레이블(예: DD)을 이 장치로 설정합니다.

알림:

Kickstart 설치의 경우 다음을 추가합니다.

```
driverdisk LABEL=DD:/e1000.rpm
```

Kickstart 파일에 추가합니다.

부팅 옵션의 경우 설치를 시작합니다.

```
inst.dd=hd:LABEL=DD:/dd.rpm
```

를 부팅 인수로서 사용합니다.

Kickstart와 부팅 옵션 모두에서 DD 를 특정 레이블로 바꾸고 dd.rpm 을 특정 이름으로 교체합니다. 하드 디스크 드라이브를 지정하려면 LABEL 대신 inst.repo 명령에서 지원하는 모든 항목을 사용하십시오. kickstart driverdisk 명령의 LABEL 을 지정하는 인수에는 영숫자가 아닌 문자를 사용하지 마십시오. (BZ#1377233)

LVM 씬 풀의 자동 파티션 동작 변경

이전에는 Kickstart 또는 대화형 설치, 예약된 크기의 20 %를 사용하든 설치에서 만들거나 사용한 모든 LVM(Logical Volume Management) 씬 풀입니다.

이번 업데이트에서는 다음과 같은 변경 사항이 추가되었습니다.

- 자동 파티셔닝을 사용하여 LVM 씬 풀을 생성하는 경우 볼륨 그룹 크기의 20 %가 예약되며 최소 1GiB 및 최대 100GiB가 사용됩니다.

- Kickstart 파일에서 logvol --thinpool --grow 명령을 사용하는 경우 thin 풀이 가능한 최대 크기로 증가하므로 볼륨 그룹에 공간이 남아 있지 않습니다. 이 경우 volgroup --reserved-space 또는 volgroup --reserved-percent 명령을 사용하여 볼륨 그룹에 일부 공간을 예약하는 것이 좋습니다. (BZ#1131247)

32 비트 부트 로더는 이제 UEFI에서 64 비트 커널을 부팅 할 수 있습니다

이번 업데이트에서는 UEFI 펌웨어가 있는 시스템에서 grub2-i386-efi 와 같은 32비트 부트 로더를 사용하여 64비트 커널을 부팅할 수 있습니다. (BZ#1310775)

Lorax는 이제 SSL 오류를 무시할 수 있습니다.

이전에는 lorax 툴에서 자체 서명된 인증서가 있는 HTTPS 리포지토리를 사용할 수 없었습니다. 이렇게 하려고 하면 계속할 방법이 없는 오류가 발생했습니다. 이번 업데이트에서는 --noverifyssl 명령줄 옵션이 유틸리티에 추가되어 서버 인증서 확인을 생략하고 오류를 우회할 수 있습니다. (BZ#1430483)

shim-signed 버전 12로 다시 시작

이번 업데이트를 통해 shim-signed 패키지가 업스트림 버전 12로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 32비트 UEFI 펌웨어 및 EFI(Extensible Firmware Interface) 유틸리티 지원이 추가되었습니다. (BZ#1310764)

gnu-efi 버전 3.0.5.-9로 업데이트

이번 업데이트를 통해 gnu-efi 패키지가 업스트림 버전 3.0.5.-9로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항이 추가되었습니다. 특히 32비트 UEFI 펌웨어 및 EFI(Extensible Firmware Interface) 유틸리티에 대한 지원이 추가되었습니다. (BZ#1310782)

killproc() 및 status()에 대해 이전 버전과의 호환성 활성화

이번 업데이트 이전에는 Red Hat Enterprise Linux 7에 제공된 /etc/rc.d/init.d/functions 스크립트에는 Red Hat Enterprise Linux 6의 일부 기능이 없었습니다. /etc/rc.d/init.d/functions 파일의 killproc() 및 status() 함수에 -b 옵션에 대한 지원을 추가하도록 initscripts 패키지가 업데이트되었습니다. 또한 Red Hat Enterprise Linux 6의 이전 버전과의 호환성을 실현하고 Red Hat Enterprise Linux 6에서 Red Hat Enterprise Linux 7로 업그레이드를 수행할 때 발생하는 회귀 문제를 방지합니다. (BZ#1428935)

DHCP_FQDN 을 사용하면 시스템의 정규화된 도메인 이름을 지정할 수 있습니다.

이전에는 ifcfg 인터페이스 구성 파일에서 시스템의 호스트 이름을 지정하는 데 DHCP_HOSTNAME 지시문을 사용해야 했습니다. 새로운 initscripts DHCP_FQDN 지시문을 사용하면 시스템의 정규화된 도메인 이름도 지정할 수 있습니다. 이는 DHCP_HOSTNAME 지시문에 보완됩니다. DHCP_HOSTNAME 및 DHCP_FQDN 이 모두 지정된 경우 DHCP_FQDN 만 사용됩니다. (BZ#1260552)

이제 설치 프로세스 중에 씬 논리 볼륨 스냅샷을 만들 수 있습니다.

이번 업데이트에서는 새 Kickstart 명령인 스냅샷에 대한 지원이 추가되었습니다. 이 명령을 사용하면 설치 전이나 설치 후 LVM 씬 볼륨 스냅샷을 만들 수 있습니다. 사용 가능한 옵션은 다음과 같습니다.

- <VG_NAME>/<lv_name > 볼륨 그룹과 논리 볼륨의 이름을 지정하여 스냅샷을 만듭니다.
- --name= 스냅샷의 이름을 지정합니다.
- --when= 설치가 시작되기 전에 스냅샷을 작성하려는 경우 사전 설치를 지정합니다. 따라서 업그레이드 전에 시스템 상태를 유지하려면 유용할 수 있습니다. 또는 설치 후 추가 변경 작업을 수행하기 전에 새로 설치된 시스템의 스냅샷을 작성하도록 지정합니다.

세 가지 옵션은 모두 필수입니다. 또한 설치 전과 후 또는 여러 논리 볼륨의 스냅샷을 찍으려면 단일 Kickstart 파일에서 이 명령을 여러 번 사용하여 스냅샷을 만들 수 있습니다. 각 -name= 매개변수가 이 작업을 수행할 때 고유한 이름을 지정했는지 확인합니다. (BZ#1113207)

12장. 커널

RHEL 7.4의 커널 버전

Red Hat Enterprise Linux 7.4는 커널 버전 3.10.0-693과 함께 배포됩니다. (BZ#1801759)

NVMe 드라이버가 커널 버전 4.10으로 다시 시작

NVM-Express 커널 드라이버가 업스트림 커널 버전 4.10으로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 가장 주목할 만한 변경 사항은 기존 RDMA NIC(Infiniband, RoCE, iWARP) 및 기존 NVMe SSD를 사용하는 초기 NVMe-over-Fabrics 전송 구현이 드라이버에 추가되었지만 DIF/DIX 및 멀티패스 지원은 포함되지 않습니다. (BZ#1383834)

crash 버전 7.1.9로 업데이트

이번 업데이트를 통해 crash 패키지가 업스트림 버전 7.1.9로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항이 추가되었습니다. (BZ#1393534)

이제 IBM Power EgressIP 3.0에 대한 vmcore 덤프 분석

크래시 유틸리티는 IBM Power#189 버전 3.0 아키텍처와 관련된 커널 페이지 테이블의 변경 사항과 일치하도록 업데이트되었습니다. 그 결과 크래시 유틸리티는 IBM Power#189 3.0 시스템에서 커널의 vmcore 덤프를 분석할 수 있게 되었습니다. (BZ#1368711)

crash IBM Power 및 IBM Power의 little-endian 변형용 업데이트

IBM Power Systems 및 IBM Power Systems의 little-endian 변형을 지원하도록 crash 패키지가 업데이트되었습니다. 이러한 패키지는 실시간 시스템을 조사하는 데 사용할 수 있는 자동 분석 도구인 핵심 분석 모음과 kexec-tools 패키지 또는 Red Hat Enterprise Linux 커널에서 생성한 커널 코어 덤프를 제공합니다. (BZ#1384944)

memkind 버전 1.3.0으로 업데이트

memkind 라이브러리가 버전 1.3.0으로 업데이트되어 이전 버전에 대해 여러 버그 수정 및 개선 사항을 제공합니다.

주요 변경 사항은 다음과 같습니다.

- 로깅 메커니즘이 도입되었습니다.
- 하드웨어 Locality(hwloc)가 통합되었으며 --with-hwloc 옵션을 사용하여 설정할 수 있습니다.

- libmemkind.so에 의해 노출된 기호가 정리되었습니다. 예를 들어 libnuma 및 jemalloc 은 더 이상 노출되지 않습니다.

- AutoHBW 파일이 /memkind/autohbw/ 디렉토리로 이동되었으며 코드가 리팩토링되고 테스트가 적절한 시나리오에 추가되었습니다.

- memkind 에 보안을 강화하는 플래그가 추가되었습니다. --disable-secure 구성 시간 옵션을 사용하여 플래그를 해제할 수 있습니다.

- jemalloc 의 구성이 사용되지 않는 기능을 해제하도록 변경되었습니다.

- 여러 기호가 더 이상 사용되지 않습니다. 자세한 내용은 더 이상 사용되지 않는 기능 부분을 참조하십시오. (BZ#1384549)

jitter Entropy RNG가 커널에 추가되었습니다.

이번 업데이트에서는 **Linux** 커널에 대한 **CPU** 타이밍 차이를 통해 엔트로피를 수집하는 **Jitter Entropy Random Number Generator(RNG)**가 추가되었습니다. 이 **RNG**는 기본적으로 **algif_rng** 인터페이스를 통해 사용할 수 있습니다. 생성된 번호는 **/dev/random** 파일을 통해 커널에 다시 추가할 수 있으므로 다른 **/dev/random** 사용자에게 이러한 숫자를 사용할 수 있습니다. 결과적으로 운영 체제에는 이제 사용 가능한 엔트로피 소스가 더 많습니다. (BZ#1270982)

/dev/random 에서 **urandom** 풀 초기화에 대한 알림 및 경고를 표시합니다.

이번 업데이트에서는 차단되지 않은 풀(**/dev/urandom**에 의해 사용)이 초기화될 때 메시지를 출력하도록 임의의 드라이버(**/dev/random**)가 수정되었습니다. (BZ#1298643)

fjes 버전 **1.2**로 업데이트

fjes 드라이버가 버전 **1.2**로 업데이트되었으며 이전 버전에 대한 버그 수정 및 개선 사항이 많이 포함되어 있습니다. (BZ#1388716)

사용자 이름 공간에 대한 전체 지원

Red Hat Enterprise Linux 7.2에서 기술 프리뷰로 도입된 사용자 이름 공간(사용자 이름 공간)이 이제 완전히 지원됩니다. 이 기능은 호스트와 컨테이너 간 격리를 개선하여 **Linux** 컨테이너를 실행하는 서버에 추가적인 보안을 제공합니다. 컨테이너 관리자는 더 이상 호스트에서 관리 작업을 수행할 수 없으므로 보안이 향상됩니다.

user.max_user_namespaces 의 기본값은 **0** 입니다. **0**이 아닌 값으로 설정하면 혼동되는 애플리케이션이 중지됩니다. 일반 작업 과정에서 값을 다시 볼 필요가 없도록 **user.max_usernamespaces** 를

15000 과 같은 큰 값으로 설정하는 것이 좋습니다. (BZ#1340238)

makedumpfile 버전 1.6.1로 업데이트

makedumpfile 패키지는 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공하는 kexec-tools 2.0.14 rpm의 일부로 업스트림 버전 1.6.1로 업그레이드되었습니다. (BZ#1384945)

Q AT 최신 업스트림 버전으로 업데이트

CloudEventt 드라이버가 최신 업스트림 버전으로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항이 추가되었습니다.

주요 버그 수정 및 개선 사항:

- Diffie-Hellman (DH) 소프트웨어에 대한 지원 추가
- ECDH(Ellliptic Curve Diffie-Hellman) 소프트웨어에 대한 지원 추가
- 곡선 P-192 및 P-256 (BZ#1382849)에 대한 오류 수정 코드 (ECC) 소프트웨어에 대한 지원이 추가되었습니다.

intel-cmt-cat 패키지 추가

이 패키지에 제공된 pqos 유틸리티를 사용하면 관리자가 L3 캐시를 모니터링하고 조작하여 유틸리티 및 성능을 향상시킬 수 있습니다.

툴은 커널 API를 우회하고 하드웨어에서 직접 작동하므로 사용하기 전에 CPU 고정이 대상 프로세스와 함께 사용해야 합니다. (BZ#1315489)

i40e 에서 신뢰할 수 있고 신뢰할 수 없는 VF 지원

이번 업데이트에서는 신뢰할 수 있고 신뢰할 수 없는 가상 기능에 대한 지원이 i40e NIC 드라이버에 추가되었습니다. (BZ#1384456)

OVS 802.1ad (QinQ) 커널 지원

이번 업데이트에서는 커널에서 802.1ad(QinQ) 네트워킹 표준을 활성화하여 OVS(Open vSwitch)와 함께 두 개의 VLAN 태그를 사용할 수 있습니다. 이 업데이트의 사용자 공간 부분은 openvswitch 패키지에서 제공합니다. (BZ#1155732)

공유 메모리 및 hugetlbfs에 대한 실시간 마이그레이션 지원

이번 업데이트에서는 공유 메모리 및 hugetlbfs 파일 시스템을 지원하기 위해 실시간 복사 후 마이그레이션을 활성화하도록 커널을 향상시킵니다. 이 기능을 사용하려면 다음을 수행합니다.

- 호스트에서 2MiB 대규모 페이지 구성
- 2MiB 대규모 페이지를 사용하여 게스트 VM을 생성
- guest VM 및 stress-test 애플리케이션을 실행하여 메모리를 테스트합니다.
- 복사 후 를 사용하여 게스트 VM을 실시간 마이그레이션합니다. (BZ#1373606)

새 패키지: dbxtool

dbxtool 패키지는 UEFI Secure Boot DBX 업데이트를 적용하기 위한 명령줄 유틸리티와 일회용 systemd 서비스를 제공합니다. (BZ#1078990)

mlx5 에서 SRIOV 신뢰할 수 있는 VF 지원

이번 업데이트에서는 SRIOV(Single Root I/O Virtualization)-trusted 가상 기능(VF)의 지원이 mlx5 드라이버에 추가되었습니다. (BZ#1383280)

4.9 커널 백포트에서의 rwsem 성능 업데이트

이번 업데이트를 통해 Linux 커널 버전 4.9의 변경 사항과 관련된 대부분의 업스트림 R/W 세마포어(rwsem) 성능이 Linux 커널로 백포트된 상태에서 kABI(커널 애플리케이션 바이너리 인터페이스)를 유지 관리합니다.

주요 변경 사항은 다음과 같습니다.

- writer-optimistic 스핀을 통해 잠금 대기 시간을 줄이고 성능 잠금을 향상시킵니다.
- 잠금 없는 대기 시간 동안 내부 스핀 잠금을 유지하지 않고 잠급니다. (BZ#1416924)

getrandom 을 Linux 커널에 추가

이번 업데이트에서는 **Linux** 커널에 **getrandom** 시스템 호출이 추가되었습니다. 결과적으로 사용자 공간은 이제 **/dev/urandom**에서 사용하는 동일한 비차트 엔트로피 풀에서 무작위성을 요청할 수 있으며 사용자 공간은 해당 풀에서 최소 **128**비트의 엔트로피가 누적될 때까지 차단할 수 있습니다. **(BZ#1432218)**

새로운 상태 라인인 **Umask**가 **/proc/<PID>/status**에 포함되어 있습니다.

이전 버전에서는 수정 없이 **process umask**를 읽을 수 없었습니다. 이러한 변경이 없으면 라이브러리에서 특히 기본 프로그램이 다중 스레드인 경우, 특히 해당 라이브러리에서 **root**를 안전하게 읽을 수 없습니다. 이제 **proc** 파일 시스템(**procfs**)이 **/proc/<PID>/status** 파일에 **umask**를 노출합니다. 형식은 **Umask: OOOO** 입니다. 여기서 **OOOO**는 작업의 **messages**에 대한 **8**진수 표현입니다. **(BZ#1391413)**

Intel® Omni-Path Architecture(OPA) 호스트 소프트웨어

Intel® Omni-Path Architecture(OPA) 호스트 소프트웨어는 **Red Hat Enterprise Linux 7.3**부터 완전히 지원됩니다. **Intel® OPA**는 클러스터형 환경의 컴퓨팅 노드와 **I/O** 노드 간에 고성능 데이터 전송(고가용성, 메시지 속도, 짧은 대기 시간)을 위해 고성능 데이터 전송(**High bandwidth**, 높은 메시지 속도, 짧은 대기 시간)을 위해 **HFI(HostSPACE Interface)** 하드웨어에 초기화 및 설정을 제공합니다.

Intel® Omni-Path Architecture 설명서를 얻는 방법에 대한 자세한 내용은 https://access.redhat.com/articles/2039623 을 참조하십시오. **(BZ#1459948)**

XTS-AES 키 확인 이제 **FIPSRegistryLogin** 요구 사항을 충족합니다.

이번 업데이트에서는 **FIPS** 모드에서 **Red Hat Enterprise Linux**를 실행하고 커널 **XTS-AES** 키 확인을 사용하는 동안 **AES** 키는 조정 키와 달라야 합니다. 이렇게 하면 **FIPShiera IG A.9** 요구 사항이 충족됩니다. 또한 **XEX** 기반 조정**-codebook** 모드를 암호 텍스트 스틸 **(XTS)** 테스트 벡터로 건너 뛰도록 표시할 수 있습니다. **(BZ#1314179)**

IBM z Systems에서 **mlx5** 가 지원됨

Mellanox mlx5 장치 드라이버는 **IBM z Systems**의 **Linux**에서도 지원되며 이더넷 **TCP/IP** 네트워크에서 사용할 수 있습니다. **(BZ#1394197)**

perf 툴에서 프로세서 캐시 줄 경합 감지 지원

perf 툴에서 **C2C(Shared Data Cache-to-Cache)** 분석을 위한 **c2c** 하위 명령을 제공합니다. 이를 통해 캐시 줄 경합을 검사하고 **true** 공유 및 **false** 공유를 모두 탐지할 수 있습니다.

경합은 **Symmetric Multi Processing (SMP)** 시스템의 프로세서 코어가 다른 프로세서에서 사용 중인 동일한 캐시 라인의 데이터 항목을 수정하는 경우에 발생합니다. 이 캐시 라인을 사용하는 다른 모든 프로세서는 복사본을 무효화하고 업데이트된 것을 요청하여 성능이 저하될 수 있습니다.

새로운 **c2c** 하위 명령은 경합이 탐지된 캐시 라인, 데이터를 읽고 쓰는 프로세스, 경합을 유발하는 명령 및 관련 **NUMA(Non-Uniform Memory Access)** 노드에 대한 자세한 정보를 제공합니다. **(BZ#1391243)**

lpfc 드라이버에서 SCSI-MQ 지원

Red Hat Enterprise Linux 7.4에서 업데이트된 lpfc 드라이버는 lpfc_use_blk_mq=1 모듈 매개 변수를 사용하여 SCSI-MQ(multiqueue) 사용을 활성화할 수 있습니다. 기본값은 0 (비활성화)입니다.

SCSI-MQ를 사용하는 비동기 IO over Fibre Channel 어댑터를 사용하는 Red Hat의 최근 성능 테스트에서는 특정 조건에서 성능 저하가 크게 저하되었습니다. 수정은 테스트 중이지만 Red Hat Enterprise Linux 7.4 General Availability에 대해서는 준비가 되지 않았습니다. (BZ#1382101)

13장. 실시간 커널

Red Hat Enterprise Linux for Real Time Kernel 정보

Red Hat Enterprise Linux for Real Time Kernel은 매우 높은 결정성이 있는 시스템에 대해 미세 조정하도록 설계되었습니다. 표준 커널 튜닝을 통해 결과의 일관성이 크게 증가할 수 있으며, 수행해야 합니다. 실시간 커널을 사용하면 표준 커널을 튜닝하여 얻을 수 있는 증가를 약간 늘릴 수 있습니다.

실시간 커널은 **rhel-7-server-rt-rpms** 리포지토리에서 사용할 수 있습니다. 설치 가이드 에는 설치 지침이 포함되어 있으며 나머지 문서는 **Red Hat Enterprise Linux for Real Time**의 제품 문서에서 확인할 수 있습니다.

kernel-rt 다시 기반

kernel-rt 소스는 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공하는 최신 **Red Hat Enterprise Linux** 커널 소스 트리를 기반으로 업그레이드되었습니다. **(BZ#1391779)**

14장. 네트워킹

NetworkManager 버전 1.8로 다시 기반

NetworkManager 패키지가 업스트림 버전 1.8로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 추가 경로 옵션에 대한 지원이 추가되었습니다.
- 재부팅이 유지될 때까지 장치의 관리되는 상태입니다.
- 이제 외부에서 관리하는 장치가 올바르게 처리됩니다.
- 다중 홈 호스트에서 네트워크로 연결된 안정성이 향상되었습니다.
- 호스트 이름 관리가 더 유연하게 구성되어 있습니다.
- 변경 및 강제 802-3 링크 속성에 대한 지원이 추가되었습니다. (BZ#1414103)

NetworkManager 에서 경로에 대한 추가 기능 지원

이번 업데이트를 통해 NetworkManager 는 몇 가지 고급 옵션을 설정할 수 있습니다. source_address (src, IPv4만 해당),type_of_service (tos), 창,maximum_transmission_unit (mtu), congestion_window (cwnd), initial_congestion_window (initcwnd) 정적 IPv4 및 연결 IPv6 경로에 대한 initial_receiver_window (initrwnd)를 제공합니다. (BZ#1373698)

NetworkManager 에서 장치 상태를 더 잘 처리

이번 업데이트를 통해 NetworkManager 는 서비스를 재시작한 후 장치의 상태를 유지하고 재시작 중에 관리되는 모드로 설정된 인터페이스를 대신합니다. 또한 NetworkManager 는 관리되지 않고 사용자 또는 다른 네트워크 서비스에서 수동으로 제어되지 않고 수동으로 제어하는 장치를 처리할 수 있습니다. (BZ#1394579)

NetworkManager 에서 MACsec (IEEE 802.1AE) 지원

이번 업데이트에서는 MACsec(Media Access Control Security) 암호화 구성 지원이 NetworkManager 에 추가되었습니다. (BZ#1337997)

NetworkManager 에서 802-3 링크 속성변경 및 적용 지원

이전에는 NetworkManager 가 802-3 링크 속성 만 노출했습니다. 802-3-ethernet.speed,802-3 이더넷.duplex, 802-3-ethernet.auto-negotiate. 이번 업데이트를 통해 변경 및 시행할 수 있습니다. auto-negotiate=yes 를 사용하거나 auto-negotiate=no,speed=<Mbit/s> , duplex= [half,full] 을 사용하여 자동으로 이 작업을 수행할 수 있습니다.

auto-negotiate=no 및 speed 또는 duplex 가 설정되지 않은 경우 링크 협상이 생략되고 auto-negotiate=no, speed=0, duplex=NULL 기본값이 유지됩니다.

또한 auto-negotiate 기본값은 yes 에서 이전 버전과의 호환성을 유지하기 위해 no 로 변경되었습니다. 이전에는 속성이 무시되었지만 이제 auto-negotiate 값이 yes 인 경우 링크 협상을 적용할 수 있었습니다. 속도 및/또는 duplex 설정되지 않은 상태로 설정하면 링크 협상이 무시됩니다. (BZ#1353612)

NetworkManager 는 장치 이름을 기반으로 하는 본딩 슬레이브 주문 지원

이전 버전에서는 슬레이브 연결에 대한 기존 활성화 순서는 마스터 인터페이스의 MAC 주소를 결정하는 데 문제가 발생할 수 있었습니다. 이번 업데이트에서는 장치 이름을 기반으로 보다 예측 가능한 순서가 추가되었습니다. NetworkManager 구성에서 slaves-order=name 설정을 사용하여 새 순서를 활성화할 수 있습니다.

새 순서는 기본적으로 비활성화되어 있으며 명시적으로 활성화해야 합니다. (BZ#1420708)

NetworkManager 에서 SR-IOV 장치에 대한 VF 지원

이번 업데이트를 통해 NetworkManager 시스템 서비스는 SR-IOV(Single Root I/O Virtualization) PCI 장치에 대한 VF(가상 기능) 생성을 지원합니다. NetworkManager 구성 파일의 device 섹션에 있는 sriov-num-vfs 옵션을 사용하여 VF 수를 지정할 수 있습니다. VF가 생성되면 NetworkManager 에서 연결 프로필을 활성화할 수 있습니다.

최대 전송 단위(MTU)와 같은 VF 인터페이스의 일부 속성은 물리적 인터페이스에 설정된 값과만 설정할 수 있습니다. (BZ#1398934)

kernel GRE 버전 4.8로 변경

커널 GRE(Generic Routing Encapsulation) 터널링이 업스트림 버전 4.8로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항이 추가되었습니다. 주요 변경 사항은 다음과 같습니다.

- IPv4 GRE 및 IPv6 GRE에 대한 경로를 전송 및 받기 위한 코드 병합
- gre (IPv4 GRE) 또는 ip6gre (IPv6 GRE) 장치를 가져오지 않고 링크 계층 주소를 변경할 수 있는 개선 사항

- IPv6 GRE 트래픽의 경우 체크섬 , spread-gather,highdma,gso, gro 와 같은 다양한 오프로드 지원

- ip6gretap 장치를 추가할 때 자동 커널 모듈 로드

- GRE 터널에 영향을 주는 Linux 커널 버전 4.8까지 오류 처리, MTU 계산, 경로 MTU 검색과 같은 기타 터널링 수정 (BZ#1369158)

dnsmasq 버전 2.76으로 다시 시작

dnsmasq 패키지는 여러 버그 수정 및 개선사항을 제공하는 버전 2.76으로 업그레이드되었습니다. 주요 변경 사항은 다음과 같습니다.

- dhcp_release6 유틸리티가 지원됩니다.

- ra-param 옵션이 추가되었습니다.

- DHCPv6 정보 요청에 대한 응답에서 RFC-4242 information-refresh-time 옵션에 대한 지원이 추가되었습니다.

- RFC-3775 호환 모바일 IPv6 지원의 ra-advrouter 모드가 추가되었습니다.

- script-arp 스크립트가 추가되었으며 dhcp-script 스크립트의 두 가지 새로운 함수가 포함되어 있습니다.

- 이제 알고리즘적으로 안정적인 주소가 아닌 DHCPv6 임시 주소 할당에 임의의 주소를 사용할 수 있습니다.

- 새로운 선택적 DNS Security Extensions (DNSSEC) 지원이 비활성화되었습니다.

- dnsmasq 는 IPv6 라우터 알림의 기본값을 변경할 수 있습니다. 결과적으로 ra-param 옵션은 dnsmasq 에서 알리는 경로의 기본 우선 순위 및 시간 간격을 변경하는 데 사용됩니다. 자세한 내

용은 dnsmasq(1) 도움말 페이지를 참조하십시오. (BZ#1375527, BZ#1398337)

BIND에서는 URI 리소스 레코드를 처리하는 방식을 변경하여 URI 이전 버전과의 호환성에도 영향을 미칩니다.

이번 업데이트에서는 URI 리소스 레코드를 사용할 때 BIND 제품군에서 더 이상 값 필드에 길이 바이트를 추가하지 않습니다. 즉, RHEL (Red Hat Enterprise Linux) 7.4의 BIND는 RFC 7553: https://tools.ietf.org/html/rfc7553 에 설명된 형식으로만 통신합니다.

이번 업데이트에서는 이전 버전의 RHEL에서 BIND를 사용하여 생성한 레코드와 새 URI 레코드를 호환되지 않습니다. 즉, RHEL 7.4의 BIND는 다음을 수행할 수 없습니다.

- RHEL에서 이전 버전의 BIND에서 제공하는 URI 레코드를 이해합니다.
- RHEL에서 이전 버전의 BIND를 사용하여 클라이언트에 URI 레코드를 제공합니다.

그러나 RHEL 7.4의 BIND는 다음을 수행할 수 있습니다.

- RHEL의 이전 및 향후 버전의 BIND에서 모두 캐시하고 레코드를 수신합니다.
- 알 수 없는 DNS 리소스 레코드로 인코딩된 이전 URI 형식의 레코드를 제공합니다. 자세한 내용은 RFC 3597을 참조하십시오. https://tools.ietf.org/html/rfc3597.

이번 업데이트 이후에는 DNS 영역 파일을 변경할 필요가 없습니다. (BZ#1388534)

Microsoft Azure 클라우드의 DDNS에 대해 DHCP 클라이언트 후크 예제 추가

Microsoft Azure 클라우드의 DDNS(Dynamic DNS)용 DHCP 클라이언트 후크의 예가 dhclient 패키지에 추가되었습니다. 이제 관리자는 이 후크를 쉽게 활성화하고 DDNS 서버에 Red Hat Enterprise Linux 클라이언트를 등록할 수 있습니다. (BZ#1374119)

dhcp_release6 에서 IPv6 주소 해제

이번 업데이트를 통해 dhcp_release6 유틸리티는 로컬 dnsmasq 서버의 IPv6 주소에 대해 Dynamic Host Configuration Protocol 버전 6 (DHCPv6) 리스를 해제할 수 있습니다. dhcp_release6 명령에 대한 자세한 내용은 dhcp_release6 (1) 매뉴얼 페이지를 참조하십시오. (BZ#1375569)

sendmail 에서 ECDHE 지원

이번 업데이트에서는 **Red Hat Enterprise Linux 7 Sendmail** 에 **eliptic Curve Diffie-Hellman Ephemeral Keys (ECDHE)** 지원이 추가되었습니다. **ECDHE**는 타원 곡선 암호화를 사용하는 **Diffie-Hellman** 프로토콜의 변형입니다. 이는 두 당사자가 안전하지 않은 채널을 통해 공유 비밀을 설정할 수 있도록 하는 익명 키 계약 프로토콜입니다. **(BZ#1124827)**

이제 Telnet에서 -6 옵션 지원

이번 업데이트를 통해 **telnet** 유틸리티는 **IPv6** 연결을 테스트하기 위해 **-6** 옵션을 지원합니다. **(BZ#1367415)**

unbound에서 음수 DNS 응답을 캐싱하기 위한 조정 가능한 TTL 제한

이번 업데이트에서는 **unbound** 서비스에 **cache-max-negative-ttl** 구성 옵션이 추가되어 음수 **DNS** 응답을 캐싱하기 위해 특별히 최대 **TTL**을 조정할 수 있습니다. 이전에는 이 제한이 도메인 **SOA** 레코드에 의해 결정되었거나 구성된 경우 모든 **DNS** 응답에 대한 최대 **TTL** 제한과 자동으로 동일합니다.

unbound 가 **DNS** 응답 캐싱의 **TTL**을 결정하는 경우 **cache-min-ttl** 옵션에 설정된 값이 **cache-max-negative-ttl** 에서 지정한 값보다 우선합니다. **(BZ#1382383)**

UDP 소켓의 확장성 개선

이번 업데이트에서는 **UDP** 전달 메모리 계정이 향상되고 **UDP** 소켓의 잠금 경합이 줄어듭니다. 그 결과 여러 피어에서 트래픽을 수신하는 **UDP** 소켓의 전체 수신 처리량이 크게 향상되었습니다. **(BZ#1388467)**

IP에서 커널에서 IP_BIND_ADDRESS_NO_PORT 지원

이번 업데이트에서는 커널에 **IP_BIND_ADDRESS_NO_PORT** 소켓 옵션이 추가되었습니다. 이를 통해 **bind()** 요청이 포트 번호 **0** 에 사용될 때 커널이 **L4 tuple** 예약을 건너뛸 수 있습니다. 결과적으로 다른 대상 호스트에 대한 많은 동시 연결을 유지할 수 있습니다. **(BZ#1374498)**

IPVS 소스 해시 스케줄링에서 L4 해시 및 대체 지원

이번 업데이트를 통해 **IP** 가상 서버**(IPVS)** 소스 해시 스케줄링 알고리즘은 다음과 같습니다.

- **L4** 해시
- 대상 서버에 대상 서버가 비활성 상태임을 나타내는 가중치가 **0** 인 경우 다음 활성 서버에 대한 요청을 대체합니다.

결과적으로 포트 번호를 기반으로 한 소스 **IP** 주소에서 요청 부하를 분산할 수 있습니다. 비활성 서버에 대한 요청은 더 이상 시간 초과되지 않습니다. **(BZ#1365002)**

iproute 이제 브리지 포트 옵션 변경 지원

이번 업데이트를 통해 상태,우선 순위 및 비용과 같은 브릿지 포트 옵션 변경 사항이 **iproute** 패키지에 추가되었습니다. 결과적으로 **iproute** 을 **bridge-utils** 패키지 대신 사용할 수 있습니다. **(BZ#1373971)**

SCTP (RFC 6458)의 소켓 API 확장의 새로운 옵션 구현

이번 업데이트에서는 **SCTP_SNDINFO** 옵션,**SCTP_NXTINFO**,**SCTP_NXTINFO** 및 **SCTP_DEFAULT_SNDINFO** 를 **Stream Control Transmission Protocol(RFC 6458)**의 소켓 **API** 확장에 구현합니다.

이러한 새로운 옵션은 더 이상 사용되지 않는 **SCTP_SNDRCV**,**SCTP_EXTRCV** 및 **SCTP_DEFAULT_SEND_PARAM** 옵션을 대체합니다. 더 이상 사용되지 않는 기능 섹션도 참조하십시오. **(BZ#1339791)**

SS는 이제 SCTP 소켓 목록 지원

이전에는 **netstat** 유틸리티에서 **SCTP(Stream Control Transmission Protocol)** 소켓 목록을 제공했습니다. 이번 업데이트를 통해 **ss** 유틸리티에서 동일한 목록을 표시할 수 있습니다. **(BZ#1063934)**

wpa_supplicant 버전 2.6로 업데이트

wpa_supplicant 패키지가 업스트림 버전 **2.6**으로 업그레이드되어 여러 버그 수정 및 개선 사항이 추가되었습니다. 특히 **wpa_supplicant** 유틸리티는 이제 **MACsec(Media Access Control Security)** 암호화 **802.1AE**를 지원하므로 기본적으로 **MACsec**을 구성에 사용할 수 있습니다. **(BZ#1404793, BZ#1338005)**

Linux 커널에는 이제 switchdev 인프라 및 mlxsw가 포함됩니다.

이번 업데이트에서는 다음 기능을 **Linux** 커널에 백포트합니다.

- 이더넷 스위치 장치 드라이버 모델 **- switchdev** 인프라. 따라서 스위치 장치는 커널에서 데이터 플레인 전달을 오프로드할 수 있습니다.
- **mlxsw** 드라이버

mlxsw 에서 지원하는 스위치 하드웨어:

- **Mellanox SwitchX-2** (단일 경로만 해당)

- Mellanox SwitchIB 및 SwitchIB-2
- Mellanox Spectrum

mlxsw 에서 지원하는 기능:

- 포트 점보 프레임, 속도 설정, 상태 설정, 통계
- splitterable과 함께 포트 분할
- 포트 미러링
- QoS: 802.1p, Data Center Bridging (DCB)
- 워크플로우 오프로드를 사용한 액세스 제어 목록(ACL)이 기술 프리뷰로 도입되었습니다.

계층 2 기능:

- VLAN
- 스프레드 트리 프로토콜 (STP)
- 팀 또는 본딩 오프로드를 사용하는 LAG(link Aggregation)
- LLDP(link Layer Discovery Protocol)

계층 3 기능:

- 유니캐스트 라우팅

이러한 모든 기능을 구성하려면 **iproute** 패키지에서 제공하는 표준 툴도 사용하십시오. (BZ#1297841, BZ#1275772, BZ#1414400, BZ#1434587, BZ#1434591)

Linux 브리지 코드가 버전 **4.9**로 다시 시작

Linux 브리지 코드가 업스트림 버전 **4.9**로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- **802.1ad VLAN** 필터링 및 **Tx VLAN** 가속 지원
- **accessibility Proxy Address Resolution Protocol (ARP)**
- **switchdev**를 사용하여 오프로드 전환 지원
- 사용자 **mdb** 항목에 대한 **VLAN** 지원
- **mdb** 항목의 확장 속성 지원
- 임시 포트 라우터 지원
- **VLAN**별 통계 지원
- 인터넷 그룹 관리 프로토콜/**Multicast Listener Discovery (IGMP/MLD)** 통계 지원
- **sysfs** 를 사용하여 지원하는 모든 구성 설정은 이제 **netlink**에서도 지원됩니다.
- 알 수 없는 멀티 캐스트 홍수를 제어하기 위해 포트별 플래그 추가 **(BZ#1352289)**

bind-dyndb-ldap 버전 **11.1**을 다시 기반으로 합니다.

bind-dyndb-ldap 패키지가 업스트림 버전 11.1로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

특히 /etc/named.conf 파일에서 이제 새로운 DynDB API를 사용합니다. bind-dyndb-ldap 패키지를 업데이트하면 파일이 새 API 스타일로 자동 변환됩니다. (BZ#1393889)

BIND의 업스트림 버전 9.11.0의 dyndb API가 Red Hat Enterprise Linux에 추가되었습니다.

이번 업데이트에서는 업스트림에서 bind 패키지 버전 9.11.0에 도입된 dyndb 시스템 플러그인의 API를 백포트합니다. 결과적으로 Red Hat Enterprise Linux의 bind-dyndb-ldap 플러그인은 이제 새 API를 사용합니다. Red Hat Enterprise Linux의 이전 릴리스에서 사용된 다운스트림 기능 dynamic_db 는 더 이상 지원되지 않습니다.

업스트림 dyndb 는 다운스트림 dynamic_db 와 다른 구성 구문을 사용하므로 이 업데이트의 구문도 변경됩니다. 그러나 수동 구성을 변경할 필요는 없습니다. (BZ#1393886)

tboot 버전 1.9.5로 다시 시작

tboot 패키지가 업스트림 버전 1.9.5로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 이번 업데이트에서는 TPM(Trusted Platform Module) 2.0을 위한 2세대 LCP(link Control Protocol) 생성 유틸리티와 업데이트된 LCP 생성 유틸리티에 대한 사용자 가이드가 추가되었습니다.
- Intel Platform Trust Technology(PTT) 및 Linux PTT 드라이버의 올바른 동작을 보장하기 위해 해결방법이 구현되었습니다.
- Linux 커널의 새로운 기능을 수용할 수 있도록 Linux 커널 헤더 구조 선언에 새 필드가 추가되었습니다. (BZ#1384210)

rdma 버전 13에 다시 빌드하여 rdma-core 통합과 관련된 패키지

rdma 패키지와 관련된 패키지가 업그레이드되어 단일 소스 패키지인 rdma-core 버전 13으로 통합되었습니다. 패키지는 다음과 같습니다.

- rdma

- **iwpmd**
- **libibverbs**
- **librdmacm**
- **ibacm**
- **libibumad**
- **libocrdma**
- **libmlx4**
- **libmlx5**
- **libhfi1verbs**
- **libi40iw**
- **srp_daemon(이전 srptools)**
- **libmthca**
- **libcxgb3**
- **libcxgb4**

- libnes
- libipathverbs
- librxe
- rdma-ndd

이전에 포함되지 않은 다음 패키지가 새 패키지 rdma-core 의 일부로 추가되었습니다.

- libqedr
- libhns
- libvmw_pvrdma

모든 ibverbs 하드웨어별 공급자 라이브러리는 이제 libibverbs 하위 패키지에 번들되어 설치를 간소화하고 버전 관리 불일치를 방지할 수 있습니다. (BZ#1404035)

고정 MAC 주소에 대한 OVN IP 주소 관리 지원 추가

이번 업데이트에서는 사용자 지정 고정 MAC 주소를 사용하여 동적 IP 주소 할당 지원이 추가되었습니다. 결과적으로 OVN(Open Virtual Network) 사용자는 정적 MAC 주소와 연결된 동적 IP를 사용하여 구성을 생성할 수 있습니다. (BZ#1368043)

다중 홈 호스트에서 네트워크 안정성 개선

다른 인터페이스에 이미 존재하는 경로와의 인터페이스에서 NetworkManager 유틸리티가 이제 역방향 경로 필터링 방법을 Strict 에서 Loose 로 자동 전환합니다. 이를 통해 다중 홈 호스트 시스템에서 네트워크 안정성이 향상됩니다. (BZ#1394344)

GENRuntimeConfig, VXLAN, GRE 터널의 오프로드 지원

이번 업데이트를 통해 GENRuntimeConfig, VXLAN, GRE 터널의 오프로드를 지원하는 인프라가 추가되었습니다. 또한 GEN서 터널 구현에서 다양한 버그가 수정되었습니다. (BZ#1326309)

터널 트래픽용 LCO 지원

이번 업데이트를 통해 특정 네트워크 카드가 터널 트래픽에 대해 체크섬 오프로드를 사용할 수 있도록 LS(Local Checksum Offloading) 기술이 추가되었습니다. 이번 개선된 기능을 통해 VXLAN, GRE, 기타 터널의 성능이 향상되었습니다. (BZ#1326318)

NIC에서 터널 성능 개선

이번 업데이트를 통해 기본적으로 터널 오프로드를 지원하지 않는 일부 NIC(네트워크 인터페이스 카드)에서 터널 성능이 향상되었습니다. 결과적으로 사용자는 이러한 NIC에서 기존 하드웨어 오프로드를 활용할 수 있습니다. (BZ#1326353)

커널에서 NPT 가 지원됨

이번 업데이트를 통해 RFC 6296에 정의된 IPv6-to-IPv6 Network Prefix Translation (NPTv6) 함수가 netfilter 프레임워크에 추가되었습니다. 결과적으로 IPv6 접두사 간에 상태 비저장 변환을 위해 NPT 를 활성화할 수 있습니다. (BZ#1432897)

D-Bus API를 통해 DNS 구성이 지원됨

이전에는 외부 애플리케이션에서 NetworkManager 에서 사용하는 DNS 매개 변수를 쉽게 검색할 수 없었습니다. 이번 업데이트를 통해 D-Bus API를 통해 DNS 구성이 지원됩니다. 결과적으로 이름 서버 및 도메인을 포함한 모든 DNS 관련 정보는 NetworkManager 의 D-Bus API를 통해 클라이언트 애플리케이션에서 사용할 수 있습니다. 이러한 애플리케이션의 예로는 이제 DNS 구성을 표시할 수 있는 nmcli 툴이 있습니다. (BZ#1404594)

RuntimeClass 지원이 별도의 패키지로 이동

이번 업데이트를 통해PPP(Point-to-Point Protocol) 지원이 별도의 선택적 NetworkManager-ppp 패키지로 이동되었습니다. 결과적으로 NetworkManager 의 종속성 체인이 작아지고 설치된 패키지 수를 제한할 수 있습니다.

RuntimeClass 설정을 구성하려면 NetworkManager-ppp 패키지가 설치되어 있는지 확인해야 합니다. (BZ#1404598)

tc 유틸리티에서 헤더를 지원합니다 .

tc 유틸리티는 커널 헤더 트래픽 제어 분류기를 사용하도록 개선되었습니다. 이번 업데이트를 통해 사용자는 인터페이스에서 개화 기 규칙을 추가, 수정 또는 삭제할 수 있습니다. (BZ#1422629)

SCTP 전달 경로에서 CRC32c 값 계산 수정

이전 버전에서는 커널이 오프로드를 지원하지 않는 인터페이스로 전달할 때 kernel이 오프로드된 체크섬을 사용하여 SCTP(Stream Control Transmission Protocol) 패킷의 CRC32c 값을 잘못 계산했습니다. 이번 업데이트에서는 전달 경로에서 CRC32c 의 계산을 수정합니다. 그 결과 이제 SCTP 패킷이 설명된 상황에서 올바르게 전송됩니다. (BZ#1072503)

새 패키지: iperf3

이번 업데이트에서는 iperf3 패키지 버전 3.1.7이 Red Hat Enterprise Linux 7에 추가되었습니다. iperf3 유틸리티를 사용하면 IP 네트워크에서 수행할 수 있는 최대 대역폭을 적극적으로 측정할 수 있습니다. (BZ#913329)

이제 OVN 설치에서 쉽게 구성할 수 있는 firewalld 규칙 지원

이 기능은 OVN(Open Virtual Network)의 firewalld 구성 규칙을 openvswitch 패키지에 추가합니다. 따라서 사용자는 firewalld 구성을 수동으로 생성하지 않고 firewalld 를 활성화하여 더 쉽게 OVN을 설치할 수 있습니다. (BZ#1390938)

netlink 에서 브리지 마스터 속성 지원

이번 업데이트를 통해 브리지 속성이 변경될 때마다 리스너로 알림이 전송됩니다. 여기에는 sysfs, rtnl, ioctl 또는 사용자 애플리케이션에 의해 트리거되는 변경 사항이 포함됩니다(예: NetworkManager. (BZ#950243)

15장. 보안

새로운 패키지: tang, clevis, jose, luksmeta

네트워크 Bound 디스크 암호화(NBDE)를 사용하면 시스템을 재부팅할 때 암호를 수동으로 입력하지 않고도 물리적 및 가상 머신에서 하드 드라이브의 루트 볼륨을 암호화할 수 있습니다.

- Tang은 데이터를 네트워크 존재에 바인딩하는 서버입니다. 여기에는 원격 서비스에 바인딩하기 위한 암호화 작업을 제공하는 데몬이 포함됩니다. tang 패키지는 RuntimeClass 프로젝트의 서버 측면을 제공합니다.

- Clevis는 자동화된 암호 해독을 위한 플러그인 프레임워크입니다. 데이터의 자동 암호 해독 또는 LUKS 볼륨의 자동 잠금 해제를 제공하는 데 사용할 수 있습니다. clevis 패키지는 RuntimeClass 프로젝트의 클라이언트 측면을 제공합니다.

- José는 JavaScript 오브젝트 서명 및 암호화 표준의 C- language 구현입니다. jose 패키지는 clevis 및 tang 패키지에 종속되어 있습니다.

- LUKSMeta는 LUKSv1 헤더에 메타데이터를 저장하기 위한 간단한 라이브러리입니다. luksmeta 패키지는 clevis 및 tang 패키지에 종속되어 있습니다.

tang-nagios 및 clevis-udisk2 하위 패키지는 기술 프리뷰로만 사용할 수 있습니다. (BZ#1300697, BZ#1300696, BZ#1399228, BZ#1399229)

새 패키지: usbguard

USBGuard 소프트웨어 프레임워크는 장치 속성을 기반으로 기본 화이트리스트 및 블랙리스트 기능을 구현하여 침입형 USB 장치에 대한 시스템 보호 기능을 제공합니다. 사용자 정의 정책을 적용하기 위해 USBGuard 는 Linux 커널 USB 장치 권한 부여 기능을 사용합니다. USBGuard 프레임워크는 다음 구성 요소를 제공합니다.

- 동적 상호 작용 및 정책 적용을 위한 프로세스 간 통신(IPC) 인터페이스가 있는 데몬 구성 요소

- 실행 중인 USBGuard 인스턴스와 상호 작용하는 명령줄 인터페이스

- USB 장치 권한 부여 정책을 작성하는 규칙 언어

- 공유 라이브러리에서 구현된 데몬 구성 요소와 상호 작용 위한 **C++ API(BZ#1395615)**

openssh 버전 **7.4**로 다시 기반

openssh 패키지가 업스트림 버전 **7.4**로 업데이트되어 다음과 같은 여러 개선 사항, 새로운 기능 및 버그 수정이 제공됩니다.

- **SFTP** 에서 중단된 업로드의 재개에 대한 지원이 추가되었습니다.
- 인증 실패 메시지의 확장 로그 형식을 추가했습니다.
- **SHA-256** 알고리즘을 사용하는 새 지문 유형을 추가했습니다.
- 외부 **PIN** 항목 장치가 있는 **PKCS#11** 장치 사용에 대한 지원이 추가되었습니다.
- **OpenSSH** 서버에서 **SSH-1** 프로토콜에 대한 지원 삭제
- 레거시 **v00** 인증서 형식에 대한 지원 삭제
- **ssh** 유틸리티에 대한 **PubkeyAcceptedKeyTypes** 및 **HostKeyAlgorithms** 구성 옵션을 추가하여 키 유형을 선택적으로 비활성화할 수 있도록 **sshd** 데몬을 추가했습니다.
- **OpenSSH** 클라이언트에 **AddKeysToAgent** 옵션을 추가했습니다.
- **ProxyJump ssh** 옵션과 해당 **-J** 명령줄 플래그를 추가했습니다.
- **Diffie-Hellman 2K, 4K** 및 **8K** 그룹에 대한 키 교환 방법에 대한 지원이 추가되었습니다.
- **ssh_config** 파일에 대해 **Include** 지시어를 추가했습니다.

- **UseLogin** 옵션에 대한 지원 삭제

- 서버에서 사전 인증 압축 지원이 제거되었습니다.

- 이제 **seccomp** 필터가 사전 인증 프로세스에 사용됩니다. **(BZ#1341754)**

audit 버전 **2.7.6**으로 다시 시작

audit 패키지가 업스트림 버전 **2.7.6**으로 업데이트되어 다음과 같은 향상된 기능, 새로운 기능 및 버그 수정이 제공됩니다.

- 이제 **auditd** 서비스가 시작될 때 로깅 디렉터리 권한을 자동으로 조정합니다. 이렇게 하면 패키지 업그레이드를 수행한 후 디렉터리 권한을 올바르게 유지할 수 있습니다.

- **ausearch** 유틸리티에는 새로운 **--format** 출력 옵션이 있습니다. **--format** 텍스트 옵션은 발생하는 상황을 설명하는 영어 문장으로 이벤트를 제공합니다. **--format csv** 옵션은 **CSV(Comma Separated Value)** 형식의 출력되는 일부 메타데이터 필드 외에도 오브젝트, 개체, 작업, 결과 등에 로그를 정규화합니다. 이는 이벤트 정보를 데이터베이스, 스프레드트 또는 기타 분석 프로그램으로 푸시하여 감사 이벤트를 보고, 차트 또는 분석하는 데 적합합니다.

- **auditctl** 유틸리티는 **--reset-lost** 명령줄 옵션을 통해 커널에서 손실된 이벤트 카운터를 재설정할 수 있습니다. 이렇게 하면 **0**일로 값을 재설정할 수 있으므로 손실된 이벤트를 더 쉽게 확인할 수 있습니다.

- **ausearch** 및 **aureport** 에는 이제 시스템이 부팅 된 이후 이벤트를 찾을 수 있는 **--start** 명령줄 옵션에 대한 부팅 옵션이 있습니다.

- **ausearch** 및 **aureport** 는 새 **--escape** 명령줄 옵션을 제공하여 감사 필드를 위해 어떤 종류의 이스케이프가 수행되는지 더 잘 제어할 수 있습니다. 현재 **raw,tty,shell, shell_quote** 이스케이프를 지원합니다.

- **auditctl** 에서는 더 이상 **entry** 필터를 사용하여 규칙을 허용하지 않습니다. **Red Hat Enterprise Linux 5** 이후에는 이 필터가 지원되지 않았습니다. 이번 릴리스 이전에는 **Red Hat Enterprise Linux 6** 및 **7**에서 **auditctl** 에서 모든 항목 규칙을 종료 필터로 이동하여 항목 필터가 더 이상 사용되지 않음을 경고했습니다. **(BZ#1381601)**

opensc 버전 **0.16.0**으로 다시 기반

라이브러리 및 유틸리티의 OpenSC 세트는 스마트 카드 작업에 대한 지원을 제공합니다. OpenSC 는 암호화 작업을 지원하는 카드에 중점을 두고 인증, 메일 암호화 또는 디지털 서명에 사용할 수 있습니다.

Red Hat Enterprise Linux 7.4의 주요 개선 사항은 다음과 같습니다.

- OpenSC 는CAC(Common Access Card) 카드에 대한 지원을 추가합니다.
- OpenSC 는 PKCS#11 API를 구현하며 이제 CoolKey revision 기능을 제공합니다. opensc 패키지는 coolkey 패키지를 대체합니다.

coolkey 패키지는 Red Hat Enterprise Linux 7의 라이프 사이클 기간 동안 계속 지원되지만 opensc 패키지를 통해 새로운 하드웨어 사용은 제공됩니다. (BZ#1081088, BZ#1373164)

openssl 버전 1.0.2k로 다시 시작

openssl 패키지가 업스트림 버전 1.0.2k로 업데이트되어 다음과 같은 여러 개선 사항, 새로운 기능 및 버그 수정이 제공됩니다.

- DTLS(Datagram Transport Layer Security TLS) 프로토콜 버전 1.2에 대한 지원이 추가되었습니다.
- TLS의 ECDHE 키 교환에 대한 자동 elliptic 곡선 선택 지원이 추가되었습니다.
- Application-Layer Protocol Negotiation (ALPN)에 대한 지원이 추가되었습니다.
- RSA-PSS, RSA-OAEP, ECDH 및 X9.42 DH 체계에 대한 CMS (Cryptographic Message Syntax) 지원이 추가되었습니다.

이 버전은 이전 Red Hat Enterprise Linux 7 릴리스의 OpenSSL 라이브러리 버전에서 API 및 ABI와 호환됩니다. (BZ#1276310)

openssl-ibmca 버전 1.3.0으로 다시 기반

openssl-ibmca 패키지가 업스트림 버전 1.3.0으로 업데이트되어 이전 버전에 비해 여러 버그 수정 및 개선 사항이 추가되었습니다. 주요 변경 사항은 다음과 같습니다.

- SHA-512에 대한 지원이 추가되었습니다.

- 암호화 방법은 ibmca 엔진이 시작될 때 동적으로 로드됩니다. 이를 통해 libica 라이브러리를 통해 하드웨어에서 지원되는 경우 ibmca 가 직접 암호화 방법을 사용할 수 있습니다.

- 스트림 암호화 모드를 사용한 블록 크기 처리 버그가 수정되었습니다. (BZ#1274385)

OpenSCAP 1.2는 NIST 인증입니다.

OpenSCAP 1.2SCAP(Security Content Automation Protocol) 스캐너는 미국 정부에서 Red Hat Enterprise Linux 6 및 7의 평가 구성 및 취약점 스캐너로 NIST(표준 및 기술) 인증을 받았습니다. OpenSCAP 은 보안 자동화 콘텐츠를 올바르게 분석하고 평가하며 NIST가 민감한 보안 불일치 환경에서 실행하기 위해 필요한 기능 및 문서를 제공합니다. 또한 OpenSCAP 은 Linux 컨테이너를 평가하는 첫 번째 NIST 인증 구성 스캐너입니다. 사용 사례에 따라 PCI 및 DoD 보안 기술 구현 가이드(STIG) 규정 준수를 위한 Red Hat Enterprise Linux 7 호스트 구성과 CVE(Common Vulnerabilities and Exposures) 데이터를 사용하여 알려진 취약점 검사를 수행하는 것이 포함됩니다. (BZ#1363826)

libreswan 버전 3.20으로 다시 시작

libreswan 패키지는 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공하는 업스트림 버전 3.20으로 업그레이드되었습니다. 주요 개선 사항은 다음과 같습니다.

- 모든 호스트에서 간단한 구성을 사용하여 많은 수의 호스트를 포함하는 IPsec 배포를 활성화하는 Opportunistic IPsec (Mesh Encryption)에 대한 지원이 추가되었습니다.

- FIPS는 더 강화되었습니다.

- Virtualtunnel Interface (VTI)를 사용하여 라우팅 기반 VPN 지원이 추가되었습니다.

- 루트가 아닌 구성에 대한 지원이 개선되었습니다.

- OCSP(Online Certificate Status Protocol) 및 CRL(Certificate Revocation Lists) 지원이 개선되었습니다.

- 새로운 whack 명령 옵션 추가: --fipsstatus,--fetchcrls,--globalstatus, --shuntstatus.

- NAT Opportunistic Encryption (OE) Client Address Translation: leftcat=yes 에 대한 지원이 추가되었습니다.

- 트래픽 흐름 기밀 메커니즘에 대한 지원이 추가되었습니다. tfc=.

- RFC 4307bis 및 RFC 7321bis에 따라 암호 기본 설정이 업데이트되었습니다.

- Extended sequence Numbers (ESN): esn=yes 에 대한 지원이 추가되었습니다.

- 재생 창 비활성화 및 증가에 대한 지원 추가: replay-window=. (BZ#1399883)

감사 이제 세션 ID 기반 필터링 지원

이번 업데이트를 통해 Linux 감사 시스템에서는 sessionid 값을 기반으로 감사 메시지를 필터링하는 사용자 규칙을 지원합니다. (BZ#1382504)

libseccomp 에서 IBM Power 아키텍처 지원

이번 업데이트를 통해 libseccomp 라이브러리는 IBM Power, 64비트 IBM Power 및 64비트 little-endian IBM Power 아키텍처를 지원하여 GNOME 리베이스를 활성화합니다. (BZ#1425007)

AUDIT_KERN_MODULE 은 모듈 로드를 기록합니다.

AUDIT_KERN_MODULE 보조 레코드가 init_module(), finit_module() 및 delete_module() 함수의 AUDIT_SYSCALL 레코드에 추가되었습니다. 이 정보는 audit_context 구조에 저장됩니다. (BZ#1382500)

OpenSSH 는 이제 공개 키 서명에 SHA-2를 사용합니다.

이전에는 OpenSSH 에서 RSA 및 DSA 키를 사용하는 공개 키 서명에 SHA-1 해시 알고리즘을 사용했습니다. SHA-1은 더 이상 안전한 것으로 간주되지 않으며 새로운 SSH 프로토콜 확장에서는 SHA-2를 사용할 수 있습니다. 이번 업데이트를 통해 SHA-2는 공개 키 서명의 기본 알고리즘입니다. SHA-1은 이전 버전과의 호환성 목적으로만 사용할 수 있습니다. (BZ#1322911)

firewalld 에서 추가 IP 세트 지원

이 **firewalld** 서비스 데몬 업데이트를 통해 다음 **ipset** 유형에 대한 지원이 추가되었습니다.

- **hash:ip,port**
- **hash:ip,port,ip**
- **hash:ip,port,net**
- **hash:ip,mark**
- **hash:net,net**
- **hash:net,port**
- **hash:net,port,net**
- **hash:net,iface**

동시에 소스 및 대상의 조합을 제공하는 다음 **ipset** 유형은 **firewalld** 의 소스로 지원되지 않습니다. 이러한 유형을 사용하는 **IP** 세트는 **firewalld** 에서 생성되지만 사용량은 직접 규칙으로 제한됩니다.

- **hash:ip,port,ip**
- **hash:ip,port,net**
- **hash:net,net**
- **hash:net,port,net**

ipset 패키지가 업스트림 버전 6.29에 다시 시작되었으며 다음 ipset 유형이 추가로 지원됩니다.

- hash:mac
- hash:net,port,net
- hash:net,net
- hash:ip,mark (BZ#1419058)

firewalld 는 이제 풍부한 규칙에서 ICMP 유형에 대한 작업 지원

이번 업데이트를 통해 firewalld 서비스 데몬을 사용하면 허용, 로그 및 표시 작업이 포함된 풍부한 규칙에ICMP(Internet Control Message Protocol) 유형을 사용할 수 있습니다. (BZ#1409544)

firewalld 에서 비활성화된 자동 도우미 할당 지원

이 업데이트의 firewalld 서비스 데몬에서는 비활성화된 자동 도우미 할당 기능을 지원합니다. 자동 도우미 할당을 해제하는 경우에도 추가 규칙을 추가하지 않고 firewalld 도우미를 사용할 수 있습니다. (BZ#1006225)

nss nss-util 은/는 기본적으로 SHA-256을 사용합니다.

이번 업데이트를 통해 디지털 서명을 만들 때 강력한 해시 알고리즘을 사용하도록 NSS 라이브러리의 기본 구성이 변경되었습니다. RSA, EC 및 2048비트(또는 긴) DSA 키를 사용하면 SHA-256 알고리즘이 사용됩니다.

이제 certutil,crlutil, cmsutil 과 같은 NSS 유틸리티도 기본 구성에서 SHA-256을 사용합니다. (BZ#1309781)

감사 필터 제외 규칙에 추가 필드가 포함됩니다.

exclude 필터가 향상되었으며 이제 msgtype 필드뿐만 아니라 pid,uid,gid,auid,sessionID, SELinux 유형을 포함합니다. (BZ#1382508)

PROCTITLE 에서 감사 이벤트에서 전체 명령을 제공합니다.

이번 업데이트에서는 감사 이벤트에 추가된 PROCTITLE 레코드가 도입되었습니다. PROCTITLE 은 실행 중인 전체 명령을 제공합니다. PROCTITLE 값이 인코딩되므로 감사 이벤트 구문 분석기를 우회할

수 없습니다. PROCTITLE 값은 사용자 공간 날짜에 의해 조작되기 때문에 여전히 신뢰할 수 없습니다. (BZ#1299527)

nss-softokn 버전 3.28.3으로 업데이트

nss-softokn 패키지가 업스트림 버전 3.28.3으로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- TLS(RFC 7905), 인터넷 키 교환 프로토콜(IKE), IPsec(RFC 7634)에서 사용하는 ChaCha20-Poly1305(RFC 7539) 알고리즘에 대한 지원이 추가되었습니다.
- 키 교환 목적으로 Curve25519/X25519 곡선에 대한 지원이 추가되었습니다.
- Extended Master Secret (RFC 7627) 확장에 대한 지원이 추가되었습니다. (BZ#1369055)

libica 버전 3.0.2로 업데이트

libica 패키지가 업스트림 버전 3.0.2로 업그레이드되었으며 이전 버전에 비해 여러 수정 사항이 제공됩니다. 주요 추가 기능은 다음과 같습니다.

- FIPS (Federal Information Processing Standards) 모드 지원
- Deterministic Random Bit Generator에 대한 지원 강화 및 업데이트된 보안 사양 NIST SP 800-90A를 준수하는 pseudorandom 번호 생성 지원 (BZ#1391558)

opencryptoki 버전 3.6.2로 다시 시작

opencryptoki 패키지가 업스트림 버전 3.6.2로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다.

- OpenSSL 1.1 지원 추가
- 더 이상 사용되지 않는 OpenSSL 인터페이스를 교체했습니다.
- 더 이상 사용되지 않는 libica 인터페이스 교체

- IBM CryptoConcurrency (ICA)의 성능 개선

- rc=8에 대한 지원이 추가되었습니다. icsf 토큰에 reasoncode=2028 오류 메시지가 추가되었습니다. (BZ#1391559)

AUDIT_NETFILTER_PKT 이벤트가 정규화되었습니다.

AUDIT_NETFILTER_PKT 감사 이벤트가 간소화되고 메시지 필드가 일관된 방식으로 표시됩니다. (BZ#1382494)

p11tool 은 저장된 ID를 지정하여 오브젝트 작성 지원

이번 업데이트를 통해 p11tool GnuTLS PKCS#11 툴은 저장된 ID를 지정하여 오브젝트를 작성하는 새로운 --id 옵션을 지원합니다. 그러면 p11tool 보다 더 많은 애플리케이션에서 작성한 오브젝트를 처리할 수 있습니다. (BZ#1399232)

새 패키지: nss-pem

이번 업데이트에서는 이전에 nss 패키지의 일부인 nss-pem 패키지가 별도의 패키지로 도입되었습니다. nss-pem 패키지는 PKCS#11 모듈로 구현된 NS(Network Security Services)용 PEM 파일 리더를 제공합니다. (BZ#1316546)

pmrfc3164 는 에서 pmrfc3164sd 를 대체합니다. rsyslog

rsyslog 패키지 업데이트로 BSD syslog 프로토콜 형식의 로그를 구문 분석하는 데 사용되는 pmrfc3164sd 모듈(RFC 3164)은 공식 pmrfc3164 모듈로 교체되었습니다. 공식 모듈은 pmrfc3164sd 기능을 완전히 다루지 않으므로 rsyslog 에서 계속 사용할 수 있습니다. 그러나 가능한 경우 새로운 pmrfc3164 모듈을 사용하는 것이 좋습니다. pmrfc3164sd 모듈은 더 이상 지원되지 않습니다. (BZ#1431616)

libreswan 이제 right=%opportunisticgroup지원

이번 업데이트에서는 Libreswan 구성의 conn 부분에 있는 올바른 옵션에 대한 %opportunisticgroup 값이 지원됩니다. 이렇게 하면 X.509 인증을 사용하는 opportunistic IPsec이 가능하므로 대규모 환경에서 관리 오버헤드가 크게 줄어듭니다. (BZ#1324458)

ca-certificates Mozilla Firefox 52.2 ESR 요구 사항 충족

최신 Mozilla Firefox ESR(Extended Support Release)과 함께 게시된 대로 NNS(Network Security Services) 코드 및 CA(인증 기관) 목록이 업데이트되었습니다. 업데이트된 CA 목록은 PKI(Internet Public Key Infrastructure)에 사용되는 인증서와의 호환성을 향상시킵니다. 인증서 검증 거부를 방지하기 위해 Red Hat은 2017년 6월 12일에 업데이트된 CA 목록을 설치할 것을 권장합니다. (BZ#1444413)

nss Mozilla Firefox 52.2 ESR 요구 사항 충족

최신 Mozilla Firefox ESR(Extended Support Release)과 함께 게시된 대로 인증 기관(CA) 목록이 업데이트되었습니다. 업데이트된 CA 목록은 PKI(Internet Public Key Infrastructure)에 사용되는 인증서와의 호환성을 향상시킵니다. 인증서 검증 거부를 방지하기 위해 Red Hat은 2017년 6월 12일에 업데이트된 CA 목록을 설치할 것을 권장합니다. (BZ#1444414)

scap-security-guide 버전 0.1.33로 업데이트

scap-security-guide 패키지가 업스트림 버전 0.1.33으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 이 새 버전에서는 기존 규정 준수 프로필을 개선하고 적용 범위를 확장하여 다음 두 가지 새 구성 기준선을 포함합니다.

- PCI-DSS v3 Control Baseline에 대한 지원 연장
- 미국 정부 공산 클라우드 서비스 (C2S)에 대한 지원 연장
- 공인 클라우드 공급자용 Red Hat Corporate Profile 연장.
- Red Hat Enterprise Linux 7 프로파일에 대한 DISA(Security Technical Implementation Guide)에 대한 지원이 추가되어 Red Hat Enterprise Linux V1R1 프로파일의 DISAReplicas에 대한 지원이 추가되었습니다.
- 비기본 정보 시스템 및 조직 (NIST 800-171) 프로필에서 분류되지 않은 정보에 대한 지원이 추가되었습니다. Red Hat Enterprise Linux 7은 Red Hat Enterprise Linux 7을 CAUI(Controlled Unclassified Information) 보안을 위해 확인된 NIST 특수 발행 800-53 컨트롤로 구성합니다.
- 미국 정부 구성 기준선(USGCB/STIG) 프로필에 대한 지원이 추가되어 미국 S와의 파트너십을 통해 개발되었습니다. 국가 표준 및 기술 (NIST), U. S. 국방부, 국가안보국, Red Hat.

USGCB/STIG 프로필은 다음 문서에서 구성 요구 사항을 구현합니다.

- 국가 보안 시스템 지시 사항 1253 (CNSSI 1253)
- NIST Controlled Unclassified Information (NIST 800-171)

- 중간 영향 시스템 (NIST 800-53)에 대한 NIST 800-53 제어 선택
- U. S. 정부 구성 기준선 (USGCB)
- General Purpose Operating Systems v4.0 (OSPP v4.0)의 NIAP 보호 프로필
- DISA 운영 체제 보안 요구 사항 가이드 (OS SRG)

이전에 여러 개의 프로필이 제거되거나 병합되었습니다. (BZ#1410914)

16장. 서버 및 서비스

chrony 버전 3.1로 업데이트

chrony 패키지가 업스트림 버전 3.1로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 개선 사항은 다음과 같습니다.

- 정확도를 높이기 위해 소프트웨어 및 하드웨어 타임스탬프 지원이 추가되었습니다(마이크로초 정확도가 가능할 수 있음).
- symmetric 네트워크 지니터로 정확도가 향상되었습니다.
- interleaved 모드에 대한 지원이 추가되었습니다.
- 인증을 명령 키로 교체하기 위해 Unix 도메인 소켓에 대한 구성 및 모니터링 지원이 추가되었습니다(원격 구성은 더 이상 가능하지 않음).
- 서버 자동 교체 기능이 향상되었습니다.
- ntpd 데몬과 호환되는 고립 모드가 추가되었습니다.
- NTP 서버에 대한 응답 속도 제한이 추가되었습니다.
- 정보 형식의 문서를 대체하는 자세한 도움말 페이지를 추가했습니다. (BZ#1387223)

linuxptp 버전 1.8로 다시 기반

linuxptp 패키지가 업스트림 버전 1.8로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 개선 사항은 다음과 같습니다.

- 대규모 네트워크의 네트워크 트래픽을 줄이기 위해 유니캐스트 메시지를 사용하여 하이브리드 종단 간(E2E) 지연 측정 지원이 추가되었습니다.
- PTP(독립 정밀 시간 프로토콜) 하드웨어 클럭을 사용하여 경계 클럭(BC) 실행 지원이 추가되었습니다.

- PTP 메시지의 TTL(Time to Live) 및 서로 다른 서비스 코드 포인트(DSCP)를 구성하는 옵션이 추가되었습니다. (BZ#1359311)

tuned 버전 2.8.0로 다시 기반

tuned 패키지가 업스트림 버전 2.8.0로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- CPU 파티션 프로파일이 추가되었습니다.
- 코어 격리 지원이 추가되었습니다.
- initrd 오버레이에 대한 지원이 추가되었습니다.
- 상속이 향상되었습니다.
- udev 장치 관리자를 기반으로 하는 regexp 장치 일치가 구현되었습니다. (BZ#1388454, BZ#1395855, BZ#1395899, BZ#1408308, BZ#1394965)

logrotate 는 이제 /var/lib/logrotate/logrotate.status 를 기본 상태 파일로 사용합니다.

이전에는 logrotate cron 작업에서 logrotate 상태 파일에 대한 수정된 경로를 사용했습니다. 결과적으로 cron 작업에서 사용하는 경로가 logrotate 자체에서 사용하는 기본 상태 파일 경로와 일치하지 않았습니다. 혼동을 방지하기 위해 logrotate 에서 사용하는 기본 상태 파일 경로가 logrotate cron 작업에서 사용하는 상태 파일 경로와 일치하도록 변경되었습니다. 결과적으로 logrotate 는 이제 두 시나리오에서 /var/lib/logrotate/logrotate.status 를 기본 상태 파일 경로로 사용합니다. (BZ#1381719)

rsyslog 버전 8.24.0으로 업데이트

rsyslog 유틸리티는 업스트림 버전 8.24.0을 기반으로 하며 수많은 개선 사항, 새로운 기능 및 버그 수정이 포함되어 있습니다. 주요 개선사항은 다음과 같습니다.

- 새로운 코어 엔진이 구현되어 더 빠른 메시지 처리를 제공합니다.
- JSON 형식의 데이터를 처리할 때 속도 및 안정성이 향상되었습니다.

- **RainerScript** 구성 형식은 기본값으로 선택되었으며 더 많은 옵션을 사용하여 개선되었습니다.

- 외부 애플리케이션을 사용하여 **rsyslog** 내에서 메시지를 조작하기 위한 새로운 **mmexternal** 모듈이 추가되었습니다.

- **omprog** 모듈은 외부 바이너리와 더 나은 통신을 위해 개선 사항을 받았습니다.

- 모듈 **imrelp** 및 **omrelp** 는 이제 **TLS** 프로토콜을 사용하여 암호화된 전송을 지원합니다.

- **imuxsock** 모듈에서는 글로벌 규칙 세트를 재정의하는 개별 소켓에 대한 규칙 세트를 지원합니다.

- **imuxsock** 모듈을 사용하는 경우 속도 제한 메시지에 이제 속도 제한을 유발하는 프로세스의 **PID**가 포함됩니다.

- 이제 **TCP** 서버 오류 메시지에 원격 호스트의 **IP** 주소가 포함됩니다.

- **imjournal** 모듈은 영구 **journald** 구성으로 전환한 후 더 이상 로그 수신을 중지하지 않습니다.

- 시스템의 시계가 이전 시간으로 설정된 경우 재부팅 후 런타임 저널에 대한 로깅이 더 이상 완전히 중지되지 않습니다.

- 이전에는 **copytruncate** 옵션이 있는 **logrotate** 유틸리티에서 로그 파일을 순환하면 **imfile** 모듈에서 순환되는 파일에서 모든 로그 메시지를 읽지 못할 수 있었습니다. 결과적으로 이러한 로그 메시지가 손실되었습니다. 이 문제를 해결하기 위해 **imfile** 모듈이 확장되었습니다. **consquence** 에서 **logrotate copytruncate** 를 로그 파일에 사용하면 메시지가 더 이상 손실되지 않습니다.

사용자 지정 모듈을 사용하는 고객은 현재 **rsyslog** 버전에 대한 모듈을 업데이트하는 것이 좋습니다.

더 이상 사용되지 않는 **rsyslog** 옵션에 대한 자세한 내용은 더 이상 사용되지 않는 기능 장을 참조하십시오. **(BZ#1313490, BZ#1174345, BZ#1053641, BZ#1196230, BZ#1326216, BZ#1088021, BZ#1419228, BZ#1133687)**

mod_nss에 대한 새로운 캐시 구성 옵션

이번 업데이트에서는 mod_nss 모듈에 OCSP 응답의 cahing을 제어하는 새로운 옵션이 추가되었습니다. 새로운 옵션을 통해 사용자는 다음을 제어할 수 있습니다.

- OCSP 응답을 기다리는 시간
- OCSP 캐시 크기
- 항목의 존재 여부에 대한 최소 기간 및 최대 기간 (BZ#1392582)

데이터베이스 및 접두사 옵션이 nss_pcache에서 제거됨

nss_pcache pin-caching 서비스는 더 이상 mod_nss Apache 모듈의 NSS(Network Security Services) 데이터베이스를 공유하지 않습니다. nss_pcache 는 토큰에 액세스할 필요가 없기 때문입니다. NSS 데이터베이스 및 접두사에 대한 옵션이 제거되어 이제 mod_nss 에 의해 자동으로 처리됩니다. (BZ#1382102)

새 패키지: libfastjson

이번 업데이트에서는 libfastjson 라이브러리를 rsyslog 의 json-c 라이브러리를 대체합니다. libfastjson 의 제한된 기능 세트를 사용하면 json-c 에 비해 성능이 크게 향상됩니다. (BZ#1395145)

tuned 에서 initrd 오버레이 지원

tuned 는 이제 기본(Dracut) initrd 이미지를 확장할 수 있는 initrd 오버레이를 지원합니다. 부트 로더 플러그인에서 지원합니다. 예에서는 Tuned 프로파일의 일반적인 사용법을 보여줍니다.

```
[bootloader]
initrd_add_dir=${i:PROFILE_DIR}/overlay.img
```

그러면 프로필이 활성화될 때 overlay.img 디렉터리의 콘텐츠가 현재 initrd에 추가됩니다. (BZ#1414098)

openwsman 은 이제 특정 SSL 프로토콜 비활성화 지원

이전에는 openwsman 유틸리티를 사용하여 특정 SSL 프로토콜을 비활성화할 수 있는 방법이 없었습니다. 비활성화된 프로토콜 목록에 대한 새로운 구성 파일 옵션이 추가되었습니다. 그 결과 openwsman 구성 파일을 통해 특정 SSL 프로토콜을 비활성화할 수 있습니다. (BZ#1190689)

rear 버전 2.0으로 업데이트

Red Hat Enterprise Linux 7에서 여러 버그를 수정하고 다양한 개선 사항을 추가하는 **rear** 패키지를 업데이트했습니다. 주요 변경 사항은 다음과 같습니다.

- 이제 **XFS** 파일 시스템에서 **CRC(Cyclic** 중복 검사) 기능이 기본적으로 활성화되어 있습니다. 이전에는 이 변경 사항을 동작으로 다시 무시하고 호환되지 않는 **UUID** 플래그를 사용하여 **/boot** 파티션을 포맷했습니다. 이로 인해 복구 프로세스가 실패했습니다. 이 리베이스를 사용하면 **CRC** 기능을 다시 확인하고 복구 중에 **UUID**를 적절하게 유지합니다.

- **IBM Power Systems** 아키텍처에 대한 **GRUB** 및 **GRUB2** 부트 로더 지원이 추가되었습니다.

- **/usr/share/rear/conf/default.conf** 구성 파일에서 **NETFS_ingressgatewayORE_CAPABILITIES** 지시문이 **y** 옵션으로 설정된 경우 **Linux** 기능이 보존됩니다.

- 이제 **CIFS** 인증 정보가 복구 이미지에 보존됩니다.

- **GRUB_SUPERUSER** 및 **GRUB_RESCUE_PASSWORD** 지시문이 삭제되어 현재 실행 중인 시스템에서 **GRUB2** 부트로더의 예기치 않은 동작이 변경되지 않습니다.

- 문서가 개선되었습니다.

- 여러 백업 생성이 활성화되었습니다. **(BZ#1355667)**

python-tornado 버전 **4.2.1**로 업데이트

python-tornado 패키지가 업스트림 버전 **4.2.1**로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 새 기능을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- **DNS** 확인을 위한 비동기 인터페이스를 제공하는 새로운 **tornado.netutil.Resolver** 클래스

- 새로운 **tornado.tcpclient** 모듈은 비차단 **DNS, SSL** 핸드킹 및 **IPv6** 지원을 사용하여 **TCP** 연결을 생성합니다.

- **IOLoop.instance()** 함수는 스레드로부터 안전

- 로깅이 향상되었습니다. 낮은 수준의 로그는 덜 빈번합니다. **Tornado** 는 루트 로거 대신 자체 로거를 사용하므로 보다 자세한 구성이 가능합니다.

- 여러 참조 주기는 **python-tornado** 내에서 구분되어 **CPython**에서 보다 효율적인 가비지 컬렉션을 가능하게 합니다.

- 코루틴은 이제 더 빠르고 **Tornado** 내에서 광범위하게 사용됩니다. (BZ#1158617)

17장. 스토리지

RAID 수준 사용을 위해 LVM에 추가된 지원

LVM에서는 이전에 기술 프리뷰로 사용 가능한 RAID 인수에 대한 전체 지원을 제공하므로 사용자가 RAID 논리 볼륨을 하나의 RAID 수준에서 다른 RAID 수준으로 변환할 수 있습니다. 이번 릴리스에서는 RAID takeover 조합 수가 확장됩니다. 일부 전환에 대한 지원은 중간 단계가 필요할 수 있습니다. RAID 사용 방법을 통해 추가된 새로운 RAID 유형은 이전 릴리스 커널 버전에서 지원되지 않습니다. 이러한 RAID 유형은 raid0, raid0_meta, raid5_n 및 raid6_{ls,rs,la,ra,n}_6입니다. 이러한 RAID 유형을 생성하거나 Red Hat Enterprise Linux 7.4에서 RAID 유형으로 변환하는 사용자는 이전 릴리스를 실행하는 시스템에서 논리 볼륨을 활성화할 수 없습니다. RAID takeover는 단일 머신 모드의 최상위 논리 볼륨에서만 사용할 수 있습니다(즉, 클러스터 볼륨 그룹 또는 RAID가 스냅샷 또는 씬 풀의 일부인 동안 takeover를 사용할 수 없음). (BZ#1366296)

LVM에서 RAID 복구 지원

LVM에서 RAID 복구 기능을 지원합니다. takeover를 사용하면 사용자가 하나의 RAID 유형에서 다른 RAID 유형으로 변경할 수 있지만, reshaping을 사용하면 RAID 알고리즘, 스트라이프 크기, 지역 크기 또는 이미지 수와 같은 속성을 변경할 수 있습니다. 예를 들어, 사용자는 두 개의 추가 장치를 추가하여 3방향 스트라이프를 5방향 스트라이프로 변경할 수 있습니다. Reshaping은 단일 시스템 모드에서 최상위 논리 볼륨에서만 사용할 수 있으며 논리 볼륨이 사용되지 않는 경우에만 사용할 수 있습니다(예: 파일 시스템에서 마운트되는 경우). (BZ#1191935, BZ#834579, BZ#1191978, BZ#1392947)

장치 매퍼 선형 장치는 이제 DAX 지원

dm-linear 및 dm-stripe 대상에 직접 액세스 (DAX) 지원이 추가되었습니다. 이제 다중 Volatile Dual In-line Memory Module(NVDIMM) 장치를 결합하여 더 큰 PVM(영구 메모리) 블록 장치를 제공할 수 있습니다. (BZ#1384648)

libstoragemgmt 버전 1.4.0으로 다시 시작

libstoragemgmt 패키지가 업스트림 버전 1.4.0으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 다음 라이브러리가 추가되었습니다.

- Query serial number of local disk: lsm_local_disk_serial_num_get()/lsm.LocalDisk.serial_num_get()
- Query LED status of local disk: lsm_local_disk_led_status_get()/lsm.LocalDisk.led_status_get()
- Query link speed of local disk: lsm_local_disk_link_speed_get()/lsm.LocalDisk.link_speed_get()

주요 버그 수정 사항은 다음과 같습니다.

- Dell PowerEdge RAID 컨트롤러 (PERC)의 megaraid 플러그인이 수정되었습니다.
- NVM(NVMe) 디스크의 로컬 디스크 회전 속도 쿼리가 수정되었습니다.
- 로컬 디스크 쿼리에 대한 lsmcli 잘못된 오류 처리가 수정되었습니다.
- gcc 컴파일 경고가 모두 수정되었습니다.
- autoconf AC_OUTPUT 매크로의 더 이상 사용되지 않는 사용이 수정되었습니다. (BZ#1403142)

15.100.00.00 버전으로 업데이트

MPT3sas 스토리지 드라이버가 버전 15.100.00.00으로 업데이트되어 새 장치에 대한 지원이 추가되었습니다. 자세한 내용은 공급 업체에 문의하십시오. (BZ#1306453)

lpfc 드라이버의 lpfc_no_hba_reset 모듈 매개 변수를 사용할 수 있습니다.

이번 업데이트에서는 lpfc _no_hba_reset 모듈 매개변수를 추가하여 HBA(Fibulex Fibre Channel Host Bus Adapters) 모델의 lpfc 드라이버가 향상되었습니다. 이 매개변수는 SCSI 오류 처리 중에 재설정하지 않는 HBA의 하나 이상의 16진수 전체 포트 번호(WkubeconfigN) 목록을 허용합니다.

이제 lpfc 를 통해 SCSI 오류 처리 시간 동안 HBA를 재설정할 수 있는 포트를 제어할 수 있습니다. 또한 lpfc 를 사용하면 SCSI 오류 처리 시간의 상한을 나타내는 eh_deadline 매개 변수를 설정할 수 있습니다. (BZ#1366564)

LVM에서 Veritas Dynamic Multi-Pathing 시스템을 감지하고 더 이상 기본 장치 경로에 직접 액세스하지 않습니다.

LVM이 Veritas Dynamic Multi-Pathing을 사용하여 제대로 작동하려면 설정 파일 /etc/lvm/lvm.conf 의 devices 섹션에서 obtain_device_list_from_udev 를 0으로 설정해야 합니다. 이러한 다중 경로 장치는 표준 udev 인터페이스를 통해 노출되지 않으므로 LVM이 없는 경우 해당 존재를 인식하지 못합니다. (BZ#1346280)

libnvdimm 커널 하위 시스템은 이제 PMEM 서브디언을 지원합니다.

Intel의 NVMe(Non-Volatile Dual In-line Memory Module) 라벨 사양이 확장되어 리전별로 둘 이상의

영구 메모리(PMEM) 네임스페이스를 구성할 수 있습니다(interleave 설정). Red Hat Enterprise Linux 7.4와 함께 제공되는 커널은 이러한 새로운 구성을 지원하도록 수정되었습니다.

서브디vision 지원이 없으면 이전에는 pmem,장치 dax 또는 섹터 의 단일 모드만 사용할 수 있었습니다. 이번 업데이트를 통해 단일 리전을 세분화할 수 있으며 각 하위 리전은 서로 독립적으로 구성할 수 있습니다. (BZ#1383827)

multipathd 가 실행되지 않는 경우 경고 메시지

다중 경로가 실행되지 않는 동안 다중 경로 장치를 생성하거나 나열하는 다중 경로 명령을 실행하면 사용자에게 경고 메시지가 표시됩니다.

multipathd 가 실행되고 있지 않은 경우 장치는 실패한 경로를 복원하거나 장치 설정 변경 사항에 대응할 수 없습니다. 다중 경로 장치가 있고 multipathd 가 실행되지 않는 경우 multipathd 데몬이 경고 메시지를 출력합니다. (BZ#1359510)

구조화된 출력을 제공하기 위해 multipathd에 C 라이브러리 인터페이스 추가

이제 libdmmp 라이브러리를 사용하여 multipathd에서 구조화된 정보를 가져올 수 있습니다. multipathd에서 정보를 가져오려는 다른 프로그램에서 명령을 실행하고 결과를 구문 분석하지 않고도 이 정보를 얻을 수 있습니다. (BZ#1430097)

새 제거 다중 경로 구성 값

다중 경로 장치가 일시적으로 사용 중인 경우 다중 경로 장치 제거가 실패합니다. 이제 remove_retries 구성 값을 설정하여 사용 중인 다중 경로 장치 제거를 다시 시도하는 횟수를 제어할 수 있습니다. 기본값은 0이며, 이 경우 다중 경로 다시 시도 실패가 제거되지 않습니다. (BZ#1368211)

새 multipathd reset multipaths stats 명령

다중 경로에서는 두 개의 새 다중 경로 명령을 지원합니다. multipathd reset multipaths statistics 및 multipathd reset multipath d reset dev statistics . 이러한 명령은 다중 경로가 모든 장치 또는 지정된 장치에 대해 각각 추적하는 장치 통계를 재설정합니다. 이를 통해 사용자는 장치 통계를 변경한 후 재설정할 수 있습니다. (BZ#1416569)

new disable_changed_wwids mulitpath 설정 매개변수

다중 경로에서는 새로운 multipath.conf 기본값 섹션 매개변수, disable_changed_wwids 를 지원합니다. 이 값을 설정하면 경로 장치가 사용 중인 동안 wwid를 변경하고 wwid가 이전 값으로 돌아갈 때까지 경로 장치에 대한 액세스를 비활성화하는 경우 이 알림을 받습니다.

scsi 장치의 wwid가 변경되면 장치가 다른 LUN에 다시 매핑되었음을 나타냅니다. scsi 장치를 사용하는 동안 이 문제가 발생하면 데이터 손상이 발생할 수 있습니다. disable_changed_wwids 매개변수를 설정하면 scsi 장치가 wwid를 변경할 때 사용자에게 경고합니다. 대부분의 경우 다중 경로가 원래 LUN에서

매핑 해제되지 않는 즉시 경로 장치에 대한 액세스를 비활성화하여 손상 가능성을 제거합니다. 그러나 **multipathd** 는 **scsi** 장치가 다시 매핑되기 전에 변경 사항을 항상 **catch**할 수 있는 것은 아니므로 손상에 대한 창이 계속 있을 수 있습니다. 사용 중인 **scsi** 장치는 현재 지원되지 않습니다. **(BZ#1169168)**

HPE 3PAR 어레이의 업데이트된 내장 구성

이제 **3PAR** 어레이의 기본 제공 구성에서 **no_path_retry** 를 **12**로 설정합니다. **(BZ#1279355)**

NFINIDAT InfiniBox.* 장치에 대한 기본 제공 구성 추가

다중 경로의 자동 구성 **NFINIDAT InfiniBox.*** 장치 **(BZ#1362409)**

device-mapper-multipath 에서 **max_sectors_kb** 구성 매개변수를 지원

이번 업데이트를 통해 **device-mapper-multipath** 는 **multipath.conf** 파일의 **defaults, devices** 및 **multipaths** 섹션에 새로운 **max_sectors_kb** 매개변수를 제공합니다. **max_sectors_kb** 매개변수를 사용하면 다중 경로 장치를 먼저 활성화하기 전에 **max_sectors_kb** 장치 대기열 매개변수를 다중 경로의 모든 기본 경로에 지정된 값으로 설정할 수 있습니다.

다중 경로 장치가 생성되면 장치는 경로 장치에서 **max_sectors_kb** 값을 상속합니다. 다중 경로 장치의 이 값을 수동으로 늘리거나 경로 장치의 이 값을 낮추면 다중 경로 장치에서 허용하는 경로 장치보다 큰 **I/O** 작업을 생성할 수 있습니다.

max_sectors_kb multipath.conf 매개 변수를 사용하면 경로 장치 상단에 다중 경로를 생성하기 전에 이러한 값을 쉽게 설정할 수 있으며 잘못된 **I/O** 작업이 전달되지 않도록 합니다. **(BZ#1394059)**

새로운 **detect_checker** 다중 경로 구성 매개변수

VNX2와 같은 일부 장치는 선택적으로 **ALUA** 모드로 구성할 수 있습니다. 이 모드에서는 비**ALUA** 모드와 다른 **path_checker** 및 우선순위 를 사용해야 합니다. 다중 경로에서는 **multipath.conf** 기본값 및 **devices** 섹션에서 **detect_checker** 매개변수를 지원합니다. 이 값을 설정하면 다중 경로가 **ALUA**를 지원하는지 여부를 감지하며, 이렇게 하면 구성된 **path_checker** 를 재정의하고 대신 **TUR** 검사기를 사용합니다. **detect_checker** 옵션을 사용하면 선택적 **ALUA** 모드가 있는 장치를 해당 모드와 관계없이 올바르게 자동 구성할 수 있습니다. **(BZ#1372032)**

멀티패스에 **Nimble** 스토리지 장치에 대한 기본 구성이 내장되어 있습니다.

이제 다중 경로 기본 하드웨어 테이블에 **Nimble** 스토리지 어레이에 대한 항목이 포함됩니다. **(BZ#1406226)**

LVM에서 **RAID** 논리 볼륨의 크기 축소 지원

Red Hat Enterprise Linux 74에서는 **lvreduce** 또는 **lvresize** 명령을 사용하여 **RAID** 논리 볼륨의 크기를 줄일 수 있습니다. **(BZ#1394048)**

iprutils 버전 2.4.14로 다시 시작

iprutils 패키지가 업스트림 버전 **2.4.14**로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 사항:

- **endian swapped device_id**가 이전 버전과 호환됩니다.
- 베어 메탈 모드에서 **VSET** 쓰기 캐시가 허용됩니다.
- 듀얼 어댑터 설정에서 **RAIDS** 생성이 수정되었습니다.
- 단일 어댑터 구성에 대한 재빌드 확인은 기본적으로 비활성화되어 있습니다. **(BZ#1384382)**

mdadm 버전 4.0으로 업데이트

mdadm 패키지가 업스트림 버전 **4.0**으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 특히 이번 업데이트에서는 **Intel Matrix Storage Manager(IMSM)** 메타데이터에 대한 잘못된 블록 관리 지원이 추가되었습니다. 이 업데이트에 포함된 기능은 외부 메타데이터 형식에서 지원되며 **Red Hat**은 **Intel Hyperconverged Storage Technology enterprise (Intel RSTe)** 소프트웨어 스택을 계속 지원합니다. **(BZ#1380017)**

thin 풀이 50%를 초과할 때 LVM에서 씬 풀의 크기를 확장합니다.

씬 풀 논리 볼륨이 **50%** 이상 채워지면 기본적으로 **dmeventd thin** 플러그인에서 **dmeventd thin_command** 명령을 **5%** 증가시킵니다. 이렇게 하면 구성 파일의 활성화 섹션에 구성된 **thin_pool_autoextend_threshold** 위에 채워진 씬 풀의 크기가 조정됩니다. 사용자는 외부 명령을 구성하고 **lvm.conf** 파일의 **dmeventd** 섹션에서 이 명령을 **thin_command** 값으로 지정하여 이 기본값을 덮어쓸 수 있습니다. 씬 플러그인 및 씬 풀을 유지 관리하기 위해 외부 명령을 구성하는 방법은 **dmeventd(8)** 매뉴얼 페이지를 참조하십시오.

이전 릴리스에서는 씬 풀 크기 조정에 실패한 경우 **dmeventd** 플러그인은 **95 %** 이상의 컴파일 시간 정의 임계값에 도달할 때 **thin pool**와 연결된 모든 씬 볼륨을 무조건 마운트 해제하려고 합니다. 기본적으로 **dmeventd** 플러그인은 더 이상 볼륨을 마운트 해제하지 않습니다. 이전 논리를 재현하려면 외부 스크립트를 구성해야 합니다. **(BZ#1442992)**

LVM에서 dm-cache 메타데이터 버전 2 지원

LVM/DM 캐시가 크게 개선되었습니다. 이는 더 큰 캐시 크기를 지원하고, 워크로드 변경, 시작 및 종료 시간을 크게 개선하며 전반적인 성능이 향상됩니다. 이제 **LVM**을 사용하여 캐시 논리 볼륨을 생성할 때 **dm-cache** 메타데이터 형식의 버전 **2**가 기본값입니다. 이전에 생성된 **LVM** 캐시 논리 볼륨에 대해 버전 **1**

이 계속 지원됩니다. 버전 2로 업그레이드하려면 이전 캐시 계층을 제거하고 새 캐시 계층을 생성해야 합니다. (BZ#1436748)

지정된 하드웨어에서 DIF/DIX (T10PI) 지원

SCSI T10 DIF/DIX는 하드웨어 공급 업체가 이를 인증하고 특정 HBA 및 스토리지 어레이 구성에 대한 완전한 지원을 제공하는 경우 Red Hat Enterprise Linux 7.4에서 완전하게 지원됩니다. DIF/DIX는 다른 구성에서 지원되지 않으며 부팅 장치에서는 지원되지 않으며 가상화된 게스트에서 지원되지 않습니다.

현재 다음 공급업체는 이러한 지원을 제공하는 것으로 알려져 있습니다.

FUJITSU는 DIF 및 DIX를 지원합니다.

EMULEX 16G FC HBA:

- EMULEX LPe16000/LPe16002, 10.2.254.0 BIOS, 10.4.255.23 FW는 다음과 같습니다.
- FUJITSU ETERNUS DX100 S3, DX500 S3, DX500 S3, DX8100 S3, DX8700 S3, DX8900 S3, DX200F, DX60 S3, AF650

QLOGIC 16G FC HBA:

- QLOGIC QLE2670/QLE2672, 3.28 BIOS, 8.00.00 FW, with:
- FUJITSU ETERNUS DX100 S3, DX500 S3, DX600 S3, DX8100 S3, DX8700 S3, DX8900 S3, DX200F, DX60 S3

T10 DIX에는 디스크 블록에서 체크섬의 생성 및 검증을 제공하는 데이터베이스 또는 기타 소프트웨어가 필요합니다. 현재 지원되는 Linux 파일 시스템에는 이 기능이 없습니다.

EMC는 DIF를 지원합니다.

EMULEX 8G FC HBA:

- 펌웨어 **2.01a10** 이상이 포함된 **LPe12000** 및 **LPe12002-E.**

- **Enginuity 597 Vertical EMC Symmetrix VMAX** 시리즈와 **Enginuity 5876.82.57** 이상이 포함된 **EMC VMAX3** 시리즈

EMULEX 16G FC HBA:

- **10.0.803.25** 이상이 포함된 **LPe16000B-E** 및 **LPe16002B-E:**

- **Enginuity 597 Vertical EMC Symmetrix VMAX** 시리즈와 **Enginuity 5876.82.57** 이상이 포함된 **EMC VMAX3** 시리즈

QLOGIC 16G FC HBA:

- **QLE2670-E-SP** 및 **QLE2672-E-SP,** 다음과 같이

- **Enginuity 597 Vertical EMC Symmetrix VMAX** 시리즈와 **Enginuity 5876.82.57** 이상이 포함된 **EMC VMAX3** 시리즈

최신 상태는 하드웨어 공급 업체의 지원 정보를 참조하십시오.

DIF/DIX 지원은 다른 **HBA** 및 스토리지 어레이의 기술 프리뷰로 남아 있습니다. **(BZ#1457907)**

dmstats 기능은 이제 변경되는 파일의 통계를 추적할 수 있습니다.

이전에는 **dmstats** 기능이 크기가 변경되지 않은 파일의 통계를 보고할 수 있었습니다. 이제 파일의 변경 사항을 감시하고 파일 크기가 변경되는 경우에도 파일 **I/O**를 추적하도록 파일을 업데이트하고 매핑을 업데이트할 수 있습니다(또는 파일에 있을 수 있는 홀을 채우기). **(BZ#1378956)**

캐시된 논리 볼륨의 씬 스냅샷 지원

Red Hat Enterprise Linux 7.4의 **LVM**을 사용하면 캐시된 논리 볼륨의 씬 스냅샷을 생성할 수 있습니다. 이 기능은 이전 릴리스에서 제공되지 않았습니다. 이러한 외부 원본 캐시 논리 볼륨은 읽기 전용 상태로 변환되므로 다른 씬 풀에서 사용할 수 있습니다. **(BZ#1189108)**

새 패키지: nvmetcli

nvmetcli 유틸리티를 사용하면 NVME-over-RDMA 패브릭 유형을 사용하여 Red Hat Enterprise Linux를 NVMEoF 대상으로 구성할 수 있습니다. nvmetcli 를 사용하면 대화형으로 nvmet 을 구성하거나 JSON 파일을 사용하여 구성을 저장하고 복원할 수 있습니다. (BZ#1383837)

NVDIMM 장치에 장치 DAX를 사용할 수 있습니다.

장치 DAX를 사용하면 하이퍼바이저 및 데이터베이스와 같은 사용자가 파일 시스템을 방해하지 않고도 영구 메모리에 원시 액세스할 수 있습니다. 특히 장치 DAX를 사용하면 애플리케이션에서 예측 가능한 오류 세부 정보와 사용자 공간으로부터 데이터를 지속성 도메인으로 플러시할 수 있습니다. Red Hat Enterprise Linux 7.4부터 Device Dax는 NVDIMM(Non-Volatile Dual In-line Memory Module) 장치에 사용할 수 있습니다. (BZ#1383489)

yum에 새로운 payload_gpgcheck 옵션이 추가되었습니다.

이번 업데이트를 통해 새로운 구성 옵션 **payload_gpgcheck** 가 **yum** 유틸리티에 추가되었습니다. 이 옵션을 사용하면 패키지의 페이로드 섹션에서 **GPG(GNU** 개인 정보 보호 보안) 서명 검사를 활성화하여 패키지를 설치할 때 보안 및 무결성을 향상시킬 수 있습니다. 이전에는 **gpgcheck** 옵션이 활성화된 경우 **yum** 은 헤더에서만 **GPG** 서명 검사를 수행했습니다. 결과적으로 페이로드 데이터가 변조되거나 손상된 경우 **RPM** 압축 해제 오류가 발생하고 패키지가 부분적으로 설치된 상태로 남아 있었습니다. 이로 인해 운영 체제가 일관되지 않고 취약한 상태가 될 수 있습니다.

이러한 문제를 방지하기 위해 **gpgcheck** 또는 **localpkg_gpgcheck** 옵션과 함께 새로운 **payload_gpgcheck** 옵션을 사용할 수 있습니다. 결과적으로 **payload_gpgcheck** 가 활성화되면 **yum** 은 페이로드에서 **GPG** 서명 검사를 수행하고 확인되지 않은 경우 트랜잭션을 중단합니다. **payload_gpgcheck** 를 사용하는 것은 다운로드한 패키지에서 **rpm -K** 를 수동으로 실행하는 것과 동일합니다. **(BZ#1343690)**

virt-who에 no-proxy 설정을 사용할 수 있습니다.

이번 업데이트를 통해 프록시 네트워크 설정을 무시하도록 **virt-who** 서비스를 설정할 수 있습니다. 이를 통해 **virt-who** 는 단방향 통신과 프록시 연결을 사용하는 환경에서 제대로 작동할 수 있습니다.

이 기능을 설정하려면 **NO_PROXY** 환경 변수를 **/etc/sysconfig/virt-who** 파일에 추가합니다. 또는 **/etc/rhsm/rhsm.conf** 파일의 **[server]** 섹션에 **no_proxy** 변수를 추가할 수 있습니다.

Red Hat Satellite 5를 사용하여 하이퍼바이저를 동기화할 때 **NO_PROXY** 설정이 작동하지 않습니다. **(BZ#1299643)**

virt-who respects independent interval settings

이번 업데이트를 통해 **virt-who** 명령은 업데이트가 있는 모든 소스의 각 간격을 보고합니다. 또한 **virt-who** 가 두 개 이상의 대상에 업데이트를 전송하도록 구성된 경우(예: **Red Hat Satellite** 인스턴스 및 **RHSM(Red Hat Subscription Management)**에 대한 간격은 별도로 유지 관리됩니다. 즉, 다른 대상과의 통신 상태에 관계없이 모든 업데이트를 구성된 각 대상으로 보낼 수 있습니다. **(BZ#1436811)**

virt-who-password에 암호 옵션이 추가되었습니다.

이번 업데이트를 통해 **virt-who-password** 유틸리티에 **-p** 및 **--password** 옵션이 추가되었습니다. 이를 통해 스크립트에서 유틸리티를 사용할 수 있습니다. **(BZ#1426058)**

정규식과 와일드카드를 일부 **virt-who** 구성 매개변수에서 사용할 수 있습니다.

이번 업데이트를 통해 **filter_hosts** 및 **exclude_hosts** 구성 매개변수에서 정규식과 와일드카드를 사용할 수 있습니다. 이를 통해 **virt-who** 는 훨씬 더 쉽게 보고할 호스트 목록을 유지 관리할 수 있습니다.

정규식과 와일드카드를 사용하여 보고하거나 제외할 호스트를 지정하면 호스트 목록이 훨씬 더 간결할 수 있습니다. (BZ#1405967)

virt-who 설정 파일을 보다 쉽게 관리할 수 있습니다.

이제 virt-who 서비스는 .conf 확장자로 끝나는 /etc/virt-who.d/ 디렉토리에 있는 설정 파일만 사용합니다. 이를 통해 테스트 또는 백업과 같이 virt-who 구성 파일을 보다 쉽게 관리할 수 있습니다. (BZ#1369107)

19장. 가상화

Amazon Web Services의 ENA 드라이버

이번 업데이트에서는 Red Hat Enterprise Linux 7 커널에 ENA(Amazon Elastic Network Adapter) 드라이버에 대한 지원이 추가되었습니다. ENA는 Amazon Web Services 클라우드의 특정 인스턴스 유형에 대해 Red Hat Enterprise Linux 7 게스트 가상 머신의 네트워킹 효율성을 크게 향상시킵니다.

ENA에 대한 자세한 내용은 https://aws.amazon.com/blogs/aws/elastic-network-adapter-high-performance-network-interface-for-amazon-ec2 을 참조하십시오. (BZ#1357491, BZ#1410047)

합성 Hyper-V FC 어댑터는 storvsc 드라이버에서 지원됩니다.

이번 업데이트에서는 Hyper-V 가상화에서 storvsc 드라이버가 파이버 채널(FC) 장치를 처리하는 방식이 향상되었습니다. 특히 새로운 합성 파이버 채널(FC) 어댑터가 Hyper-V 하이퍼바이저에 구성된 경우 새 hostX (예: host1) 파일이 /sys/class/fc_host/ 및 /sys/class/scsi_host/ 디렉터리에 생성됩니다. 이 파일에는 Hyper-V FC Adapter의 세계 전체 포트 번호(WWNN)에 의해 결정되는 port_name 및 host_name 항목이 포함되어 있습니다. (BZ#1308632, BZ#1425469)

부모 HBA는 WWNN/WWPN 쌍으로 정의할 수 있습니다.

이번 릴리스에서는 scsi_host# 외에도 WWNN(WWNN) 및 World Wide Port Name(WANDN)으로 상위 호스트 버스 어댑터(HBA)를 식별할 수 있습니다. scsi_host# 에서 정의한 경우 하드웨어가 호스트 시스템에 추가되면 호스트 시스템이 재부팅된 후 scsi_host#이 변경될 수 있습니다. WWNN/WWPN 쌍을 사용하면 호스트 시스템에 대한 하드웨어 변경과 관계없이 할당은 변경되지 않은 상태로 유지됩니다. (BZ#1349696)

libvirt 버전 3.2.0으로 다시 기반

libvirt 패키지가 업스트림 버전 3.2.0으로 업그레이드되어 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항:

- 이번 업데이트를 통해 특정 libvirt 스토리지 하위 드라이버를 설치하고 제거할 수 있으므로 설치 공간이 줄어듭니다.
- 이제 NSS(Name Services Switch)에 KVM 게스트 이름을 네트워크 주소로 자동으로 확인하도록 /etc/nsswitch.conf 파일을 구성할 수 있습니다. (BZ#1382640)

KVM에서 MCE 지원

이번 업데이트에서는 KVM 커널 모듈에 MCE(Machine Check Exception) 지원이 추가되어 KVM 게스트 가상 머신에서 Intel Xeon v5 프로세서의 LSCE(Local MCE) 기능을 사용할 수 있습니다. LMCE는 모든 스레드에 브로드캐핑하는 대신 단일 프로세서 스레드에 MCE를 제공할 수 있으므로 시스템 검사에서

필요한 것보다 많은 vCPU의 성능에 영향을 미치지 않습니다. 결과적으로 많은 프로세서 스레드가 있는 머신에서 MCE를 처리할 때 소프트웨어 로드가 줄어듭니다. (BZ#1402102, BZ#1402116)

tun/tap 장치에서 rx batching에 대한 지원 추가

이번 릴리스에서는 tun/tap 장치에 대한 rx 일괄 처리가 지원됩니다. 이를 통해 번들된 네트워크 프레임을 수신하여 성능을 향상시킬 수 있습니다. (BZ#1414627)

libguestfs 버전 1.36.3으로 업데이트

libguestfs 패키지가 업스트림 버전 1.36.3으로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. 주요 변경 사항은 다음과 같습니다.

- 이번 업데이트에서는 tail -f 명령과 유사하게 게스트 내의 로그 파일을 후속(세부 정보)하는 데 사용할 수 있는 virt-tail 유틸리티가 추가되었습니다. 자세한 내용은 virt-tail(1) 매뉴얼 페이지를 참조하십시오.

- virt-v2v 유틸리티는 더 많은 운영 체제 및 더 많은 입력 소스를 지원합니다. 또한 Windows 게스트의 변환이 크게 다시 작성되고 단순화되었습니다.

- virt-customize,virt-builder, virt-systprep 유틸리티에 대해 여러 옵션이 추가되었습니다. (BZ#1359086)

QXL 드라이버의 virt-v2v 설치 개선

이번 업데이트에서는 Windows 게스트 가상 머신에서 QXL 드라이버 설치의 virt-v2v 구현이 다시 작동하여 QXL 드라이버가 이러한 게스트에 올바르게 설치되도록 합니다. (BZ#1233093, BZ#1255610, BZ#1357427, BZ#1374651)

virt-v2v 는 디스크 이미지를 qcow2 형식 1.1로 내보낼 수 있습니다.

이번 업데이트를 통해 -o rhev 옵션을 사용하는 경우 virt-v2v 유틸리티는 qcow2 형식 버전 1.1과 호환되는 디스크 이미지를 내보냅니다. 또한 virt-v2v 는 vdsm 출력 모드에 --vdsm-compat=COMPAT 옵션을 추가합니다. 이 옵션은 -o vdsm 옵션으로 이미지를 내보낼 때 virt-v2v 가 사용하는 qcow2 형식의 버전을 지정합니다. (BZ#1400205)

LUKS 전체 디스크 암호화 게스트에서 추가 virt 툴을 사용할 수 있습니다.

이번 업데이트에서는 virt-customize,virt-get-kernel,virt-sparsify, virt-sysprep 툴을 사용하여 LUKS 전체 디스크 암호화 게스트 작업을 지원합니다. 결과적으로 이러한 툴은 LUKS 전체 디스크 암호화 게스트를 열기 위한 키 또는 암호를 제공할 수 있습니다. (BZ#1362649)

모든 libguestfs 명령에 대한 탭 완료

모든 **libguestfs** 툴에 대해 **Bash** 완료 스크립트가 추가되었습니다. 결과적으로 모든 **libguestfs** 명령과 함께 **bash**에서 **Tab** 완료를 사용할 수 있습니다. (BZ#1367738)

크기 조정 디스크를 원격 위치에 직접 작성할 수 있습니다.

이번 업데이트를 통해 **virt-resize** 유틸리티에서 출력을 원격 위치에 쓸 수 있습니다. 예를 들어 **Ceph** 스토리지 볼륨에 크기 조정 디스크 이미지를 직접 작성할 때 유용할 수 있습니다. **URI**를 사용하여 **virt-resize** 출력 디스크를 지정할 수 있습니다. 지원되는 모든 입력 프로토콜 및 형식을 사용하여 출력을 지정할 수 있습니다. (BZ#1404182)

사용자 네임스페이스가 완전히 지원됨

이전에 기술 프리뷰로 사용 가능한 사용자 네임스페이스 기능이 이제 완전히 지원됩니다. 호스트와 컨테이너 간에 더 나은 격리를 제공하여 **Linux** 컨테이너를 실행하는 서버에 추가 보안을 제공합니다. 컨테이너 관리자는 더 이상 호스트에서 관리 작업을 수행할 수 없으므로 보안이 향상됩니다. (BZ#1138782)

Hyper-V에서 게스트 가상 머신에서 PCI Express 버스를 통해 연결하는 장치에 드라이버 추가

이번 업데이트에서는 **PCI Express** 버스를 통해 연결되는 장치가 **Hyper-V** 하이퍼바이저에서 실행되는 **Red Hat Enterprise Linux** 게스트 가상 머신에 전달될 때 루트 **PCI** 버스를 노출하는 새로운 드라이버가 추가되었습니다. 이 기능은 현재 **Microsoft Windows Server 2016**에서 지원됩니다. (BZ#1302147)

20장. ATOMIC HOST 및 컨테이너

Red Hat Enterprise Linux Atomic Host

Red Hat Enterprise Linux Atomic Host는 Linux 컨테이너 실행을 위해 최적화된 안전한 경량의 운영 체제입니다. 최신 새로운 기능, 알려진 문제 및 기술 프리뷰는 **Atomic Host** 및 **Containers** 릴리스 노트를 참조하십시오.

21장. RED HAT SOFTWARE COLLECTIONS

Red Hat Software Collections는 **AMD64** 및 **Intel 64** 아키텍처에서 지원되는 모든 **Red Hat Enterprise Linux 6** 및 **Red Hat Enterprise Linux 7** 릴리스에 설치하고 사용할 수 있는 일련의 동적 프로그래밍 언어, 데이터베이스 서버 및 관련 패키지를 제공하는 **Red Hat** 콘텐츠 집합입니다. **Red Hat Developer Toolset**은 별도의 소프트웨어 컬렉션에 포함되어 있습니다.

Red Hat Developer Toolset은 **Red Hat Enterprise Linux** 플랫폼을 사용하는 개발자를 위해 설계되었습니다. 현재 **GNU** 컴파일러 컬렉션, **GNU Debugger** 및 기타 개발, 디버깅 및 성능 모니터링 툴을 제공합니다. **Red Hat Software Collections 2.3**부터는 **Eclipse** 개발 플랫폼이 별도의 소프트웨어 컬렉션으로 제공됩니다.

Red Hat Software Collections와 함께 배포된 동적 언어, 데이터베이스 서버 및 기타 툴은 **Red Hat Enterprise Linux**로 제공되는 기본 시스템 툴을 대체하지 않으며 이러한 툴을 선호하는 툴을 사용하지 않습니다. **Red Hat Software Collections**는 **scl** 유틸리티를 기반으로 하는 대체 패키징 메커니즘을 사용하여 병렬 패키지 세트를 제공합니다. 이 세트를 사용하면 **Red Hat Enterprise Linux**에서 대체 패키지 버전을 선택적으로 사용할 수 있습니다. **scl** 유틸리티를 사용하면 언제든지 실행할 패키지 버전을 선택할 수 있습니다.

중요

Red Hat Software Collections는 **Red Hat Enterprise Linux**보다 라이프사이클과 지원 기간이 짧습니다. 자세한 내용은 **Red Hat Software Collections** 제품 라이프 사이클 을 참조하십시오.

개별 소프트웨어 컬렉션의 세트, 시스템 요구 사항, 알려진 문제, 사용 및 세부 사항에 포함된 구성 요소에 대한 **Red Hat Software Collections** 설명서 를 참조하십시오.

이 소프트웨어 컬렉션, 설치, 사용, 알려진 문제 등에 포함된 구성 요소에 대한 자세한 내용은 **Red Hat Developer Toolset** 설명서 를 참조하십시오.

II 부. 주요 버그 수정

이 부분에서는 **Red Hat Enterprise Linux 7.4**에서 사용자에게 상당한 영향을 미치는 버그 수정에 대해 설명합니다.

22장. 일반 업데이트

Addition of CtrlAltDelBurstAction for Systemd

/etc/systemd/system.conf (BZ#1353028)에 CtrlAltDelBurstAction 옵션을 설정하여 여러 CTRL+ALT+DEL 이벤트에 대한 systemd 응답을 구성할 수 있습니다.

Cgred 는 NSS 사용자 및 그룹과 관련된 규칙을 수정할 수 있습니다.

이전에는 이름 서비스 스위치(NSS) 사용자 및 그룹을 제공하는 서비스 후 cgred 서비스가 시작되지 않았습니다. 또한 유효하지 않은 규칙을 건너뛰는 방법에 대한 정보는 디버그 모드에서만 표시되었습니다. 결과적으로 NSS 사용자 및 그룹과 관련된 cgrules.conf 파일의 규칙은 로그 메시지 없이 무시되었습니다. 이번 업데이트를 통해 cgred 는 nss-user-lookup 대상과 건너뛰기 규칙에 대한 로그 메시지 수준이 경고로 변경되어 cgred 데몬의 기본 로그 수준도 설정됩니다. 결과적으로 cgred 를 시작하기 전에 NSS 사용자와 그룹이 항상 해결됩니다. 또한 cgrules.conf 의 일부 규칙이 유효하지 않은 경우 경고 메시지가 기록됩니다. (BZ#1406927)

23장. 인증 및 상호 운용성

yum 은 설치 후 패키지 충돌을 더 이상 보고하지 않습니다. **ipa-client**

사용자가 **ipa-client** 패키지를 설치한 후 **yum** 유틸리티에서 예기치 않게 보고된 **ipa** 패키지와 **freeipa** 패키지 간의 충돌을 보고했습니다. 실패한 트랜잭션 후 또는 **yum check** 명령을 사용한 후 이러한 오류가 발생했습니다. 이번 업데이트를 통해 **yum** 은 **RPM**에서 이러한 충돌이 발생할 수 있으므로 더 이상 자체 구성 패키지에 대한 오류를 보고하지 않습니다. 그 결과 **yum** 은 **ipa-client** 을 설치한 후 설명 된 오류를 더 이상 표시하지 않습니다. **(BZ#1370134)**

FIPS 모드에서 **slapd_pk11_getInternalKeySlot()** 함수가 토큰의 키 슬롯을 검색하는 데 사용됩니다.

Red Hat Directory Server는 보안 데이터베이스에서 **FIPS** 모드가 활성화되면 이전에 고정 토큰 이름에서 키 슬롯을 검색하려고 했습니다. 그러나 토큰 이름은 변경될 수 있습니다. 키 슬롯을 찾을 수 없는 경우 **Directory Server**에서 복제 관리자의 암호를 디코딩할 수 없으며 복제 세션이 실패합니다. 이 문제를 해결하기 위해 **slapd_pk11_getInternalKeySlot()** 함수는 이제 **FIPS** 모드를 사용하여 현재 키 슬롯을 검색합니다. 결과적으로 **SSL** 또는 **STTARTTLS** 를 사용하는 복제 세션이 더 이상 설명된 상황에서 실패하지 않습니다. **(BZ#1378209)**

인증서 시스템이 **FIPS** 모드의 시스템에 **Thales HSM**을 사용하여 더 이상 설치되지 않습니다.

Thales 하드웨어 보안 모듈**(HSM)**을 사용하여 **CS(Certificate System)**를 설치한 후 **HSM**에서 모든 시스템 키를 생성한 경우 **SSL** 프로토콜이 제대로 작동하지 않았습니다. 결과적으로 **FIPS** 모드가 활성화된 시스템에 **CS**가 설치되지 않았으므로 **server.xml** 파일에서 **sslRangeCiphers** 매개변수를 수동으로 수정해야 합니다. 이 버그가 수정되었으며 **Thales HSM**이 적용된 **FIPS** 지원 시스템이 예상대로 작동합니다. **(BZ#1382066)**

이제 **pkispawn** 의 종속성 목록이 올바르게 포함됩니다. **openssl**

이전 버전에서는 **openssl** 패키지가 설치되지 않은 경우 **pkispawn** 유틸리티를 사용하여 다음 오류와 함께 실패했습니다.

```
Installation failed: [Errno 2] No such file or directory
```

openssl 패키지가 **pki-core** 패키지에 포함된 **pki-server** 패키지의 런타임 종속성으로 포함되지 않았기 때문에 이 문제가 발생했습니다. 이 버그는 누락된 종속성을 추가하여 수정되었으며 **openssl** 누락되어 더 이상 **pkispawn** 설치가 실패하지 않습니다. **(BZ#1376488)**

PKI Server 프로필 프레임워크의 오류 메시지가 클라이언트에 전달됩니다.

이전에는 **PKI** 서버가 프로필 프레임워크에서 클라이언트에 대한 인증서 요청에 의해 생성된 특정 오류 메시지를 전달하지 않았습니다. 결과적으로 웹 **UI**에 표시되는 오류 메시지 또는 **pki** 명령 출력에 표시된 오류 메시지에서 요청이 실패한 이유를 설명하지 않았습니다. 코드가 수정되어 이제 오류 메시지를 통과합니다. 이제 사용자가 등록이 실패했거나 거부된 이유를 확인할 수 있습니다. **(BZ#1249400)**

인증서 시스템이 설치 중에 **Lightweight CA** 키 복제를 시작하지 않음

이전에는 2단계 설치 중에 인증서 시스템에서 Lightweight CA 키 복제를 잘못 시작했습니다. 이로 인해 설치에 실패하고 오류가 표시되었습니다. 이번 업데이트를 통해 2단계 설치가 Lightweight CA 키 복제를 시작하지 않고 설치가 성공적으로 완료됩니다. (BZ#1378275)

이제 PKI Server가 시작 중에 주체 DN을 올바르게 비교

기본 CA에 대한 Lightweight CA 항목을 추가하는 루틴의 버그로 인해 UTF8String 이외의 인코딩을 사용하는 속성이 포함된 경우 이전에는 PKI Server에서 제목 고유 이름(DN)을 비교하지 못했습니다. 그 결과 기본 CA가 시작될 때마다 추가 경량 CA 항목이 추가되었습니다. PKI 서버는 이제 주체 DN을 표준 형식으로 비교합니다. 결과적으로 PKI 서버는 더 이상 언급 된 시나리오에 추가 경량 CA 항목을 추가하지 않습니다. (BZ#1378277)

불완전한 인증서 체인을 사용하여 중간 CA에 연결할 때 KRA 설치가 더 이상 실패하지 않습니다.

이전에는 KRA(키 복구 기관) 하위 시스템을 설치하면 KRA에서 신뢰할 수 있는 CA 인증서가 있지만 루트 CA 인증서가 없는 중간 CA에 연결하려고 하면 UNKNOWN_ISSUER 오류와 함께 실패했습니다. 이번 업데이트를 통해 KRA 설치에서 오류를 무시하고 성공적으로 완료됩니다. (BZ#1381084)

인증서 프로필의 startTime 필드에서 이제 긴 정수 형식을 사용합니다.

이전에는 인증서 시스템의 startTime 필드에 값을 정수 로 저장했습니다. 더 큰 숫자를 입력했으면 인증서 시스템이 해당 값을 음수로 해석했습니다. 결과적으로 인증 기관은 과거에 위치한 시작 날짜가 포함된 인증서를 발급했습니다. 이번 업데이트에서는 startTime 필드의 입력 형식이 긴 정수로 변경되었습니다. 결과적으로 발급된 인증서가 이제 올바른 시작 날짜를 갖습니다. (BZ#1385208)

PKCS#11 토큰으로 인해 하위 CA 설치가 더 이상 실패하지 않습니다.

이전에는NSS(Network Security Services) 라이브러리의 버그로 인해 하위 인증 기관(sub-CA)을 설치할 수 없어 SEC_ERROR_TOKEN_NOT_LOGGED_IN 오류가 발생했습니다. 이번 업데이트에서는 설치를 계속할 수 있는 설치 프로그램에 해결방법이 추가되었습니다. 오류가 계속 표시되면 이제 무시해도 됩니다. (BZ#1395817)

이제 pkispawn 스크립트가 ECC 키 크기를 올바르게 설정

이전 버전에서는 사용자가 Elliptic Curve Cryptography (ECC) 키 크기 매개변수를 사용하여 pkispawn 스크립트를 실행했을 때 nistp256 인 기본값이 아닌 다른 값으로 설정된 pkispawn 스크립트를 실행할 때 설정이 무시되었습니다. 결과적으로 생성된 PKI Server 인스턴스가 시스템 인증서를 발행하여 기본 ECC 키 곡선을 잘못 사용했습니다. 이번 업데이트를 통해 PKI 서버는 ECC 키 곡선 이름에 대해 pkispawn 구성에 설정된 값을 사용합니다. 그 결과, 이제 PKI 서버 인스턴스에서 인스턴스를 설정할 때 ECC 키 크기 세트를 사용합니다. (BZ#1397200)

FIPS 모드에서 CA 복제 설치가 더 이상 실패하지 않습니다.

이전 버전에서는 내부 NSS 토큰 이름을 처리하는 불일치로 인해 CA 복제 또는 KRA(키 복구 기관)를 FIPS 모드에서 설치할 수 없었습니다. 이번 업데이트를 통해 토큰 이름을 처리하는 코드가 통합되어 모든 토큰 이름을 일관되게 처리할 수 있습니다. t는 KRA 및 CA 복제 설치를 FIPS 모드에서 제대로 완료할 수 있습니다. (BZ#1411428)

entryUSN 속성에 32비트보다 큰 값이 포함된 경우 **PKI Server**가 더 이상 시작되지 않습니다.

이전에는 *LDAP 프로필 모니터"와 엔트리USN 속성의 값을 32비트 정수로 구문 분석했습니다. 결과적으로 속성에 해당 값보다 큰 값이 포함된 경우 **NumberFormatException** 오류가 기록되어 서버가 시작되지 않았습니다. 문제가 해결되었으며 서버는 더 이상 언급 된 시나리오에서 시작되지 않습니다. (BZ#1412681)

Tomcat 은 기본적으로 **IPv6** 에서 작동합니다.

IPv4- 특정 **127.0.0.1** 루프백 주소는 이전에 기본 서버 구성 파일에서 기본 **NetNamespace** 호스트 이름으로 사용되었습니다. 이로 인해 **IPv6-** 전용 환경에서 실행되는 서버에서 연결이 실패했습니다. 이번 업데이트를 통해 기본값은 **IPv4** 및 **IPv6** 프로토콜 모두에서 작동하는 **localhost** 로 변경됩니다. 또한 업그레이드 스크립트를 사용하여 기존 서버 인스턴스에서 **RuntimeClass** 호스트 이름을 자동으로 변경할 수 있습니다. (BZ#1413136)

pkispawn 은 더 이상 유효하지 않은 **NSS** 데이터베이스 암호를 생성하지 않습니다.

이번 업데이트 이전에는 **pkispawn** 이 **NSS** 데이터베이스에 대한 임의의 암호를 생성했으며 경우에 따라 백슬래시(\) 문자가 포함되어 있었습니다. 이로 인해 **NSS** 가 설정된 **SSL** 연결 시 문제가 발생하여 **ACCESS_SESSION_ESTABLISH_FAILURE** 오류가 발생했습니다.

이번 업데이트를 통해 무작위로 생성된 암호에 백슬래시 문자를 포함할 수 없으며 연결을 항상 설정할 수 있으므로 설치가 성공적으로 완료됩니다. (BZ#1447762)

--serial 옵션을 사용하여 사용자 인증서를 추가할 때 인증서 검색에 더 이상 실패하지 않습니다.

이전에 **--serial** 매개변수와 함께 **pki user-cert-add** 명령을 사용하면 **CA**(인증 기관)에 대한 **SSL** 연결을 잘못 설정하여 인증서 검색에 실패했습니다. 이번 업데이트를 통해 이 명령에서는 **CA**에 올바르게 구성된 **SSL** 연결을 사용하고 작업이 성공적으로 완료됩니다. (BZ#1246635)

항목이 하나만 있는 경우 **CA** 웹 인터페이스에 더 이상 빈 인증서 요청 페이지가 표시되지 않습니다.

이전에는 **CA** 웹 사용자 인터페이스의 인증서 요청 페이지에 하나의 항목만 포함된 경우 단일 항목을 표시하는 대신 빈 페이지가 표시되었습니다. 이번 업데이트에서는 웹 사용자 인터페이스가 수정되고 인증서 요청 페이지에 모든 상황에서 항목이 올바르게 표시됩니다. (BZ#1372052)

컨테이너 환경에 **PKI** 서버를 설치하면 더 이상 경고가 표시되지 않습니다.

이전에는 컨테이너 환경에 **pki-server RPM** 패키지를 설치할 때 **systemd** 데몬이 다시 로드되었습니다. 그 결과 경고가 표시되었습니다. **RPM**을 업그레이드하는 동안만 데몬을 다시 로드하기 위한 패치가 적용되었습니다. 그 결과 언급된 시나리오에 경고가 더 이상 표시되지 않습니다. (BZ#1282504)

G&D 스마트 카드를 사용하여 토큰을 다시 등록하지 않습니다.

이전에는 **Gies1.8.0e & Devrient (G&D)** 스마트 카드를 사용하여 토큰을 다시 등록할 때 특정 상황에서 토큰 등록에 실패할 수 있었습니다. 문제가 해결되어 토큰을 다시 등록하면 예상대로 작동합니다.

(BZ#1404881)

PKI Server는 시작 시 인증서 유효성 검사 오류에 대한 자세한 정보를 제공합니다.

이전에는 서버를 시작할 때 인증서 유효성 검사 오류가 발생한 경우 **PKI** 서버에서 충분한 정보를 제공하지 않았습니다. 그 결과 문제 해결이 어려웠습니다. **PKI** 서버는 이제 새로운**JSS(Java Security Services) API**를 사용하여 언급된 시나리오에서 오류의 원인에 대한 자세한 정보를 제공합니다. (BZ#1330800)

PKI 서버는 더 이상 **LDAPProfileSubsystem** 프로필을 다시 초기화하지 않습니다.

LDAPProfileSubsystem 프로필을 다시 시작하는 동안 경쟁 조건으로 인해 이전에는 **PKI** 서버가 요청된 프로필이 존재하지 않는 것으로 잘못 보고할 수 있었습니다. 결과적으로 프로필 사용 요청이 실패할 수 있었습니다. 문제가 해결되었으며 프로필 사용 요청이 더 이상 실패하지 않습니다. (BZ#1376226)

HSM에서 생성된 개인 키 추출이 더 이상 실패하지 않습니다.

이전 버전에서는 키 복구 에이전트(KRA)에서 새 **Asymmetric Key Generation REST** 서비스를 사용하여 **Lunasa** 또는 **Thales** 하드웨어 보안 모듈(HSM)에서 **symmetric** 키를 생성할 때 **PKI Server**에서 잘못된 플래그를 설정했습니다. 결과적으로 사용자는 생성된 개인 키를 검색할 수 없었습니다. 이 **HSM**에서 생성된 키에 대해 올바른 플래그를 설정하도록 코드가 업데이트되었습니다. 결과적으로 사용자는 언급된 시나리오에서 개인 키를 검색할 수 있습니다. (BZ#1386303)

pkispawn 은 더 이상 숫자로만 구성된 암호를 생성하지 않습니다.

이전에는 **pkispawn** 에서 숫자만 구성된 **NSS** 데이터베이스에 대해 임의의 암호를 생성할 수 있었습니다. 이러한 암호는 **FIPS**와 호환되지 않습니다. 이번 업데이트를 통해 설치 프로그램이 숫자, 소문자, 대문자 및 특정 문장으로 구성된 **FIPS** 호환 임의의 암호를 생성하도록 수정되었습니다. (BZ#1400149)

이제 올바른 신뢰 플래그를 사용하여 **CA** 인증서를 가져옵니다.

이전에는 **pki client-cert-import** 명령에서는 다른 **PKI** 툴과 불충분하고 일치하지 않는 **CT,c, trust** 플래그를 사용하여 **CA** 인증서를 가져왔습니다. 이번 업데이트를 통해 명령이 수정되었으며 **CA** 인증서의 신뢰 플래그를 **vGPU ,C,C** 으로 설정합니다. (BZ#1458429)

--usage 확인 옵션을 사용할 때 대칭 키 생성이 더 이상 실패하지 않습니다.

pki 유틸리티는 생성되는 대칭 키에 대한 유효한 사용 목록을 확인합니다. 이전에는 이 목록에 사용 검증이 누락되었습니다. 그 결과 **key-generate --usage verify** 옵션을 사용하면 오류 메시지가 반환됩니다. 코드가 수정되었으며 이제 **verify** 옵션이 예상대로 작동합니다. (BZ#1238684)

이후의 **PKI** 설치가 더 이상 실패하지 않습니다.

이전에는 여러 **PKI**(공개 키 인프라) 인스턴스를 배치 모드로 설치할 때 **CA** 인스턴스가 다시 시작될 때까지 설치 스크립트가 대기하지 않았습니다. 결과적으로 후속 **PKI** 인스턴스 설치에 실패할 수 있었습니다. 스크립트가 업데이트되어 새 하위 시스템이 계속 요청을 처리하기 전에 새 하위 시스템이 요청을 처리할 준비가 될 때까지 기다립니다. (BZ#1446364)

FIPS 모드에서 2 단계 하위 CA 설치가 더 이상 실패하지 않습니다.

이전 버전에서는 **FIPS** 모드의 하위 **CA** 설치 버그로 인해 설치 프로그램에서 두 번째 단계에 인스턴스가 존재하지 않기 때문에 **2**단계 설치가 실패했습니다. 이번 업데이트에서는 첫 번째 단계(설치)에 인스턴스가 존재하지 않도록 워크플로가 변경되고 두 번째 단계(구성)에는 인스턴스가 있어야 합니다.

이전 **pki_skip_configuration** 및 **pki_skip_installation** 배포 매개변수를 교체하기 위해 **pkispawn** 명령에 **'--skip-configuration'** 및 **--skip-installation** 라는 두 가지 새로운 옵션이 추가되었습니다. 이렇게 하면 수정 없이 두 단계에 대해 동일한 배포 구성 파일을 사용할 수 있습니다. **(BZ#1454450)**

인증서 요청이 거부되거나 취소된 경우 감사 로그가 더 이상 성공 상태를 기록하지 않습니다.

이전에는 인증서 요청이 거부되거나 취소된 경우 서버에서 **Outcome=Success** 를 사용하여 **CERT_REQUEST_PROCESSED** 감사 로그 항목을 생성했습니다. 요청에 대해 인증서가 발급되지 않았기 때문에 이 문제가 발생했습니다. 이 버그는 수정되었으며 **accordingRT _REQUEST_PROCESSED** 감사 로그 항목이 거부되거나 취소된 요청에 대한 이제 **Outcome=Failure** 입니다. **(BZ#1452250)**

자체 테스트에 실패한 PKI 하위 시스템이 이제 시작 시 자동으로 다시 활성화됨

이전 버전에서는 자체 테스트 실패로 인해 **PKI** 하위 시스템을 시작하지 못하면 일관성 없는 상태에서 실행되지 않도록 자동으로 비활성화되었습니다. 관리자는 문제를 수정한 후 **pki-server** 하위 시스템을 사용하여 수동으로 하위 시스템을 다시 활성화 할 것으로 예상됩니다. 그러나 이는 명확하게 전달되지 않아서 이러한 요구 사항을 항상 인식하지 못한 관리자 간의 혼란을 초래할 수 있었습니다.

이 문제를 완화하기 위해 기본적으로 모든 **PKI** 하위 시스템이 시작 시 자동으로 다시 활성화됩니다. 자체 테스트에 실패하면 하위 시스템은 이전처럼 비활성화되지만 수동 강화는 더 이상 필요하지 않습니다.

이 동작은 **/etc/pki/pki.conf** 파일 **PKI_SERVER_AUTO_ENABLE_SUBSYSTEMS** 의 새 부울 옵션으로 제어합니다. **(BZ#1454471)**

CERT_REQUEST_PROCESSED 감사 로그 항목에 인코딩 데이터 대신 인증서 일련 번호가 포함됩니다.

이전 버전에서는 **CE_REQUEST_PROCESSED** 감사 로그 항목이 **Base64**로 인코딩된 인증서 데이터가 포함되었습니다. 예:

```
[AuditEvent=CERT_REQUEST_PROCESSED]...[InfoName=certificate][InfoValue=MIIDBD...]
```

인증서 데이터는 별도로 디코딩해야 하므로 이 정보가 매우 유용하지 않았습니다. 다음 예와 같이 인증서 일련 번호를 로그 항목에 직접 포함하도록 코드가 변경되었습니다.

```
[AuditEvent=CERT_REQUEST_PROCESSED]...[CertSerialNum=7]
```

(BZ#1452344)

LDAPProfileSubsystem 프로파일 업데이트에서 속성 제거 지원

이전에는 **PKI Server**에서 **LDAPProfileSubsystem** 프로필을 업데이트할 때 속성을 제거할 수 없었습니다. 따라서 **PKI Server**가 특정 상황에서 프로필을 업데이트한 후 프로필을 로드하거나 인증서를 발행할 수 없었습니다. 패치가 적용되었으며 이제 **PKI Server**는 새 구성을 로드하기 전에 기존 프로필 구성을 지웁니다. 결과적으로 **LDAPProfileSubsystem** 프로필의 업데이트는 이제 구성 속성을 제거할 수 있습니다. (BZ#1445088)

24장. 클러스터링

클러스터에 대한 연결이 관리되지 않는 경우에도 Pacemaker Remote가 종료될 수 있습니다.

이전에는 **Pacemaker** 원격 연결이 관리되지 않는 경우 **Pacemaker** 원격 데몬에서 클러스터에서 종료를 확인하지 못했습니다. 결과적으로 **Pacemaker Remote**를 종료할 수 없었습니다. 이번 수정으로 **Pacemaker** 원격 연결이 관리되지 않는 경우 이제 클러스터가 리소스가 중지될 때까지 기다리지 않고 종료를 요청하는 **Pacemaker** 원격 노드에 즉시 보냅니다. 결과적으로 클러스터에 대한 연결이 관리되지 않는 경우에도 **Pacemaker Remote**가 종료될 수 있습니다. **(BZ#1388489)**

pcs 에서 원격 및 게스트 노드의 이름 및 호스트 확인

이전 버전에서는 **pcs** 명령에서 원격 또는 게스트 노드의 호스트 이름이 리소스 **ID**와 충돌했는지 또는 클러스터 노드와 충돌했는지 확인하지 않아 클러스터가 제대로 작동하지 않았습니다. 이번 수정으로 관련 명령에 검증이 추가되어 **pcs** 에서 사용자가 충돌하는 이름이나 원격 또는 게스트 노드의 호스트와 충돌하는 클러스터를 구성할 수 없습니다. **(BZ#1386114)**

pcs resource create 명령의 **master** 옵션의 새 구문으로 메타 속성을 올바르게 생성할 수 있습니다.

이전에는 **pcs** 리소스 생성 명령에 **--master** 플래그가 포함된 경우 키워드 **meta** 가 마스터 메타 속성으로 해석된 모든 옵션이 있었습니다. 이로 인해 **--master** 플래그가 지정될 때 프리미티브에 대한 메타 속성을 생성할 수 없었습니다. 이번 수정에서는 명령에 다음 형식을 사용하여 리소스를 마스터 슬레이브 복제본으로 지정하는 새 구문을 제공합니다.

```
pcs resource create resource_id standard:provider:type|type [resource options] master
[master_options...]
```

이를 통해 메타 옵션을 다음과 같이 지정할 수 있습니다.

```
pcs resource create resource_id standard:provider:type|type [resource_options] meta meta_options...
master [master_options...]
```

또한 이번 수정을 통해 이전 릴리스와 마찬가지로 **--clone** 플래그 대신 **clone** 옵션을 사용하여 복제 리소스를 지정합니다. 복제본 리소스를 지정하는 새 형식은 다음과 같습니다.

```
pcs resource create resource_id standard:provider:type|type [resource_options] clone
```

(BZ#1378107)

25장. 컴파일러 및 도구

이제 PCRE 라이브러리가 유니코드에 필요한 대로 ASCII가 아닌 문자를 올바르게 인식합니다.

이전에는 Perl compatibleible Regular Expressions (PCRE) 라이브러리를 사용하여 ASCII가 아닌 문자와 유니코드 문자열을 일치시킬 때 라이브러리에서 출력 가능한 ASCII가 아닌 문자를 올바르게 인식할 수 없었습니다. 패치가 적용되었으며 PCRE 라이브러리는 이제 UTF-8 모드에서 출력 가능한 ASCII가 아닌 문자를 인식합니다. (BZ#1400267)

Bundler 를 사용하여 종속성을 관리하는 애플리케이션에서 JSON 라이브러리를 올바르게 로드할 수 있습니다.

이전에는 Bundler 를 사용하여 Ruby 애플리케이션 종속성을 관리할 때 JSON 라이브러리를 로드하지 못하는 경우가 있었습니다. 결과적으로 LoadError 를 사용하여 애플리케이션이 실패했습니다. 이로 인해 Ruby on Rails 가 더 이상 JSON 라이브러리에 대한 종속성을 명시적으로 지정하지 않기 때문에 특히 문제가 발생했습니다. 이번 업데이트를 통해 JSON 은 항상 로드 경로에서 사용할 수 있으며 설명된 문제가 더 이상 발생하지 않습니다. (BZ#1308992)

이제 HTTP 또는 HTTPS 및 SSO와 함께 Git 을 사용할 수 있습니다.

libcurl 버전 7.21.7이므로 CVE-2011-2192으로 인해 Kerberos 티켓을 위임하기 위한 새로운 매개 변수가 필요합니다. 이전에는 Git 에서 이러한 매개 변수를 설정하는 방법을 제공하지 않았습니다. 결과적으로 HTTP 또는 HTTPS 연결에 Single Sign-On을 사용하는 데 실패했습니다. 이번 업데이트를 통해 Git 은 cURL --delegation 매개변수에 해당하는 새로운 http.delegation 구성 변수를 제공합니다. 사용자는 Kerberos 티켓을 위임해야 하는 경우 이 매개 변수를 설정해야 합니다. (BZ#1369173)

이제 rescan-scsi-bus.sh --luns=1 을 다시 스캔합니다. 이제 1로 번호가 지정된 LUN만 스캔합니다.

sg3_utils 패키지에는 SCSI 명령을 장치로 보내는 유틸리티가 포함되어 있습니다. 버전 1.28-5 및 이전 버전의 sg3_utils 에서 rescan-scsi-bus.sh --luns=1 명령은 1로 번호가 지정된 논리 단위 번호(LUN)만 다시 스캔했습니다. 버전 1.28-6으로 업데이트한 후 모든 LUN 을 잘못 다시 스캔한 후 --luns=1 을 다시 스캔합니다. 이번 업데이트를 통해 기본 소스 코드가 수정되었으며 재scan -scsi-bus.sh --luns=1 은 1로 번호가 지정된 LUN만 스캔합니다. (BZ#1380744)

ps 는 더 이상 대기 채널 이름에서 접두사를 제거하지 않습니다.

ps 유틸리티는 이전에 sys_ 및 do_ 접두사를 대기 채널(WCHAN) 데이터에서 제거했습니다. 이로 인해 사용자가 ps 출력에 이러한 접두사를 의도적으로 포함하는 이름의 함수를 구분하지 못했습니다. 접두사를 제거하는 코드가 제거되었으며 ps 는 이제 전체 대기 채널 이름이 표시됩니다. (BZ#1373246)

.history 파일이 네트워크 파일 시스템에 있으면 tcsh 가 더 이상 응답하지 않습니다.

이전에는 .history 파일이 NFS 또는 Samba와 같은 네트워크 파일 시스템에 있는 경우 tcsh 명령 언어 인터프리터가 로그인 프로세스 중에 응답하지 않는 경우가 있었습니다. .history 파일 잠금이 네트워크 파일 시스템에 있는 경우 .history 파일 잠금을 방지하기 위해 패치가 적용되었으며 tcsh 는 더 이상 설명된 상황에서 응답하지 않습니다.

tcsh를 여러 개 실행하는 경우 . history가 손상될 수 있습니다. 이 문제를 해결하려면 lock 매개변수를 savehist 옵션에 추가하여 명시적 파일 잠금 메커니즘을 활성화합니다. 예:

```
$ cat /etc/csh.cshrc
# csh configuration for all shell invocations.
set savehist = (1024 merge lock)
```

lock 옵션은 .history 가 네트워크 파일 시스템에 있을 때 tcsh 를 파일 잠금을 사용하도록 강제 적용하려면 savehist 옵션의 세 번째 매개 변수여야 합니다. Red Hat은 lock 매개변수를 사용할 것을 보장하지 않으므로 로그인 프로세스 중에 tcsh 가 응답하지 않게 됩니다. (BZ#1388426)

fcoeadm --target 이 더 이상 fcoeadm 이 충돌하지 않음

이전 버전에서는 fcoeadm --target 명령을 실행하면 fcoeadm 유틸리티가 세그먼트화 오류로 예기치 않게 종료되는 경우가 있었습니다. 이번 업데이트를 통해 fcoeadm 이 비FCoE 대상의 sysfs 경로를 무시하도록 수정되었으며 fcoeadm --target 은 더 이상 fcoeadm 이 충돌하지 않습니다. (BZ#1384707)

tar 옵션 --directory 가 더 이상 무시되지 않음

이전에는 --remove-files 옵션과 함께 사용할 때 tar 명령의 --directory 옵션이 무시되었습니다. 그 결과 현재 작업 디렉터리의 파일은 --directory 옵션으로 지정된 디렉터리에 있는 파일 대신 제거되었습니다. 이 버그를 해결하기 위해 --directory 옵션을 검색, 저장 및 수행하는 새로운 함수 및 속성이 추가되었습니다. 결과적으로 --directory 옵션으로 지정된 디렉터리에서 파일이 올바르게 제거됩니다. (BZ#1319820)

tar 옵션 --xattrs-exclude 및 --xattrs-include 는 더 이상 무시되지 않음

이전에는 tar 명령에서 --xattrs-exclude 및 --xattrs-include 옵션을 무시했습니다. 이 버그를 해결하기 위해 tar 은 확장 특성을 가져올 때 포함 및 마스크를 제외하도록 수정되었습니다. 결과적으로 --xattrs-exclude 및 --xattrs-include 옵션이 더 이상 무시되지 않습니다. (BZ#1341786)

tar 에서 증분 백업을 올바르게 복원합니다.

이전에는 tar 명령이 증분 백업을 올바르게 복원하지 않았습니다. 그 결과 증분 백업에서 삭제된 파일이 복원 시 제거되지 않았습니다. 버그가 수정되었으며 tar 은 이제 증분 백업을 올바르게 복원합니다. (BZ#1184697)

perl-homedir 프로필 스크립트에서 csh를 지원

이전에는 perl-homedir 프로필 스크립트에서 C 쉘 (csh) 구문을 처리할 수 없었습니다. 결과적으로 perl-homedir 패키지가 설치되고 /etc/sysconfig/perl-homedir 파일에 PERL_HOMEDIR=0 행이 포함된 경우 프로파일 스크립트를 실행하면 다음과 같은 오류가 발생했습니다.

```
PERL_HOMEDIR=0: Command not found.
```

이번 업데이트에서는 **csh** 구문에 대한 지원이 추가되어 설명된 문제는 더 이상 발생하지 않습니다. (BZ#1122993)

getaddrinfo 가 초기화되지 않은 데이터에 더 이상 액세스하지 않음

nscd 데몬이 활성화된 시스템에서 **glibc** 라이브러리의 **getaddrinfo()** 함수가 초기화되지 않은 데이터에 액세스할 수 있으므로 잘못된 주소 정보를 반환할 수 있습니다. 이번 업데이트에서는 초기화되지 않은 데이터 액세스를 방지하고 올바른 주소가 반환되도록 합니다. (BZ#1324568)

glibc의 malloc 구현에서 수행되는 추가 보안 검사

이전에는 **glibc** 라이브러리가 어설션 없이 컴파일되었기 때문에 **malloc** 을 구현하는 함수가 힙 일관성을 확인하지 않았습니다. 이로 인해 힙 기반 버퍼 오버플로가 악용될 위험이 높아졌습니다. 힙 일관성 검사가 어설션에서 명시적 확인으로 변환되었습니다. 결과적으로 **glibc** 에서 **malloc** 구현에 대한 호출 보안이 향상되었습니다. (BZ#1326739)

chrpath 버전 0.16으로 다시 시작

chrpath 패키지가 업스트림 버전 **0.16**으로 업그레이드되어 이전 버전에 비해 여러 버그 수정이 제공됩니다. 특히 **chrpath** 툴은 **64**비트 시스템에서 **64**비트 바이너리의 실행 경로 속성만 수정하고 **32**비트 시스템에서 **32**비트 바이너리를 수정할 수 있었습니다. 이 버그가 수정되었으며 **64**비트 시스템의 **chrpath** 는 이제 **64**비트 시스템에서 **32**비트 시스템에 대한 **32**비트 시스템 및 바이너리의 실행 경로를 수정할 수 있습니다. (BZ#1271380)

system-config- language 패키지에 대한 업데이트된 번역

system-config- language 에 대한 누락된 번역을 해결하기 위해 다음 **10**개 언어가 추가되었습니다. **de, es, fr, it, ja, ko, pt_BR, ru, zh_CN, zh_TW. (BZ#1304223)**

호스트 이름에 도메인 부분이 없을 때 redfish 헤더가 불완전한 이메일을 발송하지 않습니다.

이전에는 호스트 이름에 도메인 이름이 포함되지 않은 경우 **Mutt** 이메일 클라이언트에서 호스트 이름이 누락된 **From** 헤더가 있는 이메일을 전송했습니다. 결과적으로 이러한 이메일에 응답하는 것은 불가능했습니다. 이 버그가 수정되었으며 이제 **Mutt** 은 도메인 부분을 포함하지 않는 호스트 이름을 올바르게 처리합니다. (BZ#1388512)

strace 는 open() 함수의 경우 O_TMPFILE 플래그 및 모드를 올바르게 표시합니다.

이전에는 **strace** 유틸리티에서 시스템 함수 **open()** 에 대한 **O_TMPFILE** 플래그의 존재를 인식하지 못했으며 모드 옵션이 있는지 여부가 확인되었습니다. 그 결과 **strace** 출력에 각 플래그의 이름이 표시되지 않았으며 **mode** 옵션 값이 없었습니다. **strace** 유틸리티가 이 상황을 인식하도록 확장되었습니다. 결과적으로 **O_TMPFILE** 플래그 및 모드가 올바르게 표시됩니다. (BZ#1377847)

대규모 프로그램을 연결할 때 더 이상 LD가 무한 루프에 들어가지 않습니다.

IBM Power Systems 아키텍처의 대규모 프로그램에서는 . **text** 세그먼트 가 두 개의 스텁 섹션으로 서비스됩니다. 이전에는 섹션 중 하나가 항상 증가했기 때문에 이러한 세그먼트를 스케일링할 때 **ld** 링커 크기 조정 조건이 충족되지 않았습니다. 결과적으로 **ld** 는 무한 루프를 입력했으며 종료되어야 했습니다.

LD는 이러한 상황을 인식하고 크기 조정 종료 조건을 변경하기 위해 확장되었습니다. 결과적으로 **ld** 가 올바르게 종료됩니다. **(BZ#1406498)**

숨겨진 기호에 대한 개체 간 참조에 대한 골드 경고 메시지

gold 링커는 하나의 라이브러리의 코드가 두 번째 라이브러리 또는 개체 파일의 숨겨진 기호를 참조하는 공유 라이브러리를 연결할 때 경고 메시지를 생성합니다. 이전에는 **gold** 에서 다른 라이브러리 또는 오브젝트 파일에 동일한 기호에 대한 표시 정의를 제공한 경우에도 이 경고 메시지가 생성되었습니다. 이 버그를 해결하기 위해 **gold** 은 이 특정 케이스에 대한 확인으로 연장되었으며 기호의 표시 정의가 없는 경우에만 경고 메시지를 생성합니다. 결과적으로 **gold** 에 더 이상 잘못된 경고 메시지가 표시되지 않습니다. **(BZ#1326710)**

Intel Xeon® C3xxx 프로세서의 **OProfile** 기본 이벤트**(Digitively)** 고정

이전 버전에서는 **Intel Xeon® C3xxx** 프로세서의 **OProfile** 에 대한 기본 사이클 카운트 이벤트에 **Denvertondatabind**가 포함된 잘못된 값이 사용되었습니다. 결과적으로 **OProfile** 샘플링 및 기본 이벤트 사용 계산이 작동하지 않았습니다. 관련 **OProfile** 설정이 수정되었습니다. 결과적으로 기본 이벤트는 이제 **Denverton 6443**이 있는 **Intel Xeon® C3xxx** 프로세서에서 작동합니다. **(BZ#1380809)**

26장. 데스크탑

empathy 는 이제 Google 후에 인증서 체인을 검증할 수 있습니다.

이전에는 **Empathy** 인스턴트 메시징 클라이언트가 체인의 **Equifax Secure Certificate Authority**와 같은 기존 인증 기관을 무시하여 **Google article**의 인증서 체인을 검증할 수 없었습니다. 그 결과, **Empathy** 는 체인에 문제가 없는 경우에도 **Google intended**에 연결할 때 잘못된 인증서에 대해 사용자에게 묻는 메시지를 표시합니다. 이번 업데이트에서는 버그 및 **Empathy** 가 서버에서 반환한 목록에서 비활성화된 기존 인증 기관을 무시하고 유효한 대체 체인을 구성하려고 합니다. **(BZ#1386616)**

27장. 파일 시스템

이제 재시도 타임아웃을 설정하면 SSSD에서 마운트하지 않고도 EgressIP가 시작되지 않을 수 있습니다.

EgressIP 유틸리티를 시작할 때 sss 맵 소스가 맵 정보를 제공할 준비가 되지 않은 경우가 있었지만, sss 는 맵이 존재하지 않고 사용할 수 없는 조건을 구분하기 위한 적절한 오류를 반환하지 않았습니다. 그 결과 자동 마운트가 제대로 작동하지 않았으며, SSSD에서 마운트 하지 않고 EgressIP이 시작되었습니다. 이 버그를 수정하려면 map 이 구성 가능한 시간 동안 오류가 없을 때 SSSD에 마스터 맵 을 다시 시도합니다. 이제 마스터 맵이 읽히고 sssd가 예상대로 시작되도록 재시도 시간 제한을 적절한 값으로 설정할 수 있습니다. (BZ#1101782)

autofs 패키지에 README.autofs-schema 파일과 업데이트된 스키마가 포함됩니다.

samples/autofs.schema 배포 파일이 오래되어 올바르지 않았습니다. 그 결과 다른 사람이 잘못된 LDAP 스키마를 사용하고 있을 수 있습니다. 그러나 사용 중인 스키마 변경은 적용할 수 없습니다.However, a change of the schema in use cannot be enforced. 이번 업데이트로 다음이 가능합니다:

- README.autofs-schema 파일이 추가되어 문제를 설명하고 가능한 경우 사용할 스키마를 권장합니다.
- autofs 패키지에 포함된 스키마가 samples/autofs.schema.new 로 업데이트되었습니다. (BZ#1383910)

NIS 서버에 저장된 맵에 액세스하기 위해 더 이상 자동 마운트 를 다시 시작할 필요가 없습니다.

이전에는 EgressIP 유틸리티 가 시작될 때 NIS 클라이언트 서비스를 대기하지 않았습니다. 그 결과 프로그램 시작 시 네트워크 맵 소스를 사용할 수 없는 경우 마스터 맵을 읽을 수 없고 자동 마운트 서비스를 다시 시작하여 NIS 서버에 저장된 맵에 액세스해야 했습니다. 이번 업데이트를 통해 E gressIP 은 마스터 맵을 사용하여 시작 맵을 가져올 때까지 대기합니다. 결과적으로 자동 마운트 를 통해 NIS 도메인의 맵에 액세스할 수 있으며 모든 부팅 시 EgressIP을 다시 시작할 필요가 없습니다.

구성된 대기 시간 후에도 NIS 맵을 계속 사용할 수 없는 경우 EgressIP 구성 master_wait 옵션을 늘려야 할 수 있습니다. 대부분의 경우 패키지에서 사용하는 대기 시간으로 충분합니다. (BZ#1383194)

EgressIP을 사용하여 로컬 마운트 가용성을 확인하면 실패하기 전에 더 이상 시간 초과가 발생하지 않습니다.

이전에는 로컬 시스템의 바인드 마운트를 사용할 수 있을 것으로 예상되어 sssd가 local로 간주하는 마운트 요청에 대해 서버 가용성 프로브가 수행되지 않았습니다. bind 마운트에 실패한 경우 로컬 시스템의 NFS 마운트를 시도했습니다. 그러나 NFS 서버가 로컬 시스템에서 실행되지 않은 경우 마운트 시도가 실패하기 전에 시간 초과가 발생하는 경우가 있습니다.

bind 마운트가 처음 시도되었지만 실패하는 케이스에 가용성 프로브가 추가되었으며, EgressIP는 이

제 로컬 시스템에서 NFS 서버를 사용하려고 합니다. 결과적으로 로컬 시스템에 바인딩 마운트가 실패하면 로컬 NFS 서버가 실행되지 않으면 로컬 시스템에서 NFS 마운트를 시도하는 폴백이 빠르게 실패합니다. (BZ#1420574)

GFS2 파일 시스템을 읽기 전용으로 마운트할 때 저널이 idle로 표시됩니다.

이전에는 GFS2 파일 시스템을 읽기 전용으로 마운트할 때 커널이 파일 시스템 저널을 유휴 상태로 표시하지 않았습니다. 그 결과 gfs2_log_flush() 함수가 저널에 헤더 블록을 잘못 작성하려고 시도했으며 order-of-order 오류가 기록되었습니다. GFS2 파일 시스템을 읽기 전용으로 마운트할 때 저널 유휴 상태를 표시하는 패치가 적용되었습니다. 그 결과 설명된 시나리오에서 언급된 오류가 더 이상 발생하지 않습니다. (BZ#1213119)

id 명령으로 더 이상 잘못된 UID 및 GID가 표시되지 않습니다.

NFSv4 서버에 연결된 NFSv4 클라이언트에서 Red Hat Enterprise Linux를 실행하면 NFS id mapper 키에서 키가 만료된 후 id 명령에서 잘못된 UID 및 GID가 표시되었습니다. 문제는 만료된 키가 가비지 수집될 때까지 5분 동안 지속되며, 그 후 인증 키에 새 키가 생성되고 id 명령에서 올바른 출력을 제공했습니다. 이번 업데이트를 통해 인증 키 기능이 수정되었으며 id 명령은 더 이상 설명된 상황에서 잘못된 출력을 표시하지 않습니다. (BZ#1408330)

레이블이 지정된 NFS가 기본적으로 꺼져 있습니다.

Red Hat Enterprise Linux NFS 서버의 SELinux 레이블은 일반적으로 NFS 클라이언트에 표시되지 않습니다. 대신 NFS 클라이언트는 서버에 있는 파일에 있는 레이블에 관계없이 nfs_t 유형으로 레이블이 지정된 모든 파일을 확인합니다.

Red Hat Enterprise Linux 7.3부터 NFS 서버는 개별 파일 레이블을 클라이언트에 전달할 수 있습니다. 최근 Fedora 클라이언트와 같은 최근 클라이언트는 해당 파일이 서버에 있는 것과 동일한 레이블로 레이블이 지정된 NFS 파일을 참조하십시오. 이는 특정 경우에 유용하지만 서버가 Red Hat Enterprise Linux 7.3 이상으로 업그레이드된 후 최근 클라이언트의 예기치 않은 액세스 권한 문제로 이어질 수도 있습니다.

레이블이 지정된 NFS 지원은 NFS 서버에서 기본적으로 꺼져 있습니다. security_label 내보내기 옵션을 사용하여 레이블이 지정된 NFS 지원을 다시 활성화할 수 있습니다. (BZ#1406885)

shutdown 상태에 도달하면 mount가 더 이상 무한 루프에 들어가지 않습니다.

EgressIP 마운트가 종료 상태에 도달했으며 마운트 처리 스레드가 종료 알림을 읽기 전에 마운트 요청이 도착하고 처리된 경우 EgressIP 마운트를 정리하지 않고 이전에 종료했던 마운트 처리 스레드가 종료되었습니다. 그 결과 기본 프로그램은 종료 조건에 도달하지 않고 resulting-managed 마운트가 마운트되었으므로 무한 루프를 입력했습니다. 이 버그를 해결하기 위해 이제 각 요청이 처리된 후에 종료 상태 점검이 수행되고, EgressIP 마운트가 종료 상태에 도달하면 정리 작업이 수행됩니다. 그 결과 resulting 데몬은 이제 종료 시 예상대로 종료됩니다. (BZ#1420584)

네임스페이스를 처리할 때 EgressIP이 더 안정적입니다.

이전 버전에서는 **EgressIP** 커널 모듈이 경로의 마지막 구성 요소가 현재 네임스페이스의 마운트 지점인지 여부를 확인할 수 없었습니다. 이 버그로 인해 **E gressIP** 에서 전파 개인 네임스페이스에 복제한 마운트 지점이 이미 있는지 여부를 잘못 결정하지 못하는 경우가 있습니다.

결과적으로 자동 마운트 지점을 마운트하지 못하고 **Too** 많은 수준의 심볼릭 링크가 반환되었습니다. 예를 들어 **sssd** 마운트가 활성화된 동안 **PrivateTmp** 옵션을 사용하는 **systemd** 서비스가 다시 시작된 경우 발생했습니다.

이번 업데이트를 통해 커널에 네임스페이스 인식이 마운트된 검사가 추가되었습니다. 결과적으로 **EgressIP** 마운트 를 포함하는 마운트 네임스페이스가 전파 개인 네임스페이스에 복제되는 경우에 더 탄력적으로 액세스할 수 있습니다.

자세한 내용은 **https://access.redhat.com/articles/3104671** 의 **KBase** 문서를 참조하십시오. **(BZ#1320588)**

28장. 설치 및 부팅

자동 파티셔닝은 IBM z 시리즈의 단일 FBA DASD에 설치할 때 작동합니다.

이전에는 대상 cms 디스크 레이아웃을 사용하여 하나의 고정 블록 아키텍처(FBA)를 사용하여 IBM z Series 시스템에 Red Hat Enterprise Linux 7을 설치할 때 cms 형식의 FBA DASD에서 지원되지 않는 장치에서 여러 파티션을 생성하려고 시도했기 때문에 자동 파티셔닝이 실패했습니다. 이로 인해 디스크가 손상된 설치를 완료했습니다.

이번 업데이트를 통해 설치 관리자는 먼저 대상 DASD에 msdos 파티션 테이블을 생성하여 장치에서 최대 3개의 파티션을 허용합니다. 설치 프로그램이 3개 이하의 파티션만 생성하는 경우 설치에 성공합니다. 설치 프로그램이 별도의 /home 파티션을 생성하지 않도록 autopart --nohome Kickstart 옵션을 사용하는 것이 좋습니다. (BZ#1214407)

Kickstart가 디스크에서 진행해도 Kickstart에 구성된 브리지 활성화가 더 이상 실패하지 않습니다.

이전에는 브리지 장치가 Kickstart 파일에 구성되어 디스크에서 Kickstart 파일을 가져온 경우 네트워크 연결이 부족하여 브리지가 생성되지 않았으며 초기 단계에서 설치에 실패했습니다. 이번 업데이트를 통해 브리지 Kickstart 구성이 초기 단계에서 dracut 툴로 전달됩니다. 결과적으로 dracut 은 설치 초기 단계에서 네트워크가 필요하지 않은 경우에도 브리지 장치를 만들고 활성화할 수 있습니다. (BZ#1373360)

이제 Anaconda에서 암호 없이 사용자를 올바르게 생성할 수 있습니다.

이전에는 대화형 설치 중에 Create User (사용자 만들기) 화면에서 이 계정을 사용하려면 Require a password (암호 확인) 옵션을 선택 해제할 수 없었습니다. 따라서 설치 중에 생성된 모든 사용자 계정에는 암호가 필요합니다. 이 버그가 수정되었으며 이제 암호 없이 사용자를 만들 수 있습니다. (BZ#1380277)

더 이상 open-vm-tools-1.8.0 및 종속 항목을 설치하지 않는 최소 설치

open-vm-tools-desktop 패키지는 이전에 @platform-vmware 패키지 그룹(Virtualization 유틸리티 및 VMWare용 드라이버)에서 기본값으로 표시되었습니다. 이 그룹은 설치에 VMWare 하이퍼바이저를 사용하고 있음을 감지하면 Anaconda 에 의해 자동으로 설치됩니다. 동시에 이 패키지에는 최소한의 설치에 도움이 되지 않는 많은 수의 X 라이브러리를 포함하여 많은 종속 항목이 있으며, 이로 인해 Anaconda에서 불필요한 패키지가 많이 설치되었습니다.

이제 open-vm-tools-desktop 패키지가 @platform-vmware 그룹에서 선택 사항이므로 기본적으로 설치되지 않습니다. 그룹 open-vm-tools 의 다른 패키지는 필수로 유지되므로 기본적으로 설치됩니다. (BZ#1408694)

Anaconda에서 더 이상 유효하지 않은 Kickstart 파일을 생성하지 않습니다.

이전에는 설치 중에 Kickstart 파일을 사용하여 일부 LVM 논리 볼륨(- size= 매개변수)과 비교적 비교적(- percent= 매개변수) 정의된 설치 중에 Kickstart 파일을 설치한 시스템에 저장되는 결과 Kickstart 파일인 anaconda-ks.cfg 는 이 두 매개 변수를 사용하여 모든 논리 볼륨을 정의합니다. 이러한 매개 변수는 함께 사용할 수 없으며 생성된 Kickstart 파일이 유효하지 않았습니다. 이번 업데이트를 통해 Anaconda

는 상대 및 절대 크기의 사용을 올바르게 처리하고 결과 설치 후 Kickstart 파일이 유효합니다. (BZ#1317370)

Anaconda에서 더 이상 이름으로 지정된 RAID 배열을 식별하지 못했습니다.

이전 버전에서는 RAID 배열을 Kickstart 파일의 ignoredisk 또는 clearpart 명령의 이름으로 지정하면 설치 초기 단계에서 RAID 이름을 사용할 수 없기 때문에 설치를 진행할 수 없었습니다. 이번 업데이트에서는 Anaconda 가 /dev/md/ 의 장치를 일치하는 이름으로도 확인하여 RAID 지원이 향상되었습니다. 예를 들어 Kickstart 파일에 ignoredisk --only-use=myraid 명령이 포함된 경우Anaconda 는 이제 /dev/md/myraid 에 있는 어레이도 찾습니다. 이를 통해 설치 관리자는 설치 중 어느 시점에서나 이름으로 지정된 RAID 배열을 찾을 수 있으며 Kickstart 파일에서 RAID 배열 이름만 지정할 수 있습니다. (BZ#1327439)

Kickstart가 너무 짧은 암호를 더 이상 허용하지 않음

이전에는 Kickstart 파일을 사용하여 Red Hat Enterprise Linux 7을 설치할 때 Anaconda 설치 프로그램은 암호가 충분히 강력한 경우(기본적으로 품질 값 50 이상)인 경우 --minlen Kickstart 옵션에 정의된 최소 길이보다 즉시 암호를 승인했습니다. 이 버그는 수정되었으며 --minlen 옵션은 이제 강력한 암호로도 작동합니다. (BZ#1356975)

이제 IBM z Systems의 SSH를 통한 그래픽 인터페이스에서 초기 설치가 올바르게 열립니다.

이전 버전에서는 SSH를 사용하여 IBM z Systems 시스템에 연결할 때 X 전달이 활성화된 경우에도 초기 설정 인터페이스의 텍스트 버전이 열렸습니다. 이 버그가 수정되었으며 X 전달을 사용할 때 Initial Setup 의 그래픽 버전이 올바르게 열립니다. (BZ#1378082)

geolocation 서비스를 사용하는 경우 설치에 추가 시간이 필요하지 않습니다.

인터넷 액세스가 제한되거나 없는 상태에서 Red Hat Enterprise Linux 7.3을 설치할 때 설치 프로그램이 이전에 보안 정책 섹션에서 설치 요약 화면에서 몇 분 동안 일시 중지되었습니다. 보안 정책 섹션이 준비되지 않았습니다. 이는 geolocation 서비스가 시스템의 위치를 확인할 수 없기 때문에 발생했습니다. 그 결과 서비스가 시간 초과되기 전에 설치를 진행할 수 없었습니다. 이번 업데이트를 통해 Geolocation 서비스는 3초 이내에 위치를 찾을 수 없는 경우 올바르게 시간 초과되고 네트워크 연결이 제한되거나 없는 경우에도 설치가 거의 즉시 진행될 수 있습니다. (BZ#1380224)

ifup-aliases 스크립트는 이제 새 IP 주소를 추가할 때 불필요한 ARP 업데이트를 보냅니다.

하나 이상의 IP 별칭을 한 서버에서 다른 서버로 이동할 때 업스트림 라우터에 구성된ARP(Address Resolution Protocol) 시간 제한 값에 따라 연결된 IP 주소에 연결할 수 없습니다. 이 버그는 initscripts 패키지에서 해결되었으며, ifup-aliases 는 이 상황에서 네트워크의 다른 시스템을 훨씬 더 빠르게 업데이트합니다. (BZ#1367554)

이제 netconsole 유틸리티가 올바르게 시작됩니다.

이전 버전에서는 이름 서버 주소 행이 /etc/resolv.conf 파일에 없는 경우 netconsole 을 시작하면 오류가 발생하여 netconsole 이 시작되지 않았습니다. initscripts 패키지가 업데이트되었으며 이제 netconsole 이 올바르게 시작됩니다. (BZ#1278521)

RC.debug 커널을 사용하면 **initscripts**를 더 쉽게 디버깅할 수 있습니다.

이번 개선된 기능에는 커널 명령줄의 **rc.debug** 옵션이 도입되었습니다. 부팅하기 전에 커널 명령줄에 **rc.debug** 옵션을 추가하면 부팅 및 종료 프로세스 중 **initscripts** 파일의 모든 활동 로그가 생성됩니다. 로그는 **/var/log/dmesg** 로그 파일의 일부로 표시됩니다. 결과적으로 커널 명령줄에 **rc.debug** 옵션을 추가하면 필요한 경우 **initscripts** 를 더 쉽게 디버깅할 수 있습니다. **(BZ#1394191)**

더 이상 **iSCSI** 또는 **NFS**에서 **/usr** 으로 시스템을 종료하지 않습니다.

이전 버전의 **Red Hat Enterprise Linux 7**에서는 시스템 종료가 실패하는 경우가 많으며 **/usr** 폴더가 네트워크를 통해 마운트된 경우(예: **NFS** 또는 **iSCSI**)가 중단될 수 있습니다. 이 문제는 해결되었으며 이제 시스템이 정상적으로 종료되어야 합니다. **(BZ#1369790, BZ#1446171)**

RHEL-autorelabel 이 더 이상 파일 시스템이 손상되지 않습니다.

이전 버전의 **Red Hat Enterprise Linux 7**에서는 **/.autorelabel** 파일을 만들어 **SELinux** 자동 레이블이 손상되는 경우 파일 시스템이 손상되는 경우가 있었습니다. 이로 인해 시스템을 부팅할 수 없었습니다. 이 동작을 방지하기 위해 패치가 적용되었습니다. 결과적으로 **touch /. autorelabel** 명령을 사용하여 **autorelabel** 작업을 적용하면 파일 시스템이 손상될 것으로 예상되지 않습니다. **(BZ#1385272)**

이제 **rpmbuild** 명령을 올바르게 처리하려면 **Perl**이 필요합니다.

이전 버전에서는 **rpm**의 버그로 인해 **rpm build** 명령을 사용하여 패키지를 빌드할 때 문자열 상수 대신 **my variable = <<** 블록이 코드로 처리되었습니다. 이로 인해 **rpm** 에서 의도하지 않은 종속성을 패키지에 추가하여 변수에 해당 단어의 사용 및 다른 단어가 포함된 경우도 있었습니다. 이번 업데이트를 통해 **rpm** 은 종속성을 검색할 때 이러한 블록을 올바르게 건너뛰고, 패키지에 더 이상 의도하지 않은 종속성이 포함되지 않습니다. **(BZ#1378307)**

이제 설치 프로그램에서 **Kickstart**에서 **ignoredisk** 를 사용할 때 **BIOS RAID** 장치를 올바르게 인식합니다.

이전에는 **ignoredisk --onlyuse=<bios raid name >** 명령으로 **Kickstart** 파일을 사용할 때 설치 중에 일부 **BIOS RAID** 장치가 올바르게 인식되지 않았습니다. 이로 인해 장치를 사용할 수 없어 설치가 실패하고 여유 공간이 부족하게 보고되었습니다. 이번 업데이트를 통해 **Anaconda**는 **Kickstart** 파일에 지정된 경우 **BIOS RAID** 장치를 안정적으로 인식하며 이러한 상황에서 더 이상 설치되지 않습니다. **(BZ#1327463)**

이제 **ifcfg-*** 파일의 값에 대해 작은따옴표가 작동합니다.

이전에는 **ifcfg-*** 파일에서 이중 따옴표를 사용하여 값을 지정할 수 있었습니다. 작은따옴표를 사용하는 것은 작동하지 않았습니다. 이번 업데이트에서는 작은따옴표도 다음과 같이 작동합니다.

```
ONBOOT='yes'
```

(BZ#1428574)

RHEL-import-state는 더 이상 /dev/shm/ 에 대한 액세스 권한을 변경하지 않으므로 시스템이 올바르게 부팅될 수 있습니다.

이전 버전에서는 dracut 업데이트에서 새 스크립트가 도입되어 부팅 프로세스 중 문제가 발생했습니다. dracut 유틸리티가 디렉토리를 /run/initramfs/state/ 에 배치하면 새 스크립트에서 /dev/shm/ 디렉토리에 액세스 권한을 변경했습니다. 이번 업데이트를 통해 rhel-import-state는 더 이상 /dev/shm/ 에 대한 액세스 권한을 변경하지 않으며 시스템이 올바르게 시작됩니다. (BZ#1406254)

Red Hat Enterprise Linux 6의 이전 버전과의 호환성 활성화 initscripts

Red Hat Enterprise Linux 7의 initscripts 파일은 이전 버전과의 호환성을 활성화하고 Red Hat Enterprise Linux 6에서 Red Hat Enterprise Linux 7로 업그레이드할 때 발생할 수 있는 회귀 문제를 방지하기 위해 패치되었습니다. (BZ#1392766)

initscripts 이제 /etc/rwtab 및 /etc/statetab 을 설정 파일로 지정합니다.

이전에는 initscripts 패키지를 다시 설치하여 /etc/rwtab 및 /etc/statetab 파일을 교체했습니다. 이러한 파일에 사용자 구성이 포함된 경우 다시 설치 프로세스에서 해당 파일을 덮어씁니다.

구성 파일로 /etc/rwtab 및 /etc/statetab 파일을 지정하도록 initscripts 패키지가 업데이트되었습니다. 사용자가 이러한 파일을 수정한 경우 다시 설치하면 /etc/ 폴더에 새 구성이 포함된 *.rpmnew 파일이 생성됩니다. 이번 업데이트의 결과 initscripts 패키지를 다시 설치하면 /etc/rwtab 및 /etc/statetab 파일이 그대로 유지됩니다. (BZ#1434075)

ifup 스크립트가 더 이상 NetworkManager의 속도 저하되지 않음

이전에는 NetworkManager 에 알릴 때 ifup 스크립트가 매우 느렸습니다. 특히 RHV(Red Hat Virtualization) 네트워크 시작 시간에 영향을 미쳤습니다. initscripts에 패치가 적용되었으며, 설명된 문제는 더 이상 발생하지 않습니다. (BZ#1408219)

이제 kickstart에서 firstboot --disable 명령으로 GNOME Initial Setup을 비활성화할 수 있습니다.

이번 업데이트를 통해 gnome-initial-setup 패키지가 firstboot --disable kickstart 명령을 준수하도록 수정되었습니다. 그 결과, Gnome Initial Setup은 kickstart 설치 중에 견고하게 꺼질 수 있으며 설치 kickstart에 firstboot --disable 명령이 포함된 한 설명된 상황에서 첫 번째 부팅에서 사용자 계정을 생성해야 합니다. (BZ#1226819)

NM_CONTROLLED 설정은 모든 ifcfg-* 파일에서 올바르게 작동합니다.

NM_CONTROLLED=no 매개 변수가 ifcfg-* 파일의 인터페이스에 대해 설정된 경우 경우에 따라 이 구성이 상속되었습니다. 이 동작으로 인해 NetworkManager 데몬이 이러한 인터페이스를 제어하지 못했습니다. 이제 문제가 해결되었으며 이제 모든 ifcfg-* 파일에서 NM_CONTROLLED 매개 변수를 올바르게 설정할 수 있습니다. 결과적으로 사용자는 NetworkManager 에서 제어하는 인터페이스를 선택할 수 있으며 그렇지 않습니다. (BZ#1374837)

호스트 이름이 설정되지 않은 경우 dhclient 명령이 localhost 를 잘못 사용하지 않습니다.

hostname 변수가 설정되지 않은 경우 **dhclient** 명령은 호스트 이름으로 **localhost** 를 **DHCP** 서버로 잘못 전송했습니다. 이 문제는 해결되었으며 **dhclient** 는 이러한 상황에서 더 이상 잘못된 호스트 이름을 전송하지 않습니다. **(BZ#1398686)**

initscripts 유틸리티는 이제 **LVM2**를 올바르게 처리합니다.

이전 버전에서는 **initscripts** 유틸리티의 이후 버전에서는 부팅 중에 **KnativeServing change** 명령에 새로운 **--ignoreskippedcluster** 옵션을 사용했습니다. 이 옵션은 **lvm2** 유틸리티의 이전 버전에서 누락되었습니다. 따라서 이전 버전의 **LVM(Logical Volume Manager** 장치 매퍼)을 사용하는 시스템이 올바르게 부팅되지 않을 수 있었습니다. 이번 업데이트를 통해 **initscripts RPM**은 필요한 **lvm2** 버전을 나타내며 충분한 버전이 설치된 경우 **LVM2** 부팅이 올바르게 부팅됩니다. **(BZ#1398683)**

서비스 **network stop** 명령에서는 이미 중지된 서비스를 중지하지 않습니다.

이전 버전에서는 터널 인터페이스가 있는 경우 서비스 **network stop** 명령에서 이미 중지된 서비스를 중지하여 오류 메시지를 표시했습니다. 이 버그가 수정되었으며 서비스 **network stop** 명령은 이제 실행 중인 서비스만 중지합니다. **(BZ#1398679)**

루프백 장치에서 다운이 올바르게 작동합니다.

이전 버전의 **Red Hat Enterprise Linux 7**에서는 로컬 루프백 장치에서 **ifdown** 명령을 실행하지 못했습니다. 패치가 적용되었으며 이제 **ifdown** 을 사용하여 기존 루프백 장치를 제거합니다. **(BZ#1398678)**

initscripts 의 스크립트가 정적 **IPv6** 주소 할당을 보다 강력하게 처리

이전에는 시스템 초기화 중에 라우터 알림**(RA)**이 수신된 경우 **initscripts** 패키지의 스크립트가 정적 **IPv6** 주소를 올바르게 할당하지 못하는 경우가 있었습니다. 이 버그가 수정되었으며 이제 정적으로 할당된 주소가 설명된 상황에 올바르게 적용됩니다. **(BZ#1398671)**

Software Selection 에서 애드온 옵션을 선택 취소하려면 더 이상 두 번 클릭이 필요하지 않습니다.

Red Hat Enterprise Linux 7.3을 설치할 때 사용자는 기본 환경이 변경된 후 애드온 확인란을 선택 해제하기 위해 두 번 클릭해야 했습니다. 이 버그는 그래픽 설치의 **Software Selection** 대화에서 발생했습니다. 이번 업데이트를 통해 기본 환경이 변경된 후 옵션을 선택 취소하면 시스템을 두 번 클릭할 필요가 없습니다. 한 번의 클릭으로 충분합니다. **(BZ#1404158)**

대상 시스템 호스트 이름은 **Kickstart** 설치의 설치 프로그램 부팅 옵션을 통해 구성할 수 있습니다.

Red Hat Enterprise Linux 7.3에서 **Kickstart** 설치 중에 **Anaconda** 설치 프로그램 부팅 옵션을 통해 지정된 호스트 이름은 이전에 설치된 시스템에 잘못 설정되지 않았으며 기본 **localhost.localdomain** 호스트 이름 값이 대신 사용되었습니다. 이번 업데이트를 통해 부팅 옵션으로 설정된 호스트 이름을 대상 시스템 구성에 적용하도록 **Anaconda** 가 수정되었습니다. 따라서 사용자는 이제 **Kickstart** 설치에 대한 설치 관리자 부팅 옵션을 통해 대상 시스템 호스트 이름을 구성할 수 있습니다. **(BZ#1441337)**

네트워크 설정 후 **Anaconda** 에서 더 이상 설치 소스 확인을 요청하지 않습니다.

이전 버전에서는 리포지토리에서 **Anaconda** 를 설치하는 동안 리포지토리 패키지가 이미 선택된 후 사

용자가 네트워크 설정을 변경한 경우 Installation Source(설치 소스)에 필요한 확인이 필요했습니다. 네트워크를 변경한 후에도 리포지토리에 계속 연결할 수 있는 경우에도 이 요청이 수행되어 불필요한 단계가 발생했습니다. 이번 업데이트를 통해 Anaconda 설치 프로그램은 원래 소스 리포지토리를 유지하고 Network & Hostname 구성 후에도 여전히 연결할 수 있는지 확인합니다. 따라서 사용자는 원래 리포지토리에 연결할 수 없는 경우에만 설치 소스를 재구성해야 합니다. (BZ#1358778)

이제 OEMDRV 라벨을 사용하는 디스크가 자동 설치 중에 올바르게 무시됩니다.

OEMDRV 디스크 레이블은 설치 중에 드라이버 업데이트 디스크에 사용됩니다. 버그로 인해 이 레이블이 있는 디스크는 자동 설치 중에 Anaconda에서 설치 대상으로 사용하고 있었기 때문에 설치된 시스템 스토리지의 일부로 지워지고 사용되었습니다. 이번 업데이트에서는 설치 대상으로 명시적으로 선택되지 않는 한 Anaconda에서 이 레이블이 있는 디스크를 무시하도록 하고, 문제가 더 이상 발생하지 않습니다. (BZ#1412022)

29장. 커널

RAID 4 및 RAID 10 생성 및 활성화가 완전히 지원됨

Red Hat Enterprise Linux 7.3에서는 이전 릴리스를 사용하여 생성된 기존 RAID4 또는 RAID10 논리 볼륨이 활성화되지 않았습니다. 또한 사용자는 Red Hat Enterprise Linux 7.3에서 생성된 새로운 RAID4 논리 볼륨을 생성하지 않도록 지시되었습니다. 이러한 논리 볼륨은 이후 릴리스 및 업데이트에서 활성화되지 않을 수 있기 때문입니다. 이번 업데이트를 통해 Red Hat Enterprise Linux 7.4는 RAID 4 및 RAID 10 생성 및 활성화를 완전히 지원하고 Red Hat Enterprise Linux 7.3으로 생성되었을 수 있는 잘못된 RAID 4 및 RAID 10 레이아웃을 거부합니다. (BZ#1385149)

kdump 는 이제 레거시 유형 12 NVDIMM과 함께 작동합니다.

이전 버전에서는 기존 유형 12 VDIMM(Non-Volatile Dual In-line Memory Modules) 또는 memmap=XG!YG 커널 명령줄 매개 변수를 사용하여 에뮬레이션된 레거시 유형인 NVDIMM(Non-Volatile Dual In-line Memory Modules) 또는 memmap=XG!YG 커널 명령줄 매개 변수를 사용하여 에뮬레이션된 시스템에서 이전 버전에서는 커널 크래시 덤프를 성공적으로 캡처할 수 없었습니다. NVDIMM이 있는 시스템의 경우 커널 크래시 덤프를 캡처하려고 하면 데이터 손상이 발생하는 경우가 있었습니다. 이번 업데이트를 통해 기본 소스 코드가 수정되었으며 기존 유형 12 NVDIMM이 있는 시스템에서 이제 커널 크래시 덤프를 예상대로 캡처할 수 있습니다. (BZ#1351098)

ACL을 상속하는 파일을 생성하면 더 이상 마스크가 손실되지 않습니다.

이전 버전에서는 ACL(액세스 제어 목록)을 상속한 파일을 생성하면 로컬 파일 시스템과 달리 마스크가 손실되었습니다. 이번 업데이트를 통해 NFSv4.2를 사용하는 클라이언트는 파일을 생성할 때 서버에 상위 디렉터리에서 권한을 상속하는 경우를 제외하고 항상 mTLS를 적용할 수 있습니다. 결과적으로 새 NFS 파일은 로컬에서 생성된 파일과 동일한 권한을 얻습니다. NFS 클라이언트 및 NFS 서버에 모두 이 업데이트를 적용하고 -overs=4.2 매개 변수를 사용하여 마운트해야 합니다. (BZ#1217546)

30장. 실시간 커널

USB를 제거해도 더 이상 MRGcollector 커널에 might_sleep() 경고가 발생하지 않습니다.

이전에 **MRGtekton** 커널에서 **USB** 장치를 제거하면 중단이 비활성화되어 있음이 발생했습니다. 결과적으로 시스템은 **might_sleep()** 경고를 기록했습니다. 이번 업데이트에서는 **local_irq_disable** 및 **local_irq_enable** 호출을 각각 **local_irq_disable_nort** 및 **local_irq_enable_nort** 로 교체하여 이 버그를 수정합니다. **(BZ#1443711)**

SNMP 응답이 더 이상 시간 초과되지 않음

이전에는 모든 **Simple Network Management Protocol** 버전 **1(SNMPv1)** 및 **Systemdv2c** 응답 다음에 기록된 마지막 **Keycloakv3** 최대 메시지 크기 속성에 대해 **Systemdv3** 메시지를 검사했습니다. 그 결과 **max** 메시지 크기가 작은 **Keycloakv3** 요청으로 인해 **SNMPv1** 및 **SNMPv2c** 대량 요청이 시간 초과될 수 있었습니다. 이번 업데이트를 통해 세션 최대 메시지 크기가 **SNMPv3** 요청에서만 확인되고, **SNMPv1** 및 **SNMPv2c** 응답이 더 이상 시간 초과되지 않습니다. **(BZ#1324306)**

ICMP 리디렉션으로 인해 커널이 더 이상 충돌하지 않습니다.

이전에는 소켓이 사용자 공간과**ICMP(Internet Control Message Protocol)** 프로세스를 리디렉션하여 경쟁 조건을 생성하는 데 실패했습니다. 이로 인해 커널이 예기치 않게 종료되었습니다. 소켓이 사용자 공간에 의해 잠길 때 **ICMP** 리디렉션 패킷 프로세스를 건너뛰고 이제 설명된 문제가 발생하지 않게 되었습니다. **(BZ#1387485)**

net.ipv4.ip_nonlocal_bind 커널 매개 변수가 네임 스페이스에 설정되어 있습니다.

이전 버전에서는 네트워크 네임 스페이스 내에서 유동 **IP** 주소를 사용하는 데 실패한 경우 다음 오류 메시지와 함께 실패했습니다.

```
bind: Cannot assign requested address.
```

이번 업데이트를 통해 커널은 네임 스페이스에서 **net.ipv4.ip_nonlocal_bind** 매개 변수의 설정을 **1** 로 참조하고 유동 **IP** 주소가 예상대로 할당됩니다. **(BZ#1363661)**

netfilter REJECT 규칙은 **SCTP** 패킷에서 작동합니다.

이전에는 **conntrack** 툴에서 **SCTP(Stream Control Transmission Protocol)** 패킷의 **CRC32c** 값을 확인하지 않았습니다. 그 결과 **netfilter REJECT** 규칙이 **SCTP** 패킷에서 예상대로 적용되지 않았습니다. 이 버그는 유효한 **CRC32c** 가 있는 **SCTP** 패킷에서 **CHECKSUM_UNNECESSARY** 를 설정하여 해결되었습니다. 그 결과 **netfilter REJECT** 는**ICMP(Internet Control Message Protocol)** 응답을 생성할 수 있습니다. **(BZ#1353218)**

NetworkManager 는 더 이상 이미 설정된 **DHCP_HOSTNAME**과 연결을 중복하지 않습니다.

이전에는 **NetworkManager** 서비스를 다시 시작한 후 이미 설정된 **DHCP_HOSTNAME** 속성과의 연결이 중복되었습니다. 결과적으로 **DHCP** 리스가 만료 시 항상 갱신되지는 않았습니다. 이번 업데이트를 통해 연결이 더 이상 중복되지 않으며 이 시나리오에서 **DHCP** 리스가 올바르게 갱신됩니다.

수정에는 일치 프로세스에서 이미 설정된 호스트 이름 속성을 무시하는 기능이 포함되어 있습니다. 가능한 문제를 방지하려면 잘못된 **ipv4.dhcp-hostname** 으로 사용되지 않는 연결을 모두 제거하십시오. 자세한 내용은 https://access.redhat.com/articles/2948041 을 참조하십시오. **(BZ#1393997)**

향상된 SCTP congestion_window 관리

이전 버전에서는 작은 데이터 청크로 인해 제로 창에서 복구할 때 **SCTP(Stream Control Transmission Protocol)** 값이 **receiver_window (rwnd)** 값을 잘못 설명했습니다. 그 결과 창 업데이트가 피어로 전송되지 않았으며 **rwnd** 의 인위적인 증가로 인해 패킷이 삭제될 수 있었습니다. 이번 업데이트에서는 이러한 작은 데이터 청크를 올바르게 지정하고 창을 다시 열 때 **rwnd** 압력 값을 무시합니다. 그 결과 이제 창 업데이트가 전송되고, 발표된 **rwnd** 는 수신 버퍼의 실제 상태를 더 잘 반영합니다. **(BZ#1084802)**

DCTCP alpha 의 값이 **0**으로 떨어지고 **cwnd** 는 **137**보다 큰 값으로 남아 있습니다.

이전에는 데이터 센터 **TCP (DCTCP)**의 알파 값이 비교되기 전에 변환되어 전체 자릿수가 손실되었습니다. 그 결과 실제 알파 값이 **15** 미만으로 떨어지지 않았으며, 튜닝되지 않은 흐름은 결국 **137**의 **congestion_window (cwnd)** 값으로 떨어졌습니다. 이 버그는 **alpha** 가 낮을 때 변경 작업을 취소하여 해결되었습니다. 결과적으로 **alpha drops to 0** 및 **cwnd** 는 일치하지 않는 흐름의 경우 **137**보다 많은 값으로 유지됩니다. **(BZ#1370638)**

ss 가 올바르게 **cwnd** 표시됩니다.

이전 버전에서는 **ss** 유틸리티에서 커널의 **TCP cwnd(Transmission Control Protocol congestion)** 값이 표시되어 서명되지 않은 **32**비트 정수로 캐스팅을 수행할 수 있었습니다. 결과적으로 일부 값은 오버플로되고 음수 값으로 해석될 수 있습니다. 이번 업데이트를 통해 **ss** 코드가 수정되었으며 유틸리티에 더 이상 음수 **cwnd** 값이 표시되지 않습니다. **(BZ#1375215)**

cwnd 의 값은 **DCTCP**를 사용하여 더 이상 증가하지 않습니다.

이전에는 패킷이 손실된 후 **congestion_window (cwnd)**가 예기치 않게 증가했습니다. 결과적으로 데이터 센터 **TCP(DCTCP)** 혼잡 제어 모듈이 동일한 흐름에서 반복된 문제가 발생했기 때문에 혼잡을 피할 수 없게 되었습니다. 이번 업데이트를 통해 **cwnd** 값이 손실에 저장되고 이전 값은 복구 시 복원됩니다. 결과적으로 새벽 은 안정적으로 유지됩니다. **(BZ#1386923)**

분리 된 범위 일치가 수정되었습니다.

이전에는 부정된 일치에 있는 다양한 값을 사용하는 경우 **true**로 평가되지 않았습니다. 이번 업데이트를 통해 일치하는 작업이 예상대로 작동합니다. 예:

```
# nft add rule ip ip_table filter_chain_input ip length != 100-200 drop
```

이제 **100** 바이트보다 작거나 **200** 바이트보다 큰 패킷을 올바르게 삭제합니다. **(BZ#1418967)**

nmcli connection show 명령으로 빈 값과 **NULL** 값 모두에 대한 올바른 출력을 표시할 수 있습니다.

이전에는 **nmcli connection show** 명령의 출력이 다른 속성 중에서 빈 값과 **null** 값을 일관되게 표시하지 않았습니다. 결과적으로 빈 값이 **--** 또는 값 없이 표시되었습니다. 이번 업데이트를 통해 **nmcli connection show** 명령의 출력이 일반 또는 예의 모드의 빈 값과 **null** 값에 대해 **--** 을 표시합니다.

내부 모드에서는 값이 원시 형식으로만 출력되고 빈 값과 **null** 값이 모두 출력되지 않습니다. (BZ#1391170)

Snmpd 는 **AgentX** 하위 에이전트에서 대규모 패킷을 더 이상 거부하지 않습니다.

이전 버전에서는 **Keycloak** 데몬(**snmpd**)에서 **AgentX** 하위 에이전트에서 **1472**바이트로 전송된 패킷 크기가 제한되었습니다. 이로 인해 **snmpd** 가 **AgentX** 하위 에이전트의 대규모 패킷을 거부했습니다. 패킷 크기 제한이 **65535**바이트로 증가되었습니다. 결과적으로 **snmpd** 는 더 이상 **AgentX** 하위 에이전트에서 큰 패킷을 거부하지 않습니다. (BZ#1286693)

macvlan를 올바르게 등록 해제할 수 있습니다.

이전 버전에서는 **Macvlan** 드라이버를 등록 해제하려고 하면 다른 네임스페이스의 장치로부터 또는 다른 네임스페이스의 장치까지 손상된 **sysfs** 링크가 실패했습니다. 이번 업데이트를 통해 **Macvlan** 이 수정되어 이 버그를 수정합니다. (BZ#1412898)

32장. 보안

사용자가 찾을 수 없는 경로의 chroot에 의존하는 구성이 올바르게 작동합니다.

Red Hat Enterprise Linux 7.3에서는 OpenSSH 툴의 chroot 프로세스가 SELinux 시스템 정책을 강화할 수 있도록 변경되었으며 chroot 를 실행하기 전에 루트 UID가 삭제되었습니다. 그 결과 사용자-검색 불가능한 경로의 chroot를 사용하는 기존 구성이 작동하지 않았습니다. openssh 패키지의 이번 업데이트로 변경 사항이 취소되었습니다. 또한 관리자가 selinuxuser_use_ssh_chroot 부울을 활성화하는 경우 제한된 사용자가 OpenSSH chroot 를 사용하도록 허용하여 SELinux 시스템 정책에서 문제가 해결되었습니다. 이제 설명된 구성이 Red Hat Enterprise Linux 7.2와 동일한 방식으로 작동합니다. (BZ#1418062)

firewalld 가 모든 ICMP 유형 지원

이전에는 인터넷 제어 메시지 프로토콜(ICMP) 유형 목록이 완료되지 않았습니다. 결과적으로 packet-too-big 와 같은 일부 ICMP 유형을 차단하거나 허용할 수 없었습니다. 이번 업데이트를 통해 추가 ICMP 유형에 대한 지원이 추가되어 firewalld 서비스 데몬에서 모든 ICMP 유형을 처리할 수 있습니다. (BZ#1401978)

docker.pp 가 container.pp 로 교체 selinux-policy

이번 업데이트 이전에는 container-selinux 패키지의 container.te 파일에 해당하는 컨테이너 인터페이스 및 docker.if 파일을 가리키는 Docker 인터페이스가 포함되어 있었습니다. 그 결과 container.te 파일을 컴파일할 때 컴파일러가 중복 인터페이스에 대해 경고했습니다. 이번 업데이트를 통해 selinux-policy 패키지의 docker.pp 파일이 container.pp 파일로 교체되었으며 설명된 시나리오에서는 경고가 더 이상 발생하지 않습니다. (BZ#1386916)

최근 추가된 커널 클래스 및 권한 selinux-policy

이전에는 커널에 여러 개의 새로운 클래스와 권한이 추가되었습니다. 결과적으로 시스템 정책에 정의되지 않은 이러한 클래스와 권한으로 인해 SELinux 거부 또는 경고가 발생했습니다. 이번 업데이트를 통해 최근 추가된 모든 커널 클래스와 사용 권한이 selinux-policy 패키지에 정의되었으며 거부 및 경고가 더 이상 발생하지 않습니다. (BZ#1368057)

nss 이제 PKCS#12 파일을 올바르게 처리

이전에는 pk12util 도구를 사용하여 PKCS#5 v2.0 형식을 사용하는 강력한 암호가 있는 PKCS#12 파일의 인증서를 나열할 때 출력이 없었습니다. 또한 pk12util 을 사용하여 SHA-2 Message Authentication Code(MAC)가 있는 PKCS#12 파일의 인증서를 나열하는 경우 MAC 오류가 보고되었지만 인증서가 출력되지 않았습니다. 이번 업데이트를 통해 PKCS#12 파일의 가져오기 및 내보내기가 OpenSSL 처리와 호환되도록 변경되고 PKCS#12 파일은 이제 설명된 시나리오에서 올바르게 처리됩니다. (BZ#1220573)

OpenSCAP 에서 유용한 메시지 및 경고만 생성합니다.

이전 버전에서는 기본 검사 출력 설정이 변경되었으며 디버그 메시지도 표준 출력에 출력되었습니다. 그 결과 OpenSCAP 출력은 오류와 경고로 가득 차 있었습니다. 출력은 읽기 어려웠고 SCAP

Workbench 도 이러한 메시지를 처리할 수 없었습니다. 이번 업데이트를 통해 기본 출력 설정 변경이 취소되었으며 이제 **OpenSCAP** 에서 유용한 출력을 생성합니다. (**BZ#1447341**)

AIDE 에서 **syslog** 형식으로 기록

이번 업데이트를 통해 **syslog_format** 옵션을 사용하는 **AIDE** 탐지 시스템이 **rsyslog-compatible** 형식으로 기록됩니다. 다중 줄 로그는 원격 **rsyslog** 서버에서 구문 분석하는 동안 문제를 발생시킵니다. 새로운 **syslog_format** 옵션을 사용하여 **AIDE** 는 이제 단일 줄로 기록된 모든 변경 사항을 로깅할 수 있습니다. (**BZ#1377215**)

OpenSCAP 보안 강화 프로필을 사용하여 설치를 진행

이번 업데이트 이전에는 **scap-security-guide** 패키지의 오타로 인해 **Anaconda** 설치 프로그램이 머신을 종료하고 다시 시작되었습니다. 결과적으로 **Red Hat Enterprise Linux 7.4** 설치 과정에서 **Criminal Justice Information Services (CJIS)**와 같은 보안 강화 프로파일을 선택할 수 없었습니다. 오타가 수정되었으며 **OpenSCAP security-hardening** 프로필을 사용하여 설치합니다. (**BZ#1450731**)

OpenSCAP 및 **SSG**가 **RHV-H** 시스템을 올바르게 스캔할 수 있습니다.

이전에는 **OpenSCAP** 및 **SCAP** 보안 가이드(**SSG**) 툴을 사용하여 **RHV-H(Red Hat Virtualization Host)**로 작동하는 **Red Hat Enterprise Linux** 시스템을 스캔하여 적용할 수 없는 결과를 반환했습니다. 이번 업데이트를 통해 **OpenSCAP**과 **SSG**는 **RHV-H**를 **Red Hat Enterprise Linux**로 올바르게 식별하여 **OpenSCAP** 및 **SSG**가 **RHV-H** 시스템을 제대로 스캔할 수 있도록 합니다. (**BZ#1420038**)

OpenSCAP 에서 **CVE OVAL** 피드에서 압축되지 않은 **XML** 파일도 처리

이전에는 **OpenSCAP** 도구가 피드에서 압축된 **CVE OVAL** 파일만 처리할 수 있었습니다. 결과적으로 **Red Hat**에서 제공하는 **CVE OVAL** 피드를 취약점 스캔의 기반으로 사용할 수 없습니다. 이번 업데이트를 통해 **OpenSCAP** 은 **ZIP** 및 **BZIP2** 파일뿐만 아니라 **CVE OVAL** 피드에서 압축되지 않은 **XML** 파일도 지원하며 **CVE OVAL** 기반 스캔은 추가 단계 없이 제대로 작동합니다. (**BZ#1440192**)

33장. 서버 및 서비스

이제 Linux 기능을 올바르게 유지합니다.

이전에는 백업 단계에서 원래 시스템에 설정된 Linux 기능을 보존하지 않았습니다. 이후 복구 된 시스템은 이러한 기능을 누락했습니다. 이번 업데이트를 통해 /usr/share/rear/conf/default.conf 구성 파일에서 NETFS_sssdORE_CAPABILITIES 지시문이 y 옵션으로 설정된 경우 Linux 기능이 올바르게 보존됩니다. (BZ#1343119)

SBLIM-cmpi-fsvol은 더 이상 비활성화됨으로 DM으로 마운트된 파일 시스템을 표시하지 않습니다.

이전에는 sblim-cmpi-fsvol 일반 정보 모델(CIM) 공급자가 DM(Device Mapper)으로 마운트된 파일 시스템(FS)을 올바르게 식별할 수 없었습니다. 결과적으로 CIM_UnixLocalFileSystem 클래스 인스턴스를 열거할 때 sblim-cmpi-fsvol에 이미 disabled로 마운트된 일부 FS가 표시되었습니다. 이번 업데이트에서는 DM으로 마운트된 FS에 대한 마운트 명령 출력을 구문 분석하지 않고 dmsetup 명령 출력을 구문 분석하도록 sblim-cmpi-fsvol이 수정되었습니다. 결과적으로 sblim-cmpi-fsvol에 DM로 마운트된 FS가 올바르게 표시됩니다. (BZ#1136116)

Cyrus SASL의 6443EGO는 이제 Microsoft Windows와 호환됩니다.

이번 업데이트 이전에는 Cyrus Simple Authentication and Security Layer (SASL)에서 Simple 및 hiera GSSAPI Negotiation Mechanism (SPNEGO)의 구현이 Microsoft Windows와 호환되지 않았습니다. 그 결과 cyrus-sasl 패키지를 사용하는 Red Hat Enterprise Linux 툴은 Windows 서비스 연결을 시도할 때 NPMEGO를 사용할 수 없었습니다. 이러한 도구는 Windows 클라이언트의 연결을 허용하지 않았습니다. cyrus-sasl 패키지가 수정되었으며 Red Hat Enterprise Linux Cyrus SASL 버전의 NPMEGO가 이제 Microsoft Windows 관련 항목과 호환됩니다. (BZ#1421663)

MariaDB init 스크립트가 실패할 때 더 이상 데이터가 손실되지 않습니다.

이전에는 MariaDB init 스크립트가 실패한 경우 전체 디렉토리에서 rm -rf 라고 했습니다. 이로 인해 데이터가 손실되거나 마운트 지점도 삭제될 수 있습니다. 이번 업데이트를 통해 init 스크립트에 몇 가지 추가 검사 메커니즘이 추가되었습니다. 이제 스크립트가 실패하면 중요한 파일 작업 이전에 생성된 타임 스탬프보다 최신 파일만 제거합니다. 또한 사람이 읽을 수 있는 상태 보고서 및 오류 메시지가 추가되었습니다. (BZ#1356897)

네트워크에 액세스하기 전에 ypbind 가 더 이상 시작되지 않습니다.

ypbind 서비스가 systemd 대상 network.target 뒤에 시작하도록 설정되었습니다. 그러나 network.target 은 ypbind 에 필요한 네트워킹 기능을 보장하지 않습니다. 그 결과 ypbind 서비스가 부팅 프로세스 중에 시작될 때 네트워크에 액세스할 수 없는 경우가 있었습니다. 대상 network-online.target 뒤에 ypbind 를 시작하도록 ypbind 의 서비스 파일이 변경되고 ypbind 는 이제 시작할 때 네트워크에 액세스할 수 있습니다. (BZ#1382804)

ypbind로 인해 원격 사용자의 계정 설정이 재시작 시 기본 설정으로 더 이상 되돌아가지 않습니다.

잘못된 서비스 시작 순서 때문에 ypbind 가 모든 NNSS(Name Service Switch) 조회 작업이 완료되기 전에 시작되지 않았습니다. 이로 인해 다음 조건을 모두 이행하기 위해 사용자 계정 설정 파일이 재시작 시 기본 설정으로 되돌아갑니다.

- Gnome Display Manager 자동 로그인 사용
- NIS 인증 사용
- NFS에 있는 홈 디렉터리

사용자/그룹 데이터베이스를 설정하기 전에 ypbind 서비스 파일 순서가 ypbind를 시작하도록 수정되었습니다. 사용자 계정 설정 파일이 올바르게 처리되었습니다. (BZ#1217435)

사용된 네트워크 정보 시스템 보안 기능으로 인해 yppasswd 가 더 이상 충돌하지 않습니다.

yppasswd 클라이언트는 다음과 같은 상황을 인식하지 못하기 때문에 암호를 검사할 때 잘못된 문자열을alt 사용하려고 했습니다.

- NIS 서버가 passwd.adjunct 맵을 사용하도록 구성되었습니다.
- 변수 MERGE_hiera=false 가 NIS 서버의 파일 /var/yp/Makefile에 설정되었습니다.

그 결과 다음과 같은 오류 메시지와 함께 yppasswd 에 실패했습니다. crypt()에 실패했습니다. yppasswd 클라이언트가 이러한 상황을 인식하도록 수정되었으며 이제 서버에서 실행 중인 yppasswdd 데몬에 검사를 위임합니다. (BZ#1401432)

evince에서 NotReady 파일을 다시 표시합니다.

버그로 인해 evince 문서 뷰어에서 EgressIP 파일의 내용을 표시하지 못했습니다. 패치가 적용되었으며 evince 는 이제 EgressIP 파일을 다시 표시합니다. (BZ#1411725)

db_verify 로 인해 libdb 가 더 이상 무료 뮤텍스에서 실행되지 않습니다.

이전에는 libdb 데이터베이스가 사용되지 않은 모든 뮤텍스를 올바르게 해제하지 않았습니다. libdb 데이터베이스 파일에서 db_verify 명령을 여러 번 실행할 때 libdb 는 뮤텍스 작업에 대한 리소스를 신속하게 실행했습니다. 그 결과 libdb 가 오류 메시지와 함께 종료되었습니다.

> Unable to allocate memory for mutex; resize mutex region

데이터베이스가 일관성 없는 상태로 유지됩니다. 이 버그는 수정되었으며 이제 libdb 가 뮤텍스를 올바르게 해제하고 설명된 문제가 더 이상 발생하지 않습니다. (BZ#1277887)

Ghostscript 가 일부 상황에서 더 이상 응답하지 않습니다.

특정 상황에서 유령 스크립트 애플리케이션이 이전에 무한 루프를 입력했으며 응답하지 않아 과도한 **CPU** 로드가 발생했습니다. 이번 업데이트에서는 설명된 문제가 발생하지 않도록 기본 코드가 수정되었습니다. **(BZ#1424752)**

postscript를 **PDF**로 변환하지 않으면 더 이상 **ps2databind**가 예기치 않게 종료되지 않습니다.

이전 버전에서는 **postscript** 파일을 **PDF**로 변환하면 **ps2databind** 유틸리티가 세그먼트 오류가 발생하여 예기치 않게 종료되었습니다. 이 버그는 수정되었으며 **postscript**를 **PDF**로 변환해도 더 이상 **ps2databind**가 충돌하지 않습니다. **(BZ#1390847)**

이제 **sapconf** 가 더 높은 **kernel.shmall** 및 **kernel.shmmax** 값으로 올바르게 작동합니다.

이전에는 **sapconf** 유틸리티에 기본적으로 **kernel.shmall** 및 **kernel.shmmax** 값이 증가했습니다. 결과적으로 **sapconf** 가 다음 오류 메시지와 함께 실패했습니다.

```
integer expression expected
```

이번 업데이트에서는 **kernel.shmall** 및 **kernel.shmmax** 의 높은 값을 허용하는 새 검사가 추가되어 설명된 문제가 더 이상 발생하지 않습니다. **(BZ#1391881)**

캐시 논리 볼륨에서 **lvconvert --repair** 가 올바르게 작동합니다.

Red Hat Enterprise Linux 7.3에서 릴리스된 **lvm2-2.02.166-1.el** 패키지의 회귀 문제로 인해 캐시 논리 볼륨에서 **lvconvert --repair** 명령을 올바르게 실행할 수 없습니다. 그 결과 내부 **LV**를 변환할 수 없음 오류가 발생했습니다. 기본 소스 코드가 이 버그를 수정하도록 수정되었으며 이제 **lvconvert --repair** 가 예상대로 작동합니다. **(BZ#1380532)**

LVM2 라이브러리 **incompatibilities**에서 더 이상 업그레이드 중에 장치 모니터링이 실패하고 업그레이드 중에 손실되는 문제가 발생하지 않습니다.

Red Hat Enterprise Linux 7.3에서 릴리스된 **lvm2-2.02.166-1.el** 패키지의 버그로 인해 해당 라이브러리는 이전 버전의 **Red Hat Enterprise Linux 7**과 호환되지 않았습니다. 비호환성으로 인해 업그레이드 중에 장치 모니터링이 실패하고 손실될 수 있습니다. 그 결과 장치 오류가 원하지 않는 **(RAID)** 또는 공간 부족 상태가 제대로 처리되지 않았습니다**(thin-p)**. 이번 업데이트에서는 호환성이 수정되고 논리 볼륨 모니터링이 예상대로 작동합니다. **(BZ#1382688)**

be2iscsi 드라이버 오류로 인해 시스템이 더 이상 응답하지 않습니다.

이전에는 **be2iscsi** 드라이버 오류로 인해 운영 체제가 응답하지 않는 경우가 있었습니다. 이번 업데이트에서는 **be2iscsi** 을 수정하고, **be2iscsi** 오류로 인해 운영 체제가 더 이상 중단되지 않습니다. **(BZ#1324918)**

미러 세그먼트 유형을 사용할 때 **lvmetad** 데몬에서 더 이상 상호 작용 문제가 발생하지 않습니다.

이전 버전에서는 기존 미러 세그먼트 유형을 **3** 개 이상의 시프로 미러링된 논리 볼륨을 만드는 데 사용되면 **lvmetad** 데몬과 상호 작용 문제가 발생할 수 있었습니다. 두 번째 장치 실패 후 발생한 문제는 **mirror fault policies**가 기본이 아닌 할당 옵션으로 설정된 경우 **lvmetad** 를 사용한 경우 장치 실패 이벤트 간의 시스템을 재부팅하지 못했습니다. 이 버그가 수정되었으며 설명된 상호 작용 문제가 더 이상 발생하지 않습니다. **(BZ#1380521)**

multipathd 데몬에 블랙리스트에 대한 잘못된 오류 메시지가 표시되지 않습니다.

이전 버전에서는 **multipathd** 데몬에 블랙리스트로 지정된 장치를 찾을 수 없다는 잘못된 오류 메시지가 표시되어 사용자에게 오류가 없을 때 오류 메시지가 표시되었습니다. 이번 수정을 통해 다중 경로에서 오류 메시지를 발행하기 전에 장치를 블랙리스트에 지정했는지 확인합니다. **(BZ#1403552)**

사용 가능한 경로가 없는 경우 다중 경로 장치 다시 로드

이전 버전에서는 다중 경로 장치의 마지막 경로 장치가 제거되면 **lvmetad** 의 상태가 올바르지 않아 다중 경로 상단에 있는 **lvm** 장치가 올바르게 작동하지 않을 수 있었습니다. 이는 장치 매퍼에서 다중 경로 장치를 다시 로드할 때 사용 중인 경로 수를 확인할 방법이 없기 때문입니다. 이로 인해 검사 비활성화 및 기타 **dm** 규칙 비활성화와 관련된 다중 경로 **udev** 규칙은 장치 테이블이 다시 로드되지 않고 다중 경로 장치에서 마지막으로 사용 가능한 경로가 실패했을 때만 작동했습니다. 이번 수정을 통해 사용 가능한 경로가 없는 경우 다중 경로 장치가 다시 로드되고 다중 경로 장치의 사용 가능한 경로가 손실될 때마다 다중 경로 **udev** 규칙이 검사 및 기타 **DM** 규칙을 올바르게 비활성화합니다. 그 결과 **lvmetad** 의 상태가 올바르고 다중 경로 상단에 있는 **LVM** 장치가 올바르게 작동합니다. **(BZ#1239173)**

쓰기 실패 후 전송된 읽기 요청은 항상 다중 경로 장치에서 동일한 데이터를 반환합니다.

이전 버전에서는 쓰기 요청이 **rbd** 모듈에 중단되고 **iSCSI** 이니시에이터와 다중 경로 계층이 애플리케이션에 대한 요청을 실패로 결정했다면 실패 후 전송된 읽기 요청이 쓰기 상태가 반영되지 않았을 수 있었습니다. 이는 **Ceph rbd** 이미지를 여러 **iSCSI** 대상을 통해 내보낼 때 **rbd** 커널 모듈이 쓰기 요청을 수신할 때 **rbd** 커널 모듈이 독점 잠금을 받기 때문입니다. 이번 수정으로 **rbd** 모듈은 읽기 및 쓰기 모두에 대해 배타적 잠금을 사용합니다. 이렇게 하면 읽기를 실행하기 전에 끊긴 쓰기가 플러시되거나 실패하게 됩니다. 결과적으로 실패한 쓰기 후 전송된 읽기 요청은 항상 동일한 데이터를 반환합니다. (BZ#1380602)

다중 경로 장치의 경로 장치가 읽기 전용으로 전환되면 다중 경로 장치가 읽기 전용으로 다시 로드됩니다.

이전 버전에서는 다중 경로 장치를 다시 로드할 때 다중 경로 코드가 항상 읽기-쓰기 장치를 먼저 다시 로드하려고 시도한 다음 읽기 전용으로 다시하지 못했습니다. 경로 장치가 커널에 이미 읽기-쓰기를 열었던 경우 장치가 읽기 전용 모드로 전환되고 읽기-쓰기 다시 로드에 성공하더라도 읽기-쓰기가 계속 열립니다. 결과적으로 경로 장치가 읽기-쓰기에서 읽기 전용으로 전환될 때 다중 경로 장치는 여전히 읽기-쓰기로 전환되지만 읽기 전용 장치에 대한 모든 쓰기가 실패합니다. 이번 수정을 통해 경로 장치가 읽기 전용으로 표시되는 **uevent** 가 표시되면 다중 경로 장치를 읽기 전용으로 다시 로드합니다. 결과적으로 다중 경로 장치의 경로 장치가 읽기 전용으로 전환되면 다중 경로 장치가 읽기 전용으로 다시 로드됩니다. (BZ#1431562)

사용자가 확인되지 않는 다중 경로 장치의 오래된 데이터에 대해 더 이상 혼란스러울 수 없습니다.

이전 버전에서는 경로 장치가 분리되었을 때(다중 경로 장치의 멤버가 아님) 장치 상태 및 검사기 상태가 장치 상태가 분리되기 전에 장치 상태에 **show paths** 명령을 사용하여 표시되었습니다. 그 결과 **show paths** 명령은 더 이상 확인하지 않은 장치에 대한 날짜 정보를 표시했습니다. 이번 수정으로 **show paths** 명령은 이제 검사기 상태로 표시되지 않고 고립된 경로의 장치 상태로 알 수 없으며 사용자는 더 이상 확인되지 않는 장치에 대해 오래된 데이터를 혼동하지 않습니다. (BZ#1402092)

실패한 경로에서 우선순위를 실행하면 **multipathd** 데몬이 더 이상 정지되지 않습니다.

이전 버전에서는 **multipathd** 가 경우에 따라 실패한 경로에서 우선순위를 실행했습니다. 이로 인해 다중 경로가 동기 우선순위로 구성된 경우 실패한 경로에서 우선순위를 실행하려고 할 수 있습니다. 이번 수정에서는 경로가 실패하고 이러한 이유로 실패하지 않는 경우 **multipathd** 가 더 이상 우선순위를 실행하지 않습니다. (BZ#1362120)

이제 시스템 업그레이드가 올바르게 활성화된 후 새로운 **RAID4** 볼륨 및 기존 **RAID4** 또는 **RAID10** 논리 볼륨

Red Hat Enterprise Linux 버전 **7.3**에서 **RAID4** 논리 볼륨을 생성하거나 기존 **RAID4** 또는 **RAID10** 논리 볼륨이 있는 시스템을 버전 **7.3**으로 업그레이드한 후 시스템에서 이러한 볼륨을 활성화하지 못하는 경우가 있습니다. 이번 업데이트를 통해 시스템에서 이러한 볼륨을 성공적으로 활성화합니다. (BZ#1386184)

PV의 잘못된 상태로 인해 **LVM** 툴이 더 이상 충돌하지 않습니다.

LVM에서 볼륨 그룹(**VG**)의 물리 볼륨(**PV**) 메타데이터 간의 특정 유형의 불일치를 관찰하면 **LVM**에서 자동으로 복구할 수 있습니다. 예를 들어 이러한 불일치는 일부 **PV**가 시스템에서 일시적으로 보이지 않는 동안 **VG**가 변경되면 **PV**가 다시 나타나는 경우입니다.

이번 업데이트 이전에는 이러한 복구 작업이 수행될 때 이 문제가 아닌 경우에도 모든 **PV**가 일시적으로 반환된 것으로 간주되는 경우가 있었습니다. 결과적으로 **LVM** 툴은 세그먼트 오류로 인해 예기치 않게 종료되는 경우가 있었습니다. 이번 업데이트에서는 설명 된 문제가 더 이상 발생하지 않습니다. **(BZ#1434054)**

35장. 시스템 및 서브스크립션 관리

구성된 리포지토리가 없는 시스템에서 더 이상 언더클라우드 가 실패하지 않음

이전에는 사용자가 구성된 리포지토리가 없는 시스템에 **OpenStack Undercloud** 를 설치하려고 할 때 **yum** 패키지 관리자는 이미 설치된 **MySQL** 종속성을 설치해야 했습니다. **conseqence**로 **Undercloud** 설치 스크립트가 실패했습니다. 버그를 해결하기 위해 **yum** 이 이미 설치된 **MySQL** 종속성을 올바르게 감지하도록 수정되었습니다. 결과적으로 **Undercloud** 설치 스크립트가 구성된 리포지토리가 없는 시스템에서 더 이상 실패하지 않습니다. **(BZ#1352585)**

일치하지 않는 경우 yum -plugin-verify 에서 제공하는 yum 명령에서 종료 상태를 1 로 설정합니다.

yum -plugin-verify 플러그인에서 제공하는 **yum** 명령은 패키지에 있는 모든 불일치에 대해 종료 코드 **0** 을 반환했습니다. 버그가 수정되었으며 불일치가 발견되면 종료 상태가 **1** 로 설정됩니다. **(BZ#1406891)**

36장. 가상화

weekBIOS는 0이 아닌 LUN을 사용하여 SCSI 장치를 인식합니다.

이전 버전에서는 **LSBIOS** 논리 장치 번호(**LUN**)가 **0**으로 설정된 경우에만 **SCSI** 장치만 인식되었습니다. 그 결과, **0**이 아닌 **LUN**으로 **SCSI** 장치를 정의한 경우, **serialBIOS**를 부팅하지 못했습니다. 이번 업데이트를 통해**hashBIOS**는 **0**이 아닌 **LUN**을 사용하여 **SCSI** 장치를 인식합니다. 그 결과 **serialBIOS**가 성공적으로 부팅되었습니다. **(BZ#1020622)**

libguestfs 툴에서 /usr/ 가 root와 동일한 파티션에 있지 않은 게스트를 올바르게 처리

이전에는 **/usr/** 디렉터리가 **root** 디렉터리와 동일한 파티션에 없는 경우 **libguestfs** 라이브러리에서 게스트 운영 체제를 인식하지 못했습니다. 그 결과 **virt-v2v** 유틸리티와 같은 여러 **libguestfs** 도구가 이러한 게스트에서 사용될 때 예상대로 수행되지 않았습니다. 이번 업데이트를 통해 **/usr/** 가 **root**와 동일한 파티션에 없는 경우 **libguestfs** 가 게스트 운영 체제를 인식할 수 있습니다. 그 결과 영향을 받는 **libguestfs** 도구가 예상대로 수행됩니다. **(BZ#1401474)**

virt-v2v 는 Windows 레지스트리가 손상되거나 손상된 Windows 게스트를 변환할 수 있습니다.

이전에는 **libguestfs** 가 **Windows** 레지스트리를 조작하는 데 사용하는 **hivex** 라이브러리에서 손상된 레지스트리를 처리할 수 없었습니다. 그 결과 **virt-v2v** 유틸리티에서 손상된 **Windows** 레지스트리 또는 손상된 **Windows** 게스트를 변환할 수 없었습니다. 이번 업데이트를 통해 **libguestfs** 는 **Windows** 레지스트리를 읽을 때 **hivex** 를 덜 엄격하게 설정합니다. 결과적으로 **virt-v2v** 는 **Windows** 레지스트리가 손상되거나 손상된 대부분의 **Windows** 게스트를 변환할 수 있습니다. **(BZ#1311890, BZ#1423436)**

virt-v2v 를 사용하여 시스템이 아닌 동적 디스크로 Windows 게스트 변환이 올바르게 작동합니다.

이전 버전에서는 **virt-v2v** 유틸리티를 사용하여 시스템이 아닌 동적 디스크가 있는 **Windows** 게스트 가상 머신을 올바르게 변환하지 않았으며 변환 후 게스트를 사용할 수 없었습니다. 이번 업데이트에서는 기본 코드가 수정되어 설명된 문제가 발생하지 않습니다.

시스템 디스크(**C:** 드라이브)에서 동적 디스크를 사용하는 **Windows** 게스트의 변환은 여전히 지원되지 않습니다. **(BZ#1265588)**

Glance 클라이언트 버전에 관계없이 게스트를 Glance 이미지로 변환할 수 있습니다.

이전 버전에서는 **Glance** 명령줄 클라이언트 버전 **1.0.0** 이상이 **virt-v2v** 변환 서버에 설치된 경우 **virt-v2v** 유틸리티를 사용하여 게스트 가상 머신을 **Glance** 이미지로 변환하지 못했습니다. 이번 릴리스에서는 이미지를 내보낼 때 **virt-v2v** 가 이미지의 모든 속성을 직접 설정합니다. 그 결과 **Glance** 로의 변환은 **virt-v2v** 변환 서버에 설치된 **Glance** 클라이언트 버전에 관계없이 작동합니다. **(BZ#1374405)**

Red Hat Enterprise Linux 6.2 - 6.5 게스트 가상 머신은 virt-v2v를 사용하여 변환할 수 있습니다.

이전 버전에서는 **Red Hat Enterprise Linux** 버전 **6.2 - 6.5**의 **SELinux file_contexts** 파일의 오류로 인해 **virt-v2v utiltiy**를 사용하여 이러한 게스트를 변환할 수 없었습니다. 이번 업데이트를 통해 **virt-v2v** 는

SElinux file_contexts 파일에서 오류를 자동으로 수정합니다. 결과적으로 **Red Hat Enterprise Linux 6.2-6.5** 게스트 가상 머신은 이제 **virt-v2v** 를 사용하여 변환할 수 있습니다. (**BZ#1374232**)

/etc/fstab 의 **RuntimeClass** 항목이 이제 **libguestfs**에 의해 올바르게 구문 분석됩니다.

이전에는 **/etc/fstab** 에서 둘 이상의 쉼표로 구분된 옵션이 있는 **vGPU** 하위 볼륨 항목이 **libguestfs** 에 의해 올바르게 구문 분석되지 않았습니다. 결과적으로 이러한 구성이 있는 **Linux** 게스트 가상 머신을 검사할 수 없어 **virt-v2v** 유틸리티가 이를 변환할 수 없었습니다. 이번 업데이트를 통해 **libguestfs** 는 **/etc/fstab** 에서 여러 개의 쉼표로 구분된 옵션이 있는 **RuntimeClass** 하위 볼륨 항목을 올바르게 구문 분석합니다. 그 결과 **virt-v2v** 를 통해 이러한 항목을 검사하고 변환할 수 있습니다. (**BZ#1383517**)

libguestfs 는 이제 인증이 필요한 **libvirt** 도메인 디스크를 올바르게 열 수 있습니다.

이전에는 **libvirt** 도메인에서 디스크를 추가할 때 **libguestfs** 에서 디스크 시크릿을 읽지 않았습니다. 따라서 **libguestfs** 는 인증이 필요한 디스크를 열 수 없었습니다. 이번 업데이트를 통해 **libguestfs** 는 **libvirt** 도메인의 디스크 시크릿(있는 경우)을 읽습니다. 그 결과 **libguestfs** 는 이제 인증이 필요한 **libvirt** 도메인의 디스크를 올바르게 열 수 있습니다. (**BZ#1392798**)

Windows UEFI 게스트 부팅이 올바르게 전환되었습니다.

이전에는 **Windows 8 UEFI** 게스트를 변환할 때 **virtio** 드라이버가 올바르게 설치되지 않았습니다. 그 결과 변환된 게스트가 부팅되지 않았습니다. 이번 업데이트를 통해 **Windows UEFI** 게스트에 **virtio** 드라이버가 올바르게 설치됩니다. 그 결과 **Windows UEFI** 게스트가 제대로 부팅되었습니다. (**BZ#1431579**)

이제 **virt-v2v** 유틸리티에서 프록시 환경 변수를 일관되게 무시합니다.

이번 업데이트 이전에는 **virt-v2v** 유틸리티를 사용하여 **VMware** 게스트 가상 머신을 변환할 때 **virt-v2v** 는 **VMware**에 대한 일부 연결에 프록시 환경 변수를 사용했지만 다른 사용자에게는 사용할 수 없습니다. 이 경우 변환이 실패하는 경우가 있습니다. 이제 **virt-v2v** 는 변환 중에 모든 프록시 환경 설정을 무시하므로 설명된 문제를 방지합니다. (**BZ#1354507**)

virt-v2v 는 필요한 경우에만 **rhev-apt.exe** 및 **rhsrvany.exe** 를 복사합니다.

이전에는 **virt-v2v** 가 **Windows** 게스트를 변환할 때 항상 **rhev-apt.exe** 및 **rhsrvany.exe** 파일을 복사했습니다. 그 결과 **Windows** 게스트가 필요하지 않은 경우에도 변환된 **Windows** 게스트에 표시되었습니다. 이번 업데이트를 통해 **virt-v2v** 는 **Windows** 게스트에 필요한 경우에만 해당 파일을 복사합니다. (**BZ#1161019**)

결합된 중간에 **VLAN**이 있는 게스트는 장애 조치 후 더 이상 트래픽 전달을 중지하지 않습니다.

이전 버전에서는 **VLAN**이 있는 게스트 가상 머신에서 **ixgbe** 가상 기능(**VF**)을 사용한 본딩 인터페이스를 통해 구성된 게스트 가상 머신에서 페일오버가 발생했을 때 결합된 네트워크 인터페이스가 트래픽을 전달하지 않았습니다. 하이퍼바이저 콘솔은 요청된 **MACVLAN** 필터로 이 오류를 기록했지만 관리적으로 거부된 메시지입니다. 이번 업데이트를 통해 장애 조치가 올바르게 처리되므로 설명된 문제가 발생하지 않습니다. (**BZ#1379787**)

< ovf:Name > 속성이 없는 **virt-v2v** 가져오기 **OVA**

이전 버전에서는 **virt-v2v** 유틸리티에서 **< ovf:Name >** 속성 없이 **OCI(Open Virtual Installings)** 가져오기를 거부했습니다. 그 결과 **virt-v2v** 유틸리티에서 **AWS(Amazon Web Services)**에서 내보낸 **OVA**를 가져오지 않았습니다. 이번 릴리스에서는 **< ovf:Name >** 특성이 없는 경우 **virt-v2v** 는 디스크 이미지 파일의 기본 이름을 가상 머신 이름으로 사용합니다. 그 결과 **virt-v2v** 유틸리티에서 **AWS**에서 내보낸 **OVA**를 가져옵니다. **(BZ#1402301)**

III 부. 기술 프리뷰

이 부분에서는 **Red Hat Enterprise Linux 7.4**에서 사용 가능한 모든 기술 프리뷰 목록을 제공합니다.

기술 프리뷰 기능에 대한 **Red Hat** 지원 범위 정보는 의 내용을 참조하십시오 **https://access.redhat.com/support/offerings/techpreview/.**

37장. 일반 업데이트

systemd-importd VM 및 컨테이너 이미지 가져오기 및 내보내기 서비스

최신 **systemd** 버전에는 이전 빌드에서 활성화되지 않은 **systemd-importd** 데몬이 포함되어 이로 인해 **machinectl pull-*** 명령이 실패했습니다. **systemd-importd** 데몬은 기술 프리뷰로 제공되며 안정적인 것으로 간주해서는 안 됩니다. (BZ#1284974)

38장. 인증 및 상호 운용성

AD 및 LDAP sudo 공급자 사용

AD(Active Directory) 공급자는 AD 서버에 연결하는 데 사용되는 백엔드입니다. Red Hat Enterprise Linux 7.2부터는 LDAP 공급자와 함께 AD sudo 공급자를 사용하는 기술 프리뷰로 사용할 수 있습니다. AD sudo 공급자를 활성화하려면 sssd.conf 파일의 [domain] 섹션에 sudo_provider=ad 설정을 추가합니다. (BZ#1068725)

IdM에서 기술 프리뷰로 DNSSEC 사용 가능

통합된 DNS가 있는 IdM(Identity Management) 서버는 이제 DNS 프로토콜의 보안을 강화하기 위해 DNS에 대한 확장 세트인 DNSSEC(DNS Security Extensions)를 지원합니다. IdM 서버에서 호스팅되는 DNS 영역은 DNSSEC를 사용하여 자동으로 서명할 수 있습니다. 암호화 키가 자동으로 생성되고 순환됩니다.

DNSSEC로 DNS 영역을 보호하기로 결정한 사용자는 다음 문서를 읽고 따르는 것이 좋습니다.

- DNSSEC Operational Practices, Version 2: http://tools.ietf.org/html/rfc6781#section-2
- DNS(Secure Domain Name System) 배포 가이드: http://dx.doi.org/10.6028/NIST.SP.800-81-2
- DNSSEC Key Rollover Timing Considerations: http://tools.ietf.org/html/rfc7583

통합된 DNS가 있는 IdM 서버는 DNSSEC를 사용하여 다른 DNS 서버에서 얻은 DNS 응답을 검증합니다. 이는 Red Hat Enterprise Linux 네트워킹 가이드에 설명된 권장 이름 지정 방법에 따라 구성되지 않은 DNS 영역의 가용성에 영향을 미칠 수 있습니다. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices. (BZ#1115294)

ID 관리 JSON-RPC API 기술 프리뷰로 사용 가능

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

Red Hat Enterprise Linux 7.3에서는 여러 버전의 API 명령을 사용하도록 IdM API가 개선되었습니다. 이전에는 기능 개선이 호환되지 않는 방식으로 명령 동작을 변경할 수 있었습니다. 이제 IdM API가 변경되더라도 기존 툴과 스크립트를 계속 사용할 수 있습니다. 이를 통해 다음을 수행할 수 있습니다.

- 관리자는 관리 클라이언트보다 서버에서 이전 또는 이후 버전의 IdM을 사용할 수 있습니다.
- 개발자는 IdM 버전이 서버에서 변경되더라도 특정 버전의 IdM 호출을 사용합니다.

모든 경우에 서버와의 통신은 예를 들어 한 쪽이 기능에 대한 새로운 옵션을 도입하는 최신 버전인지 여부에 관계없이 가능합니다.

API 사용에 대한 자세한 내용은 https://access.redhat.com/articles/2728021 (BZ#1298286)을 참조하십시오.

이제 Custodia 보안 서비스 공급자를 사용할 수 있습니다.

이제 시크릿 서비스 공급자인 Custodia를 사용할 수 있습니다. custodia는 키 또는 암호와 같은 시크릿의 프록시 역할을 합니다.

자세한 내용은 http://custodia.readthedocs.io 의 업스트림 문서를 참조하십시오. (BZ#1403214)

컨테이너화된 ID 관리 서버를 기술 프리뷰로 사용 가능

rhel7/ipa-server 컨테이너 이미지는 기술 프리뷰 기능으로 사용할 수 있습니다. rhel7/sssd 컨테이너 이미지는 이제 완전히 지원됩니다.

자세한 내용은 https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/using_containerized_identity_management_services 을 참조하십시오. (BZ#1405325, BZ#1405326)

39장. 클러스터링

pcs 툴에서 Pacemaker에서 번들 리소스를 관리

Red Hat Enterprise Linux 7.4부터 기술 프리뷰로 **pcs** 툴은 번들 리소스를 지원합니다. 이제 **pcs** 리소스 번들 생성 및 **pcs** 리소스 번들 업데이트 명령을 사용하여 번들을 생성하고 수정할 수 있습니다. **pcs resource create** 명령을 사용하여 기존 번들에 리소스를 추가할 수 있습니다. 번들 리소스에 대해 설정할 수 있는 매개변수에 대한 자세한 내용은 **pcs resource bundle --help** 명령을 실행합니다. (BZ#1433016)

40장. 컴파일러 및 도구

Shenandoah 가비지 수집기

새로운 일시 중지 시간 Shenandoah 가비지 수집기는 이제 Intel 64, AMD64 및 64비트 ARM 아키텍처에서 OpenJDK용 기술 프리뷰로 사용할 수 있습니다. Shenandoah는 사용자가 긴 일시 중지 시간 없이 큰 힙으로 실행할 수 있는 동시 비우기를 수행합니다. 자세한 내용은 https://wiki.openjdk.java.net/display/shenandoah/Main 을 참조하십시오. (BZ#1400306)

41장. 파일 시스템

ext4 및 **XFS**에서 기술 프리뷰로 파일 시스템 **DAX**를 사용할 수 있습니다.

Red Hat Enterprise Linux 7.3부터 **Direct Access (DAX)**는 애플리케이션이 영구 메모리를 주소 공간에 직접 매핑하는 수단을 기술 프리뷰로 제공합니다.

DAX를 사용하려면 시스템에서 일반적으로 하나 이상의 **Volatile Dual In-line Memory Modules (NVDIMM)** 형식으로 사용할 수 있고 **DAX**를 지원하는 파일 시스템을 **NVDIMM**에서 생성해야 합니다. 또한 **dax** 마운트 옵션을 사용하여 파일 시스템을 마운트해야 합니다. 그런 다음 **dax** 마운트 파일 시스템에서 파일의 **mmap** 을 사용하면 스토리지를 애플리케이션의 주소 공간에 직접 매핑합니다. **(BZ#1274459)**

PNFS 및 블록 레이아웃 지원

기술 프리뷰로 업스트림 코드는 **pNFS** 블록 레이아웃 기능을 제공하기 위해 **Red Hat Enterprise Linux** 클라이언트에 백포트되었습니다.

또한 **Red Hat Enterprise Linux 7.4**에는 **pNFS SCSI** 레이아웃의 기술 프리뷰가 포함되어 있습니다. 이 기능은 **pNFS** 블록 레이아웃과 유사하지만 **SCSI** 장치로만 제한되므로 쉽게 사용할 수 있습니다. 따라서 **Red Hat**은 **pNFS** 블록 레이아웃 대신 **pNFS SCSI** 레이아웃을 사용하는 것이 좋습니다. **(BZ#1111712)**

OverlayFS

OverlayFS는 일종의 통합 파일 시스템입니다. 이를 통해 사용자는 다른 파일 시스템 위에 하나의 파일 시스템을 오버레이할 수 있습니다. 변경 사항은 상위 파일 시스템에 기록되지만 하위 파일 시스템은 수정되지 않은 상태로 유지됩니다. 이를 통해 여러 사용자가 컨테이너 또는 **DVD-ROM**과 같은 파일 시스템 이미지를 공유할 수 있습니다. 여기서 기본 이미지는 읽기 전용 미디어에 있습니다. 자세한 내용은 커널 파일 **Documentation/filesystems/overlayfs.txt**를 참조하십시오.

OverlayFS는 대부분의 상황에 따라 **Red Hat Enterprise Linux 7.4**에서 기술 프리뷰로 남아 있습니다. 따라서 이 기술이 활성화되면 커널이 경고를 로깅합니다.

다음과 같은 제한 사항에 따라 **Docker**와 함께 사용할 때 **OverlayFS**에 대한 완전 지원을 사용할 수 있습니다.

- **OverlayFS**는 **Docker** 그래프 드라이버로만 사용할 수 있습니다. 이 사용은 영구저장장치가 아닌 컨테이너 **COW** 콘텐츠에서만 지원할 수 있습니다. 모든 영구 스토리지는 지원되지 않는 **OverlayFS** 볼륨에 배치해야 합니다. 기본 **Docker** 구성만 사용할 수 있습니다. 즉, 한 단계의 오버레이, **1**개의 하위 디렉터리 및 상위 수준은 동일한 파일 시스템에 있습니다.

- XFS만 현재 하위 계층 파일 시스템으로 사용할 수 있습니다.

- Red Hat Enterprise Linux 7.3 이하에서는 SELinux를 실제 머신에서 활성화 및 강제 모드로 설정해야 하지만 컨테이너 분리를 수행할 때 컨테이너에서 비활성화해야 합니다. 즉 /etc/sysconfig/docker 파일에 --selinux-enabled 가 포함되어야 합니다. Red Hat Enterprise Linux 7.4부터 OverlayFS는 SELinux 보안 레이블을 지원하며 /etc/sysconfig/docker 에 --selinux-enabled 를 지정하여 컨테이너에 대한 SELinux 지원을 활성화할 수 있습니다.

- OverlayFS 커널 ABI 및 사용자 공간 동작은 안정적이지 않으며 향후 업데이트의 변경 사항을 볼 수 있습니다.

- 컨테이너 내에서 yum 및 rpm 유틸리티가 제대로 작동하려면 yum-plugin-ovl 패키지를 사용해야 합니다.

OverlayFS는 제한된 POSIX 표준 집합을 제공합니다. OverlayFS를 사용하여 배포하기 전에 애플리케이션을 철저하게 테스트합니다.

오버레이로 사용하기 위해 -n ftype=1 옵션을 활성화한 상태에서 XFS 파일 시스템을 생성해야 합니다. rootfs 및 시스템 설치 중에 생성된 파일 시스템을 사용하여 Anaconda kickstart에 --mkfsoptions=-n ftype=1 매개변수를 설정합니다. 설치 후 새 파일 시스템을 생성할 때 # mkfs -t xfs -n ftype=1 /PATH/TO/DEVICE 명령을 실행합니다. 기존 파일 시스템을 오버레이로 사용할 수 있는지 확인하려면 # xfs_info /PATH/TO/DEVICE | grep ftype 명령을 실행하여 ftype=1 옵션이 활성화되어 있는지 확인합니다.

Red Hat Enterprise Linux 7.3 릴리스에서 OverlayFS와 관련된 여러 가지 알려진 문제가 있습니다. 자세한 내용은 Documentation/filesystems/overlayfs.txt 파일의 비표준 동작을 참조하십시오. (BZ#1206277)

PNFS SCSI 레이아웃 클라이언트 및 서버 지원이 제공됩니다.

병렬 NFS(pNFS) SCSI 레이아웃에 대한 클라이언트 및 서버 지원은 Red Hat Enterprise Linux 7.3부터 기술 프리뷰로 제공됩니다. 블록 레이아웃을 기반으로 하는 pNFS 레이아웃은 SCSI 장치에 걸쳐 정의되며 SCSI 영구 예약을 지원해야 하는 논리 단위로 순차적 일련의 고정 크기 블록이 포함되어 있습니다. 논리 장치(LU) 장치는 SCSI 장치 식별으로 식별되며, 예약 할당을 통해 펜싱을 처리합니다. (BZ#1305092)

v GPU 파일 시스템

B - Tree(B-Tree) 파일 시스템은 Red Hat Enterprise Linux 7에서 기술 프리뷰로 사용할 수 있습니다.

Red Hat Enterprise Linux 7.4에서는 이 기능에 대한 마지막 예정된 업데이트가 도입되었습니다. v GPU는 더 이상 사용되지 않습니다. 즉 Red Hat은 완전히 지원되는 기능으로 전환되지 않으며 향후 Red Hat Enterprise Linux 주요 릴리스에서 제거될 예정입니다. (BZ#1477977)

42장. 하드웨어 활성화

신뢰할 수 있는 컴퓨팅 그룹 TPM 2.0 시스템 API 라이브러리 및 관리 유틸리티 사용 가능

신뢰할 수 있는 컴퓨팅 그룹의 TPM(Trusted Platform Module) 2.0 하드웨어를 기술 프리뷰로 지원하기 위해 두 개의 새로운 패키지가 Red Hat Enterprise Linux에 추가되었습니다.

- tpm2-tss 패키지는 TPM 2.0 System API 라이브러리의 Intel 구현을 추가합니다. 이 라이브러리를 사용하면 프로그램이 TPM 2.0 장치와 상호 작용할 수 있습니다.

- tpm2-tools 패키지는 사용자 공간의 TPM 2.0 장치의 관리 및 활용을 위한 유틸리티 세트를 추가합니다. (BZ#1275027, BZ#1275029)

새 패키지: tss2

tss2 패키지는 신뢰할 수 있는 컴퓨팅 그룹 소프트웨어 스택(TSS) 2.0의 IBM 구현을 기술 프리뷰로 추가합니다. 이 패키지를 사용하면 TPM 2.0 장치와 상호 작용할 수 있습니다. (BZ#1384452)

LSI Syncro CS HA-DAS 어댑터

Red Hat Enterprise Linux 7.1에는 LSI Syncro CS 고가용성 직접 연결 스토리지(HA-DAS) 어댑터를 사용할 수 있도록 megaraid_sas 드라이버에 코드가 포함되었습니다. 이전에 활성화된 어댑터에서 megaraid_sas 드라이버가 완전히 지원되지만 Syncro CS용 이 드라이버 사용은 기술 프리뷰로 제공됩니다. 이 어댑터에 대한 지원은 LSI, 시스템 통합자 또는 시스템 공급 업체에 의해 직접 제공됩니다. Red Hat Enterprise Linux 7.2 이상에 Syncro CS를 배포하는 사용자는 Red Hat 및 LSI에 피드백을 제공하는 것이 좋습니다. LSI Syncro CS 솔루션에 대한 자세한 내용은 http://www.lsi.com/products/shared-das/pages/default.aspx 을 참조하십시오. (BZ#1062759)

43장. 설치 및 부팅

멀티 스레드 xz 압축 rpm-build

현재 코어를 하나만 사용하므로 고도의 병렬 빌드에 시간이 오래 걸릴 수 있습니다. 특히 코어가 많은 하드웨어에 구축된 대규모 프로젝트를 지속적으로 통합할 때 문제가 됩니다.

기술 프리뷰로 제공되는 이 기능은 %_source_ paidload 또는 %_binary_ paidload 매크로를 wLTX.xzdio 패턴으로 설정할 때 소스 및 바이너리 패키지에 대해 다중 스레드 xz 압축을 활성화합니다. L 은 기본적으로 6인 압축 수준을 나타내며 X 는 사용할 스레드 수입니다(예: w6T12.xzdio). 이 작업은 /usr/lib/rpm/macros 파일을 편집하거나 사양 파일 내에서 또는 명령줄에 매크로를 선언하여 수행할 수 있습니다. (BZ#1278924)

44장. 커널

이기종 메모리 관리 (기술 프리뷰로 포함)

Red Hat Enterprise Linux 7.3은 이기종 메모리 관리(**HMM**) 기능을 기술 프리뷰로 도입했습니다. 이 기능은 프로세스 주소 공간을 자체 메모리 관리 장치(**MMU**)에 미러링하려는 장치의 도우미 계층으로 커널에 추가되었습니다. 따라서 **CPU**가 아닌 프로세서는 통합된 시스템 주소 공간을 사용하여 시스템 메모리를 읽을 수 있습니다. 이 기능을 활성화하려면 커널 명령줄에 **experimental_hmm=enable** 을 추가합니다. **(BZ#1230959)**

criu 버전 2.12로 업데이트

Red Hat Enterprise Linux 7.2에서는 **criu** 툴을 기술 프리뷰로 도입했습니다. 이 툴은 실행 중인 애플리케이션을 정지하고 파일 컬렉션으로 저장하는 데 사용할 수 있는 **Checkpoint/Restore in User-space(CRIU)** 를 구현합니다. 나중에이 응용 프로그램은 정지 상태에서 복원 할 수 있습니다.

criu 툴은 구조화된 데이터에 대한 언어 중립적인 플랫폼 중립적인 확장 가능 메커니즘인 프로토콜 버퍼에 따라 달라집니다. 이 종속성을 제공하는 **protobuf** 및 **protobuf-c** 패키지는 **Red Hat Enterprise Linux 7.2**에 기술 프리뷰로 도입되었습니다.

Red Hat Enterprise Linux 7.4에서 **criu** 패키지는 업스트림 버전 **2.12**로 업그레이드되었으며 이전 버전에 비해 여러 버그 수정 및 개선 사항을 제공합니다. **(BZ#1400230)**

kexec 를 기술 프리뷰로

kexec 시스템 호출은 기술 프리뷰로 제공되었습니다. 이 시스템 호출을 사용하면 현재 실행 중인 커널에서 다른 커널로 로드 및 부팅할 수 있으므로 커널 내에서 부트 로더의 기능을 수행할 수 있습니다. 표준 시스템 부팅 중에 일반적으로 수행되는 하드웨어 초기화는 **kexec** 부팅 중에 수행되지 않으므로 재부팅에 필요한 시간이 크게 줄어듭니다. **(BZ#1460849)**

kexec 속도가 기술 프리뷰로 재부팅

기술 프리뷰로 이번 업데이트에서는 **kexec** 빠른 재부팅 기능이 추가되어 재부팅이 훨씬 빨라집니다. 이 기능을 사용하려면 **kexec** 커널을 수동으로 로드한 다음 운영 체제를 재부팅해야 합니다. 기본 재부팅 작업으로 **kexec** 를 빠르게 재부팅 하도록 할 수 없습니다.

특히 **Anaconda** 에 **kexec fast reboot** 를 사용합니다. **kexec fast reboot default**를 설정하도록 여전히 활성화되어 있지 않습니다. 그러나 **Anaconda** 와 함께 사용하면 사용자가 **anaconda** 옵션으로 커널을 부팅하면 설치가 완료된 후 자동으로 **kexec** 빠른 재부팅 을 사용할 수 있습니다. **kexec** 재부팅을 예약하려면 커널 명령줄에서 **inst.kexec** 명령을 사용하거나 **Kickstart** 파일에 **reboot --kexec** 행을 포함합니다. **(BZ#1464377)**

네임 스페이스에 대한 권한이 없는 액세스 권한을 기술 프리뷰로 활성화할 수 있습니다.

필요한 경우 **namespace.unpriv_enable** 커널 명령줄 옵션을 기술 프리뷰로 설정할 수 있습니다.

기본 설정은 **OFF**입니다.

1 로 설정하면 **CLONE_NEWNS** 플래그를 사용하여 **clone()** 함수에 대한 호출을 권한이 없는 사용자로 실행해도 더 이상 오류를 반환하지 않으며 작업을 허용합니다.

그러나 네임 스페이스에 대한 권한이 없는 액세스를 활성화하려면 마운트 네임 스페이스를 생성하기 위해 일부 사용자 네임 스페이스에 **CAP_SYS_ADMIN** 플래그를 설정해야 합니다. **(BZ#1350553)**

KASLR as a Technology Preview

이제 **KASLR(**커널 주소 공간 레이아웃 임의화**)**을 기술 프리뷰로 사용할 수 있습니다. **KASLR**은 커널 텍스트 **KASLR** 및 **mm KASLR**을 포함하는 커널 기능입니다. 이 두 부분은 **Linux** 커널의 보안을 강화하기 위해 함께 작동합니다.

커널 텍스트 자체의 실제 주소와 가상 주소는 다른 위치로 임의로 지정됩니다. 커널의 실제 주소는 **64TB** 미만인 반면 커널의 가상 주소는 **[0xffffffffff80000000, 0xffffffc000000], 1GB** 공간 간에 제한됩니다.

3 mm 섹션의 시작 주소**(**직접 매핑**, vmalloc, vmemmap** 섹션**)**는 특정 영역에서 무작위로 지정됩니다. 이전에는 이러한 섹션의 주소를 시작하는 것이 고정된 값이었습니다.

따라서 **KASLR**은 이 코드가 관심의 기호가 커널 주소 공간에 위치하는 위치에 의존하는 경우 커널의 실행을 악의적인 코드로 삽입 및 리디렉션하는 것을 방지할 수 있습니다.

KASLR 코드는 이제 **Linux** 커널에서 컴파일되지만 기본적으로 비활성화되어 있습니다. 이 옵션을 사용하려면 커널 명령줄에 **kaslr** 커널 옵션을 추가하여 명시적으로 활성화합니다. **(BZ#1449762)**

유연한 파일 레이아웃을 사용하여 **NFSv4 pNFS** 클라이언트 업데이트

NFSv4 클라이언트의 유연한 파일 레이아웃은 **Red Hat Enterprise Linux 7.2**에서 기술 프리뷰로 처음 도입되었습니다. **Red Hat Enterprise Linux 7.4**는 이 기능에 대한 업데이트를 추가하지만 기술 프리뷰로 계속 제공됩니다.

NFSv4 의 유연한 파일 레이아웃을 사용하면 중단 없는 파일 이동성 및 클라이언트 측 미러링과 같은 고급 기능을 사용할 수 있으므로 데이터베이스, 빅 데이터 및 가상화와 같은 영역이 향상됩니다. **NFS** 의 유

연한 파일 레이아웃에 대한 자세한 내용은 https://datatracker.ietf.org/doc/draft-ietf-nfsv4-flex-files/ 를 참조하십시오. (BZ#1349668)

CUIR 개선 범위 탐지

MAC(Control Unit Initiated Reconfiguration)에 대한 Linux 지원은 다운 타임 없이 동시 스토리지 서비스를 사용할 수 있습니다. LPAR(Logical Partitioning) 모드에서 실행되는 Linux 인스턴스에 대한 지원 외에도 IBM z/VM 시스템의 Linux 인스턴스 지원이 기술 프리뷰로 추가되었습니다. (BZ#1274456)

qla2xxx 드라이버에서 기술 프리뷰로 SCSI-MQ

Red Hat Enterprise Linux 7.4에서 업데이트된 qla2xxx& amp; 드라이버는 이제 ql2xmqsupport=1 모듈 매개 변수를 사용하여 SCSI-MQ(multiqueue) 사용을 활성화할 수 있습니다. 기본값은 0 (비활성화) 입니다. qla2xxx 드라이버와 함께 사용하는 경우 SCSI-MQ functinality는 기술 프리뷰로 제공됩니다.

SCSI-MQ를 사용하는 비동기 IO over Fibre Channel 어댑터를 사용하는 Red Hat의 최근 성능 테스트에서는 특정 조건에서 성능 저하가 크게 저하되었습니다. 수정은 테스트 중이지만 Red Hat Enterprise Linux 7.4 General Availability에 대해서는 준비가 되지 않았습니다. (BZ#1414957)

Intel Cache allocating Technology as a Technology Preview

이번 업데이트에서는 Intel Cache Assignment Technology(CAT)를 기술 프리뷰로 추가합니다. 이 기술을 사용하면 소프트웨어에서 캐시 할당을 정의된 캐시 하위 집합으로 제한할 수 있습니다. 정의된 하위 세트는 다른 하위 집합과 중복될 수 있습니다. (BZ#1288964)

45장. 실시간 커널

새로운 스케줄러 클래스: PLAN_DEADLINE

이번 업데이트에서는 실시간 커널의 **EgressIP_DEADLINE** 스케줄러 클래스가 기술 프리뷰로 도입되었습니다. 새 스케줄러는 애플리케이션 데드라인에 따라 예측 가능한 작업 스케줄링을 활성화합니다. **opm_DEADLINE** 은 애플리케이션 타이머 조작을 줄임으로써 정기적인 워크로드에 도움이 됩니다. **(BZ#1297061)**

46장. 네트워킹

Cisco usNIC 드라이버

Cisco UCS(UCM) 서버에는 Cisco 전용 User Space Network Interface Controller(usNIC)를 제공하는 선택적 기능이 있어 사용자 공간 애플리케이션에 대해 RDMA(Remote Direct Memory Access)와 같은 작업을 수행할 수 있습니다. 기술 프리뷰로 제공되는 libusnic_verbs 드라이버를 사용하면 Verbs API를 기반으로 표준 InfiniBand RDMA 프로그래밍을 통해 usNIC 장치를 사용할 수 있습니다. (BZ#916384)

Cisco VIC 커널 드라이버

기술 프리뷰로 제공되는 Cisco VIC Infiniband 커널 드라이버를 사용하면 전용 Cisco 아키텍처와 같은 RDMA(Remote Directory Memory Access)를 사용할 수 있습니다. (BZ#916382)

신뢰할 수 있는 네트워크 연결

기술 프리뷰로 사용 가능한 신뢰할 수 있는 네트워크 Connect는 TLS, 802.1X 또는 IPsec과 같은 기존 네트워크 액세스 제어(예: TLS, 802.1X 또는 IPsec) 솔루션과 함께 사용됩니다. 즉, 엔드포인트의 시스템 정보(예: 운영 체제 구성 설정, 설치된 패키지 및 무결성 측정이라고도 함)를 수집합니다. trusted Network Connect는 엔드 포인트가 네트워크에 액세스할 수 있도록 허용하기 전에 네트워크 액세스 정책에 대해 이러한 측정을 확인하는 데 사용됩니다. (BZ#755087)

qlcnic 드라이버의 SR-IOV 기능

SR-IOV(Single-Root I/O virtualization)에 대한 지원이 기술 프리뷰로 qlcnic 드라이버에 추가되었습니다. 이러한 기능에 대한 지원은 QLogic에서 직접 제공하며 고객은 QLogic 및 Red Hat에 피드백을 제공할 것을 권장합니다. qlcnic 드라이버의 다른 기능은 완전히 지원됩니다. (BZ#1259547)

libnftnl 및 nftables 패키지

nftables 및 libnftl 패키지는 Red Hat Enterprise Linux 7.3 이후 기술 프리뷰로 사용할 수 있습니다.

nftables 패키지는 패킷 필터링 툴을 제공하며, 이전 패킷 필터링 툴에 비해 편의성, 기능 및 성능이 크게 향상됩니다. iptables,ip6tables,arptables, ebtables 유틸리티에 지정된 후속 제품입니다.

libnftnl 패키지는 libmnl 라이브러리를 통해 nftables Netlink의 API와 낮은 수준의 상호 작용을 위한 라이브러리를 제공합니다. (BZ#1332585)

off-loading support가 있는 Planers

Van ner는 사용자가 다양한 프로토콜의 잘 알려진 패킷 필드에 일치를 설정할 수 있도록 설계된 Traffic Control (DEV) category입니다. 복잡한 필터링 및 분류 작업에 대해 u32 분류자에서 규칙을 더 쉽게 구성할 수 있도록하기위한 것입니다. 또한 Plans는 하드웨어가 지원하는 경우 기본 하드웨어에 대한

분류 및 조치 규칙을 해제하는 기능을 지원합니다. 이제 Gragator가 기술 프리뷰로 제공됩니다. (BZ#1393375)

47장. ANSIBLE에서 지원하는 RED HAT ENTERPRISE LINUX 시스템 역할

새 패키지: ansible

현재 기술 프리뷰로 제공되는 Red Hat Enterprise Linux 시스템 역할은 Red Hat Enterprise Linux 하위 시스템의 구성 인터페이스로, Ansible 역할을 포함하여 시스템 구성을 보다 쉽게 구성할 수 있습니다. 이 인터페이스를 통해 여러 버전의 Red Hat Enterprise Linux에서 시스템 구성을 관리하고 새로운 주요 릴리스를 채택할 수 있습니다.

Red Hat Enterprise Linux 7.4를 사용하면 Red Hat Enterprise Linux System Roles 패키지가 Extras 채널을 통해 배포됩니다. Red Hat Enterprise Linux 시스템 역할에 대한 자세한 내용은 https://access.redhat.com/articles/3050101 를 참조하십시오.

알림:

- 현재 Ansible 은 Red Hat Enterprise Linux FIPS 검증 프로세스의 일부가 아닙니다. 향후 릴리스에서 이 문제를 해결하기를 바랍니다.
- Ansible 은 지원되지 않는 런타임 종속성으로 포함되고 있습니다. (BZ#1313263)

48장. 보안

tang-nagios 및 clevis-udisk2 하위 패키지는 기술 프리뷰로 사용 가능

Red Hat Enterprise Linux Network Bound Disk Encryption (NBDE) 프로젝트의 일부인 tang 및 clevis 패키지에는 tang-nagios 및 clevis-udisk2 하위 패키지가 포함됩니다. 이러한 하위 패키지는 기술 프리뷰로만 제공됩니다. (BZ#1467338)

IBM Power에서 기술 프리뷰로 usbguard를 사용할 수 있습니다.

침입 USB 장치에 대한 시스템 보호 기능을 제공하는 usbguard 패키지를 사용할 수 있습니다. 이번 업데이트를 통해 IBM Power 아키텍처의 USBGuard 소프트웨어 프레임워크가 기술 프리뷰로 제공됩니다. 완전 지원은 Red Hat Enterprise Linux의 이후 릴리스를 대상으로 합니다.

IBM z Systems에서는 USB가 지원되지 않으며 USBGuard 프레임워크는 해당 시스템에서 제공되지 않습니다. (BZ#1467369)

49장. 스토리지

SCSI의 멀티 큐 I/O 스케줄링

Red Hat Enterprise Linux 7에는 blk-mq라는 블록 장치에 대한 새로운 다중 대기열 I/O 스케줄링 메커니즘이 포함되어 있습니다. scsi-mq 패키지를 사용하면 Small Computer System Interface(SCSI) 하위 시스템이 이 새로운 대기열 메커니즘을 사용할 수 있습니다. 이 기능은 기술 프리뷰로 제공되며 기본적으로 활성화되어 있지 않습니다. 이를 활성화하려면 커널 명령줄에 scsi_mod.use_blk_mq=Y 를 추가합니다.

blk-mq는 특히 대기 시간이 짧은 장치의 경우 향상된 성능을 제공하기 위한 것이지만 항상 더 나은 성능을 제공하는 것은 보장되지 않습니다. 특히 scsi-mq를 활성화하면 특히 많은 CPU가 있는 시스템에서 성능이 크게 저하될 수 있습니다. (BZ#1109348)

libStorageMgmt API의 targetd 플러그인

Red Hat Enterprise Linux 7.1부터는 스토리지 어레이 독립적인 API인 libStorageMgmt를 사용한 스토리지 어레이 관리가 완전히 지원됩니다. 제공된 API는 안정적이고 일관되며 개발자가 다양한 스토리지 어레이를 프로그래밍 방식으로 관리하고 제공된 하드웨어 가속 기능을 사용할 수 있습니다. 시스템 관리자는 libStorageMgmt를 사용하여 스토리지를 수동으로 구성하고 포함된 명령줄 인터페이스로 스토리지 관리 작업을 자동화할 수도 있습니다.

대상 플러그인은 완전히 지원되지 않으며 기술 프리뷰로 유지됩니다. (BZ#1119909)

DIF/DIX(데이터 무결성 필드/데이터 무결성 확장) 지원

DIF/DIX는 SCSI 표준에 새로 추가되었습니다. Red Hat Enterprise Linux 7에서 기능 장에 지정된 HBA 및 스토리지 어레이는 완전히 지원되지만 다른 모든 HBA 및 스토리지 어레이의 경우 기술 프리뷰로 남아 있습니다.

DIF/DIX는 일반적으로 사용되는 512바이트 디스크 블록의 크기를 512에서 520바이트로 늘려 DIF(데이터 무결성 필드)를 추가합니다. DIF는 쓰기가 발생할 때 HBA(Host Bus Adapter)에 의해 계산된 데이터 블록의 체크섬 값을 저장합니다. 스토리지 장치는 수신 시 체크섬을 확인한 다음 데이터와 체크섬을 모두 저장합니다. 반대로, 읽기가 발생하면 스토리지 장치와 수신 HBA에서 체크섬을 확인할 수 있습니다. (BZ#1072107)

50장. 가상화

KVM 게스트에 대한 USB 3.0 지원

KVM 게스트의 USB 3.0 호스트 어댑터(xHCI) 에뮬레이션은 Red Hat Enterprise Linux 7.4에서 기술 프리뷰로 남아 있습니다. (BZ#1103193)

Intel 네트워크 어댑터를 선택하면 Hyper-V의 게스트로 SR-IOV 지원

Hyper-V에서 실행되는 Red Hat Enterprise Linux 게스트 가상 머신의 경우 새로운 PCI 패스스루 드라이버는 ixgbevf 드라이버에서 지원하는 Intel 네트워크 어댑터에 대해 SR-IOV(Single-root I/O virtualization) 기능을 사용할 수 있는 기능을 추가합니다. 이 기능은 다음 조건이 충족되면 활성화됩니다.

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

NIC의 가상 기능(VF)이 가상 머신에 연결되어 있습니다.

이 기능은 현재 Microsoft Windows Server 2016에서 지원됩니다. (BZ#1348508)

VFIO 드라이버의 경우 no-IOMMU 모드

기술 프리뷰로 이번 업데이트에서는 VFIO(가상 기능 I/O) 드라이버를 위한 No-IOMMU 모드를 추가합니다. No-IOMMU 모드는 I/O 메모리 관리 장치(IOMMU) 없이 DMA(Direct Memory Access) 액세스 권한을 사용자에게 제공합니다. 지원되지 않는 것 외에도 IOMMU에서 제공하는 I/O 관리 부족으로 인해 이 모드를 사용하는 것은 안전하지 않습니다. (BZ#1299662)

ibmvnic 장치 드라이버가 추가되었습니다.

ibmvnic 장치 드라이버는 IBM POWER 아키텍처용 Red Hat Enterprise Linux 7.3에서 기술 프리뷰로 소개되었습니다. vNIC(Virtual Network Interface Controller)는 엔터프라이즈 기능을 제공하고 네트워크 관리를 간소화하는 새로운 PowerVM 가상 네트워킹 기술입니다. SR-IOV NIC와 결합하면 가상 NIC 수준에서 대역폭 제어 품질(QoS) 기능을 제공합니다. vNIC는 가상화 오버헤드를 크게 줄여 네트워크 가상화에 필요한 CPU 및 메모리를 포함한 서버 리소스를 줄입니다. (BZ#947163)

virt-v2v 는 이제 vmx 구성 파일을 사용하여 VMware 게스트를 변환할 수 있습니다.

virt-v2v 유틸리티에는 이제 virt-v2v 유틸리티에 vmx 입력 모드가 포함되어 있어 사용자가 게스트 가

상 머신을 VMware vmx 구성 파일에서 변환할 수 있습니다. 이 작업을 수행하려면 해당 VMware 스토리지에 액세스할 수 있어야 합니다(예: NFS를 사용하여 스토리지를 마운트해야 합니다. (BZ#1441197)

virt-v2v 는 Debian 및 Ubuntu 게스트를 변환할 수 있습니다.

기술 프리뷰로 virt-v2v 유틸리티는 이제 Debian 및 Ubuntu 게스트 가상 머신을 변환할 수 있습니다. 이 변환을 수행할 때 현재 다음 문제가 발생합니다.

- virt-v2v 는 GRUB2 구성에서 기본 커널을 변경할 수 없으며 게스트에 구성된 커널은 게스트에서 더 최적의 커널 버전을 사용할 수 있더라도 변환 중에 변경되지 않습니다.

- Debian 또는 Ubuntu VMware 게스트를 KVM으로 변환한 후에는 게스트의 네트워크 인터페이스 이름이 변경될 수 있으므로 수동 구성이 필요할 수 있습니다. (BZ#1387213)

virtio 장치는 이제 vIOMMU를 사용할 수 있습니다.

기술 프리뷰로 이번 업데이트를 통해 virtio 장치가 가상 Input/Output Memory Management Unit(vIOMMU)을 사용할 수 있습니다. 이는 DMA(Direct Memory Access)의 보안 유지를 보장하는데, 해당 장치는 자동으로 허용되는 주소만 허용하도록 허용합니다. 그러나 Red Hat Enterprise Linux 7.4 이상을 사용하는 게스트 가상 머신만 이 기능을 사용할 수 있습니다. (BZ#1283251, BZ#1464891)

가상 머신 펌웨어 열기

OVMF(Open Virtual Machine Firmware)는 Red Hat Enterprise Linux 7에서 기술 프리뷰로 사용할 수 있습니다. OVMF는 AMD64 및 Intel 64 게스트를 위한 UEFI 보안 부팅 환경입니다. 그러나 RHEL 7에서 사용 가능한 가상화 구성 요소에서 OVMF를 부팅할 수 없습니다. RHEL 8에서는 OVMF가 완전히 지원됩니다. (BZ#653382)

IV 부. 장치 드라이버

이 부분에서는 **Red Hat Enterprise Linux 7.4**에서 신규 또는 업데이트된 모든 장치 드라이버의 포괄적인 목록을 제공합니다.

51장. 새로운 드라이버

스토리지 드라이버

- **nvme-fabrics**
- **nvme-rdma**
- **nvmet**
- **nvmet-rdma**
- **nvme-loop**
- **qedi**
- **qedf**

네트워크 드라이버

- **qedr**
- **rdma_rxe**
- **ntb_transport**
- **ntb_perf**
- **mdev**
- **vfio_mdev**

- **amd-xgbe**
- **atlantic**
- **libcxgb**
- **ena**
- **backuper**
- **amd8111e**
- **nfp**
- **mlxsw_core**
- **mlxsw_i2c**
- **mlxsw_spectrum**
- **mlxsw_pci**
- **mlxsw_switchx2**
- **mlxsw_switchib**
- **mlxsw_minimal**

그래픽 드라이버 및 기타 드라이버

- **ccp**
- **chcr**
- **uio_hv_generic**
- **usbip-core**
- **vhost_vsock**
- **tpm_tis_spi**
- **gpio-amdpt**
- **joydev**
- **sdio_uart**
- **ptp_kvm**
- **mei_wdt**
- **dell-rbtn**
- **dell-smo8800**
- **intel-hid**

- **dell-smbios**
- **skx_edac**
- **kvmgt**
- **pinctrl-intel**
- **pinctrl-sunrisepoint**
- **pinctrl-amd**
- **dax_pmem**
- **dax**
- **nfit**
- **ledtrig-usbport**

52장. 업데이트된 드라이버

스토리지 드라이버 업데이트

- **Aacraid** 드라이버가 **1.2.1[50792]-custom**으로 업데이트되었습니다.
- **lpfc** 드라이버가 **0:11.2.0.6** 버전으로 업데이트되었습니다.
- **vmw_pvscsi** 드라이버가 버전 **1.0.7.0-k**로 업데이트되었습니다.
- **megaraid_sas** 드라이버가 **07.701.17.00-rh1** 버전으로 업데이트되었습니다.
- **bfa** 드라이버가 **3.2.25.1** 버전으로 업데이트되었습니다.
- **hpsa** 드라이버가 **3.4.18-0-RH1** 버전으로 업데이트되었습니다.
- **be2iscsi** 드라이버가 버전 **11.2.1.0**으로 업데이트되었습니다.
- **qla2xxx** 드라이버가 버전 **8.07.00.38.07.4-k1**로 업데이트되었습니다.
- **MPT2sas** 드라이버가 버전 **20.103.00.00**으로 업데이트되었습니다.
- **MPT3sas** 드라이버가 버전 **15.100.00.00**으로 업데이트되었습니다.

네트워크 드라이버 업데이트

- **ntb** 드라이버가 버전 **1.0**으로 업데이트되었습니다.
- **igbvf** 드라이버가 버전 **2.4.0-k**로 업데이트되었습니다.
- **igb** 드라이버가 버전 **5.4.0-k**로 업데이트되었습니다.

- **ixgbevf** 드라이버가 **3.2.2-k-rh7.4** 버전으로 업데이트되었습니다.
- **i40e** 드라이버가 버전 **1.6.27-k**로 업데이트되었습니다.
- **fm10k** 드라이버가 **0.21.2-k** 버전으로 업데이트되었습니다.
- **i40evf** 드라이버가 버전 **1.6.27-k**로 업데이트되었습니다.
- **ixgbe** 드라이버가 버전 **4.4.0-k-rh7.4**로 업데이트되었습니다.
- **be2net** 드라이버가 버전 **11.1.0.0r**로 업데이트되었습니다.
- **qede** 드라이버가 **8.10.10.21** 버전으로 업데이트되었습니다.
- **qlge** 드라이버가 **1.00.00.35** 버전으로 업데이트되었습니다.
- **qed** 드라이버가 **8.10.10.21** 버전으로 업데이트되었습니다.
- **bna** 드라이버가 **3.2.25.1r** 버전으로 업데이트되었습니다.
- **bnxt** 드라이버가 버전 **1.7.0**으로 업데이트되었습니다.
- **enic** 드라이버가 버전 **2.3.0.31**로 업데이트되었습니다.
- **fjes** 드라이버가 버전 **1.2**로 업데이트되었습니다.
- **hpwdt** 드라이버가 버전 **1.4.02**로 업데이트되었습니다.

그래픽 드라이버 및 기타 드라이버 업데이트

- **vmwgfx** 드라이버가 버전 **2.12.0.0**으로 업데이트되었습니다.

- **hpilo** 드라이버가 버전 **1.5.0**으로 업데이트되었습니다.

V 부. 지원되지 않는 기능

이 부분에서는 **Red Hat Enterprise Linux 7.4**의 모든 마이너 릴리스에서 더 이상 사용되지 않는 기능에 대한 개요를 제공합니다.

더 이상 사용되지 않는 기능은 **Red Hat Enterprise Linux 7**이 종료될 때까지 계속 지원됩니다. 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 *하드웨어* 구성 요소는 현재 또는 향후 주요 릴리스에서 새 배포에 사용하지 않는 것이 좋습니다. 하드웨어 드라이버 업데이트는 보안 및 중요 수정 사항으로만 제한됩니다. **Red Hat**은 가능한 한 빨리 이 하드웨어를 교체할 것을 권장합니다.

패키지 는 더 이상 사용되지 않으며 추가 사용에 권장되지 않을 수 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.

53장. RED HAT ENTERPRISE LINUX 7에서 더 이상 사용되지 않는 기능

Identity Management와 관련된 더 이상 사용되지 않는 패키지

다음 패키지는 더 이상 사용되지 않으며 향후 **Red Hat Enterprise Linux** 주요 릴리스에는 포함되지 않습니다.

더 이상 사용되지 않는 패키지	제안된 교체 패키지 또는 제품
authconfig	authselect
pam_pkcs11	sssd [a]
pam_krb5	sssd [b]
openldap-servers	사용 사례에 따라 Red Hat Enterprise Linux 또는 Red Hat Directory Server에 포함된 Identity Management로 마이그레이션하십시오. [c]

[a] SSSD(System Security Services Daemon)에는 향상된 스마트 카드 기능이 포함되어 있습니다.

[b] pam_krb5 에서 sssd 로 마이그레이션하는 방법에 대한 자세한 내용은 Red Hat Customer Portal의 pam_krb5에서 SSSD 지식 베이스로 마이그레이션하는 방법을 참조하십시오.

[c] Red Hat Directory Server에는 유효한 Directory Server 서브스크립션이 필요합니다.

더 이상 사용되지 않는 보안 알고리즘 및 프로토콜

암호화 해시 및 암호화를 제공하는 알고리즘은 수명을 가지고 있으며, 그 후에는 너무 위험하거나 안전하지 않은 것으로 간주됩니다. 자세한 내용은 **Red Hat** 고객 포털에 있는 **Red Hat Enterprise Linux 7.4** 지식 베이스에서 암호화 변경 사항을 사용하여 운영 체제 보안 강화 문서를 참조하십시오.**https://bugzilla.redhat.com/show_bug.cgi?id=1335929**

취약한 암호 및 알고리즘은 OpenSSH 에서 더 이상 기본적으로 사용되지 않습니다.

이번 업데이트를 통해 **OpenSSH** 라이브러리는 기본 구성에서 몇 가지 약한 암호 및 알고리즘을 제거합니다. 그러나 대부분의 경우 역호환성을 보장합니다.

다음은 **OpenSSH** 서버 및 클라이언트에서 제거되었습니다.

- 호스트 키 알고리즘:

- **ssh-rsa-cert-v00@openssh.com**
- **ssh-dss-cert-v00@openssh.com**

- 암호화 방식:
  - **arcfour256**
  - **arcfour128**
  - **arcfour**
  - **rijndael-cbc@lysator.liu.se**

- **macs:**
  - **hmac-md5**
  - **hmac-md5-96**
  - **hmac-md5-96-etm@openssh.com**
  - **hmac-md5-etm@openssh.com**

- **hmac-ripemd160**
- **hmac-ripemd160-etm@openssh.com**
- **hmac-ripemd160@openssh.com**
- **hmac-sha1-96**
- **hmac-sha1-96-etm@openssh.com**

다음은 **OpenSSH** 클라이언트에서 제거되었습니다.

- 암호화 방식:
  - **blowfish-cbc**
  - **cast128-cbc**
  - **3des-cbc**

OpenSSH 는 **FIPS** 모드인
에서 더 이상 **SHA-1** 기반 키 교환 알고리즘을 사용하지 않습니다.

이번 업데이트에서는 **FIPS** 모드의 기본 목록에서 **SHA-1** 기반 키 교환 알고리즘을 제거합니다. 이러한 알고리즘을 활성화하려면 **~/.ssh/config** 및 **/etc/ssh/sshd_config** 파일에 대해 다음 구성 스니펫을 사용합니다.

```
KexAlgorithms=+diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
```

SSH-1 프로토콜이 OpenSSH 서버에서 제거되었습니다.

SSH-1 프로토콜 지원이 **OpenSSH** 서버에서 제거되었습니다. 자세한 내용은 **RHEL 7.4 지식 베이스에서 서버 측 SSH-1 프로토콜 제거**를 참조하십시오.

MD5, MD4 및 SHA0은 OpenSSL 의 서명 알고리즘으로 더 이상 사용할 수 없습니다(

이번 업데이트에서는 인증서의 **MD5, MD4** 및 **SHA0** 서명 확인 지원, **CRL**(인증서 취소 목록) 및 메시지 서명이 제거되었습니다.

또한 디지털 서명을 생성하는 기본 알고리즘이 **SHA-1**에서 **SHA-256**으로 변경되었습니다. **SHA-1** 서명의 확인은 기존 목적으로 계속 활성화되어 있습니다.

시스템 관리자는 **etc/pki/tls/legacy-settings** 정책 구성 파일의 **legacySigningMDs** 옵션을 수정하여 **MD5, MD4** 또는 **SHA0** 지원을 활성화할 수 있습니다. 예를 들면 다음과 같습니다.

```
echo 'LegacySigningMDs algorithm' >> /etc/pki/tls/legacy-settings
```

둘 이상의 레거시 알고리즘을 추가하려면 새 행을 제외한 쉼표 또는 공백 문자를 사용합니다. 자세한 내용은 **OpenSSL** 패키지의 **README.legacy-settings** 파일을 참조하십시오.

OPENSSL_ENABLE_MD5_VERIFY 환경 변수를 설정하여 **MD5** 검증을 활성화할 수도 있습니다.

OpenSSL 클라이언트는 더 이상 DH가 1024비트보다 짧은 서버 연결을 허용하지 않습니다

이번 업데이트에서는 **OpenSSL** 클라이언트가 **Diffie-Hellman (DH)** 매개 변수가 **1024**비트보다 짧은 서버에 연결하지 못하도록 합니다. 이렇게 하면 **OpenSSL** 을 사용하는 클라이언트가 **Logjam**과 같은 취약점에 취약하지 않습니다.

시스템 관리자는 **/etc/pki/tls/legacy-settings** 에서 **MinimumDH bits** 옵션을 수정하여 더 짧은 **DH** 매개변수 지원을 활성화할 수 있습니다. 예를 들면 다음과 같습니다.

```
echo 'MinimumDHBits 768' > /etc/pki/tls/legacy-settings
```

이 옵션은 시스템 관리자가 필요한 경우 최소값을 높이는 데도 사용할 수 있습니다.

OpenSSL
에서 **SSL 2.0** 지원이 완전히 제거되었습니다.

7년 이상 안전하지 않은 **SSL** 프로토콜 버전 **2.0**은 **2011**년 **RFC 6176**에서 더 이상 사용되지 않습니다. **Red Hat Enterprise Linux**에서는 기본적으로 **SSL 2.0** 지원이 비활성화되어 있습니다. 이번 업데이트를 통해 **SSL 2.0** 지원이 완전히 제거되었습니다. 이 프로토콜 버전을 사용하는 **OpenSSL** 라이브러리 **API** 호출에서 오류 메시지를 반환합니다.

OpenSSL 의 **EXPORT** 암호화 제품군은 더 이상 사용되지 않습니다

이번 변경으로 인해 **OpenSSL** 툴킷의 **EXPORT** 암호화 제품군 지원이 제거됩니다. 이러한 약한 암호화 제품군을 비활성화하면 **OpenSSL** 을 사용하는 클라이언트가 **FREAK**와 같은 취약점에 취약하지 않습니다. **EXPORT** 암호화 제품군은 더 이상 **TLS** 프로토콜 구성에서 필요하지 않습니다.

gnutls 클라이언트가 더 이상 **DH**가 **1024**비트보다 짧은 서버에 연결할 수 없습니다

이러한 변경으로 인해**GnuTLS(GnuTLS)** 클라이언트가 **Diffie-Hellman(DH)** 매개 변수가 **1024**비트보다 짧은 서버에 연결하지 못하도록 합니다. 이렇게 하면 **GnuTLS** 를 사용하는 클라이언트가 **Logjam**과 같은 취약점에 취약하지 않습니다.

사용자 또는 구성에서 직접 우선순위 문자열을 허용하는 애플리케이션에서는 우선 순위 문자열 **%PROFILE_VERY_WEAK** 를 사용된 우선순위 문자열에 추가하여 이 변경 사항을 되돌릴 수 있습니다.

TLS 를 사용하는 **NSS** 클라이언트는 **DH**가 **1024**비트
보다 짧은 서버에 더 이상 연결할 수 없습니다.

이러한 변경으로 인해 **NVS(Network Security Services)** 클라이언트가 **Diffie-Hellman(DH)** 매개 변수가 **1024**비트보다 짧은 서버에 연결하지 못하도록 합니다. 이렇게 하면 **NSS** 를 사용하는 클라이언트가 **Logjam**과 같은 취약점에 취약하지 않습니다.

시스템 관리자는 **/etc/pki/nss-legacy/nss-rhel7.config** 정책 구성 파일을 다음과 같이 수정하여 더 짧은 **DH** 매개 변수 지원을 활성화할 수 있습니다.

```
library=
name=Policy
NSS=flags=policyOnly,moduleDB
config="allow=DH-MIN=767:DSA-MIN=767:RSA-MIN=767"
```

파일 끝에 빈 줄이 필요합니다.

NSS 의 EXPORT 암호화 제품군은 더 이상 사용되지 않습니다

이 변경으로 인해 **NNS(Network Security Services)** 라이브러리의 **EXPORT** 암호화 제품군 지원이 제거됩니다. 이러한 약한 암호화 제품군을 비활성화하면 **FREAK**와 같은 취약성으로부터 보호됩니다. 모든 **TLS** 프로토콜 구성에서 **EXPORT** 암호화 제품군이 필요하지 않습니다.

ca-certificates 패키지에서 제거된 기존 CA 인증서

이전 버전에서는 이전 버전의 **GnuTLS,OpenSSL, glib-networking** 라이브러리가 **PKI(Public Key Infrastructure)**와 호환되는 상태로 유지되도록 **ca-certificates** 패키지에는 기본적으로 **1024**비트 **RSA** 키가 있는 레거시 **CA** 인증서 세트가 포함되었습니다.

Red Hat Enterprise Linux 7.4에서 업데이트된 **OpenSSL,GnuTLS, glib-networking** 을 사용할 수 있으므로 루트 **CA** 인증서 교체를 올바르게 식별할 수 있습니다. 이러한 레거시 **CA** 인증서를 신뢰하는 것은 더 이상 공용 웹 **PKI** 호환성을 위해 필요하지 않습니다.

이전에 레거시 **CA** 인증서를 비활성화하는 데 사용할 수 있는 레거시 구성 메커니즘은 더 이상 지원되지 않습니다. 레거시 **CA** 인증서 목록은 비어 있습니다.

ca-legacy 도구를 계속 사용할 수 있으며 향후 재사용 가능성을 위해 현재 구성 설정도 유지합니다.

coolkey 다음으로 교체됨 opensc

OpenSC 라이브러리는 **PKCS#11 API**를 구현하고 **coolkey** 패키지를 대체합니다. **Red Hat Enterprise Linux 7**에서 **CoolKey Applet** 기능은 **opensc** 패키지에서도 제공됩니다.

coolkey 패키지는 **Red Hat Enterprise Linux 7**의 라이프 사이클 기간 동안 계속 지원되지만 **opensc** 패키지를 통해 새로운 하드웨어 사용은 제공됩니다.

rsyslog imudp 모듈의 inputname 옵션이 더 이상 사용되지 않음

rsyslog 서비스에 대한 **imudp** 모듈의 **inputname** 옵션은 더 이상 사용되지 않습니다. 대신 **name** 옵션을 사용합니다.

FedFS 가 더 이상 사용되지 않음

FedFS(FedFS)는 업스트림 FedFS 프로젝트가 더 이상 적극적으로 유지 관리되지 않기 때문에 더 이상 사용되지 않습니다. Red Hat은 FedFS 설치를 마이그레이션하는 보다 유연한 기능을 제공합니다.

v GPU 가 더 이상 사용되지 않음

Red Hat Enterprise Linux 6의 초기 릴리스 이후 vGPU 파일 시스템이 기술 프리뷰 상태에 있습니다. Red Hat은 완전히 지원되는 기능으로 Switching을 제공하지 않으며 향후 Red Hat Enterprise Linux 주요 릴리스에서 제거될 예정입니다.

v GPU 파일 시스템은 Red Hat Enterprise Linux 7.4의 업스트림에서 다양한 업데이트를 수신했으며 Red Hat Enterprise Linux 7 시리즈에서 계속 사용할 수 있습니다. 그러나 이 기능에 대한 마지막 예정된 업데이트입니다.

tcp_wrappers 더 이상 사용되지 않음

tcp_wrappers 패키지는 systat 및 systat에 대한 수신 요청을 모니터링하고 필터링할 수 있는 소규모 데몬 프로그램을 제공하는 패키지는 더 이상 사용되지 않습니다. systat,telnet,rlogin,rsh,tftp,talk,sshd 및 기타 네트워크 서비스에 대한 수신 요청을 모니터링하고 필터링할 수 있습니다.

nautilus-open-terminal 다음으로 교체됨 gnome-terminal-nautilus

Red Hat Enterprise Linux 7.3부터는 nautilus-open-terminal 패키지가 더 이상 사용되지 않고 gnome-terminal-nautilus 패키지로 교체되었습니다. 이 패키지는 Multus에서 마우스 오른쪽 클릭 컨텍스트 메뉴에 Open in Terminal 옵션을 추가하는코어 확장 기능을 제공합니다. nautilus-open-terminal 시스템을 업그레이드하는 동안 gnome-terminal-nautilus 으로 교체됩니다.

Python에서 sslwrap() 제거

sslwrap() 함수가 Python 2.7 에서 제거되었습니다. 466 Python 기능 개선 Proposal 이 구현된 후 이 기능을 사용하면 세그먼트 오류가 발생했습니다. 제거는 업스트림과 일치합니다.

대신 ssl.SSLContext 클래스와 ssl.SSLContext.wrap_socket() 함수를 사용하는 것이 좋습니다. 대부분의 애플리케이션에서는 보안 기본 설정으로 컨텍스트를 생성하는 ssl.create_default_context() 함수를 사용할 수 있습니다. 기본 컨텍스트는 시스템의 기본 신뢰 저장소도 사용합니다.

종속성으로 연결된 라이브러리의 기호는 더 이상 ld로 해결되지 않음

이전 버전에서는 일부 라이브러리가 다른 라이브러리의 종속성으로 암시적으로 링크된 경우에도 ld 링커에서 링크된 모든 기호를 해결했습니다. 이를 통해 개발자는 애플리케이션 코드에서 암시적으로 연결된

라이브러리의 기호를 사용하고 연결을 위해 이러한 라이브러리를 명시적으로 지정할 수 없었습니다.

보안상의 이유로 종속성으로 암시적으로 연결된 라이브러리의 기호에 대한 참조를 확인하지 않도록 ld 가 변경되었습니다.For security reasons, ld has been changed to resolve references in libraries linked implicitly as dependencies.

결과적으로 애플리케이션 코드가 선언되지 않은 라이브러리의 기호를 사용하여 연결 및 연결만 종속 항목으로 암시적으로 연결하려고 할 때 ld 와의 연결이 실패합니다. 종속 항목으로 연결된 라이브러리의 기호를 사용하려면 개발자는 이러한 라이브러리에 대해 명시적으로 연결해야 합니다.

이전 ld 동작을 복원하려면 -copy-dt-needed-entries 명령줄 옵션을 사용합니다. (BZ#1292230)

Windows 게스트 가상 머신 지원 제한

Red Hat Enterprise Linux 7의 경우 Windows 게스트 가상 머신은 AMQP(Advanced mission Critical)와 같은 특정 서브스크립션 프로그램에서만 지원됩니다.

libnetlink 가 더 이상 사용되지 않음

iproute-devel 패키지에 포함된 libnetlink 라이브러리가 더 이상 사용되지 않습니다. 대신 libnl 및 libmnl 라이브러리를 사용해야 합니다.

KVM의 S3 및 S4 전원 관리 상태가 더 이상 사용되지 않음

S3 (RAM에 일시 중단) 및 S4 (디스크에 일시 중단) 전원 관리 상태에 대한 기본 KVM 지원이 중단됩니다. 이 기능은 이전에 기술 프리뷰로 사용 가능했습니다.

인증서 서버 플러그인 udnPwdDirAuth가 중단됨

Red Hat Certificate Server의 udnPwdDirAuth 인증 플러그인이 Red Hat Enterprise Linux 7.3에서 제거되었습니다. 플러그인을 사용하는 프로필은 더 이상 지원되지 않습니다. udnPwdDirAuth 플러그인을 사용하여 프로필로 생성된 인증서는 승인된 경우에도 계속 유효합니다.

IdM용 Red Hat Access 플러그인이 중단됩니다.

Red Hat Access Management(IdM)용 Red Hat Access 플러그인이 Red Hat Enterprise Linux 7.3에서 제거되었습니다. 업데이트 중에 redhat-access-plugin-ipa 패키지가 자동으로 제거됩니다. 지식 베이스 액세스 및 지원 케이스 서비스와 같은 플러그인에서 이전에 제공한 기능은 Red Hat 고객 포털을 통

해 계속 사용할 수 있습니다. Red Hat은 redhat-support-tool 툴과 같은 대안을 살펴볼 것을 권장합니다.

페더레이션 SSO(Single Sign-On)를 위한 Ipsilon ID 공급자 서비스

ipsilon 패키지는 Red Hat Enterprise Linux 7.2에서 기술 프리뷰로 도입되었습니다. Ipsilon은 인증 공급자 및 애플리케이션 또는 유틸리티를 연결하여 SSO(Single Sign-On)를 허용합니다.

Red Hat은 Ipsilon을 기술 프리뷰에서 완전히 지원되는 기능으로 업그레이드하지 않습니다. ipsilon 패키지는 향후 마이너 릴리스에서 Red Hat Enterprise Linux에서 제거됩니다.

Red Hat은 Keycloak 커뮤니티 프로젝트를 기반으로 하는 웹 SSO 솔루션으로 Red Hat Single Sign-On을 출시했습니다. Red Hat Single Sign-On은 Ipsilon보다 뛰어난 기능을 제공하며 Red Hat 제품 포트폴리오에서 표준 웹 SSO 솔루션으로 지정됩니다.

몇 가지 rsyslog 옵션 더 이상 사용되지 않음

Red Hat Enterprise Linux 7.4의 rsyslog 유틸리티 버전에는 많은 수의 옵션이 더 이상 사용되지 않습니다. 이러한 옵션에는 더 이상 효과가 없으며 경고가 표시됩니다.

- 옵션 -c,-u,-q,-x,-A,-Q,-4, -6 옵션은 rsyslog 구성을 사용하여 수행할 수 있습니다.
- -l 및 -s
  옵션에 의해 이전에 제공되는 기능을 대체하지 않습니다.

memkind 라이브러리에서 더 이상 사용되지 않는 기호

memkind 라이브러리의 다음 기호는 더 이상 사용되지 않습니다.

- memkind_finalize()
- memkind_get_num_kind()
- memkind_get_kind_by_partition()

- **memkind_get_kind_by_name()**
- **memkind_partition_mmap()**
- **memkind_get_size()**
- **MEMKIND_ERROR_MEMALIGN**
- **MEMKIND_ERROR_MALLCTL**
- **MEMKIND_ERROR_GETCPU**
- **MEMKIND_ERROR_PMTT**
- **MEMKIND_ERROR_TIEDISTANCE**
- **MEMKIND_ERROR_ALIGNMENT**
- **MEMKIND_ERROR_MALLOCX**
- **MEMKIND_ERROR_REPNAME**
- **MEMKIND_ERROR_PTHREAD**
- **MEMKIND_ERROR_BADPOLICY**
- **MEMKIND_ERROR_REPPOLICY**

SCTP (RFC 6458) 용 소켓 API 확장 옵션 (RFC 6458) 더 이상 사용되지 않음

Stream Control Transmission Protocol에 대한 소켓 API 확장의 SCTP_SNDRCV,SCTP_EXTRCV 및 SCTP_DEFAULT_SEND_PARAM 은 RFC 6458 사양에 따라 더 이상 사용되지 않습니다.

새로운 옵션 SCTP_SNDINFO,SCTP_NXTINFO,SCTP_NXTINFO 및 SCTP_DEFAULT_SNDINFO 옵션은 더 이상 사용되지 않는 옵션을 대체하여 구현되었습니다.

SSLv2 및 SSLv3를 사용하여 NetApp ONTAP 관리는 더 이상 libstorageMgmt에서 지원되지 않습니다.

NetApp ONTAP 스토리지 어레이에 대한 SSLv2 및 SSLv3 연결은 libstorageMgmt 라이브러리에서 더 이상 지원되지 않습니다. 사용자는 NetApp 지원에 문의하여 TLS(Transport Layer Security) 프로토콜을 활성화할 수 있습니다.

dconf-dbus-1 은 더 이상 사용되지 않으며 dconf-editor 가 별도로 제공됩니다.

이번 업데이트를 통해 dconf-dbus-1 API가 제거되었습니다. 그러나 dconf-dbus-1 라이브러리는 바이너리 호환성을 유지하기 위해 백포트되었습니다. Red Hat은 dconf-dbus-1 대신 GDBus 라이브러리를 사용할 것을 권장합니다.

dconf-error.h 파일의 이름이 dconf-enums.h 로 변경되었습니다. 또한 이제 dconf 편집기 가 별도의 dconf-editor 패키지로 제공됩니다. 자세한 내용은 8장. *데스크탑* 참조하십시오.

freeradius는 더 이상 Auth-Type := 시스템을허용하지 않습니다.

FreeRADIUS 서버는 더 이상 rlm_unix 인증 모듈에 Auth-Type := System 옵션을 허용하지 않습니다. 이 옵션은 구성 파일의 authorize 섹션에서 unix 모듈을 사용하여 교체되었습니다.

더 이상 사용되지 않는 장치 드라이버

- 3w-9xxx
- 3w-sas
- mptbase

- **mptctl**
- **MPTSas**
- **MPtscsih**
- **MPTspi**
- **mvsas**
- **qla3xxx**
- **megaraid_sas** 드라이버의 다음 컨트롤러는 더 이상 사용되지 않습니다.
  - **Dell PERC5, PCI ID 0x15**
  - **SAS1078R, PCI ID 0x60**
  - **SAS1078DE, PCI ID 0x7C**
  - **SAS1064R, PCI ID 0x411**
  - **VERDE_ZCR, PCI ID 0x413**
  - **SAS1078GEN2, PCI ID 0x78**
- **qla2xxx** 드라이버의 다음 어댑터는 더 이상 사용되지 않습니다.

- ISP24xx, PCI ID 0x2422
- ISP24xx, PCI ID 0x2432
- ISP2422, PCI ID 0x5422
- QLE220, PCI ID 0x5432
- QLE81xx, PCI ID 0x8001
- QLE10000, PCI ID 0xF000
- QLE84xx, PCI ID 0x8044
- QLE8000, PCI ID 0x8432
- QLE82xx, PCI ID 0x8021

- be2net 드라이버에서 제어하는 다음 이더넷 어댑터는 더 이상 사용되지 않습니다.
  - redfishGERSHARK NIC, PCI ID 0x0700
- be2iscsi 드라이버의 다음 컨트롤러는 더 이상 사용되지 않습니다.
  - Emulex OneConnect 10Gb iSCSI Initiator (generic), PCI ID 0x212

- OCe10101, OCm10101, OCe10102, OCm10102 BE2 어댑터 제품군, PCI ID 0x702
- OCe10100 BE2 어댑터 제품군, PCI ID 0x703

- lpfc 드라이버의 다음 Emulex 보드가 더 이상 사용되지 않습니다.

BladeEngine 2 (BE2) 장치

- redfishGERSHARK FCOE, PCI ID 0x0704

파이버 채널(FC) 장치

- PCI ID 0x1ae5
- PROTEUS_VF, PCI ID 0xe100
- BALIUS, PCI ID 0xe131
- PROTEUS_PF, PCI ID 0xe180
- RFLY, PCI ID 0xf095
- PFLY, PCI ID 0xf098
- LP101, PCI ID 0xf0a1
- TFLY, PCI ID 0xf0a5
- BSMB, PCI ID 0xf0d1

- BMID, PCI ID 0xf0d5
- ZSMB, PCI ID 0xf0e1
- ZMID, PCI ID 0xf0e5
- NEPTUNE, PCI ID 0xf0f5
- NEPTUNE_SCSP, PCI ID 0xf0f6
- NEPTUNE_DCSP, PCI ID 0xf0f7
- FALCON, PCI ID 0xf180
- SUPERFLY, PCI ID 0xf700
- DRAGONFLY, PCI ID 0xf800
- CENTAUR, PCI ID 0xf900
- PEGASUS, PCI ID 0xf980
- THOR, PCI ID 0xfa00
- VIPER, PCI ID 0xfb00
- LP10000S, PCI ID 0xfc00

- LP11000S, PCI ID 0xfc10
- LPE11000S, PCI ID 0xfc20
- PROTEUS_S, PCI ID 0xfc50
- HELIOS, PCI ID 0xfd00
- HELIOS_SCSP, PCI ID 0xfd11
- HELIOS_DCSP, PCI ID 0xfd12
- ZEPHYR, PCI ID 0xfe00
- HORNET, PCI ID 0xfe05
- ZEPHYR_SCSP, PCI ID 0xfe11
- ZEPHYR_DCSP, PCI ID 0xfe12

시스템에서 하드웨어의 **PCI ID**를 확인하려면 **lspci -nn** 명령을 실행합니다.

여기에 나열되지 않은 드라이버의 다른 컨트롤러는 변경되지 않은 채로 남아 있습니다.

SFN4XXX 어댑터가 더 이상 사용되지 않음

Red Hat Enterprise Linux 7.4부터 **SFN4XXX Solarflare** 네트워크 어댑터는 더 이상 사용되지 않습니다. 이전에는 **Solarflare**에 모든 어댑터에 대해 단일 드라이버 **sfc** 가 있었습니다. 최근 **SFN4XXX** 지원은 **sfc**에서 분할되었으며 **sfc -falcon** 이라는 새로운 **SFN4XXX-only** 드라이버로 이동했습니다. 현재 두 드라이버는 계속 지원되지만 **sfc-falcon** 및 **SFN4XXX** 지원은 향후 주요 릴리스에서 제거될 예정입니다.

FCoE 스토리지 기술만 시작한 소프트웨어는 더 이상 사용되지 않습니다.

FCoE(Fibre Channel over Ethernet) 스토리지 기술의 일부만 시작된 소프트웨어는 고객 채택이 제한되어 더 이상 사용되지 않습니다. 스토리지 기술만 시작한 소프트웨어는 **Red Hat Enterprise Linux 7**의 라이프 사이클 기간 동안 계속 지원됩니다. 사용 중단 알림은 **Red Hat Enterprise Linux**의 향후 주요 릴리스에서 소프트웨어 시작 기반 **FCoE** 지원을 제거하려는 의도를 나타냅니다. 하드웨어 지원 및 관련 사용자 공간 툴(예: 드라이버, **libfc** 또는 **libfcoe**)은 사용 중단 알림의 영향을 받지 않습니다.

libvirt-lxc 툴을 사용하는 컨테이너가 더 이상 사용되지 않음

다음 **libvirt-lxc** 패키지는 **Red Hat Enterprise Linux 7.1** 이후 더 이상 사용되지 않습니다.

- **libvirt-daemon-driver-lxc**
- **libvirt-daemon-lxc**
- **libvirt-login-shell**

향후 **Linux** 컨테이너 프레임워크 개발은 이제 **docker** 명령줄 인터페이스를 기반으로 합니다. **libvirt-lxc** 툴링은 **Red Hat Enterprise Linux (Red Hat Enterprise Linux 7** 포함)의 향후 릴리스에서 제거될 수 있으며 사용자 정의 컨테이너 관리 애플리케이션 개발에 의존하지 않아야 합니다.

자세한 내용은 **Red Hat KnowledgeBase** 문서를 참조하십시오.

VI 부. 알려진 문제

이 부분에서는 **Red Hat Enterprise Linux 7.4**에서 알려진 문제를 설명합니다.

54장. 인증 및 상호 운용성

sudo 예기치 않게 그룹 조회를 수행할 때 액세스를 거부합니다.

이 문제는 이러한 조건을 모두 충족하는 시스템에서 발생합니다.

- 그룹 이름은 파일 또는 **sss** 와 같은 여러 **NNSS(Name Service Switch)** 소스에서 사용할 수 있는 **sudoers** 규칙에 구성되어 있습니다.

- **NSS** 우선순위는 로컬 그룹 정의로 설정됩니다. **/etc/nsswitch.conf** 파일에 다음 행이 포함된 경우 적용됩니다.

```
sudoers: files sss
```

- **match_group_by_gid** 라는 **sudo Defaults** 옵션이 **true** 로 설정됩니다. 이는 옵션의 기본값입니다.

NSS 소스 우선 순위로 인해 **sudo** 유틸리티에서 지정된 그룹의 **GID**를 조회하려고 할 때 **sudo** 는 로컬 그룹 정의만 설명하는 결과를 받습니다. 따라서 사용자가 원격 그룹의 멤버이지만 로컬 그룹이 아닌 경우 **sudoers** 규칙이 일치하지 않으며 **sudo** 는 액세스를 거부합니다.

이 문제를 해결하려면 다음 중 하나를 선택합니다.

- **sudoers** 에 대해 **match_group_by_gid** 기본값을 명시적으로 비활성화합니다. **/etc/sudoers** 파일을 열고 다음 행을 추가합니다.

```
Defaults !match_group_by_gid
```

- 파일에서 **sss NSS** 소스의 우선 순위를 지정하도록 **NSS**를 구성합니다. **/etc/nsswitch.conf** 파일을 열고 파일 앞에 **sss** 가 나열되어 있는지 확인합니다.

```
sudoers: sss files
```

이렇게 하면 **sudo** 가 원격 그룹에 속한 사용자에 대한 액세스를 허용합니다. **(BZ#1293306)**

KCM 인증 정보 캐시가 단일 인증 정보 캐시의 많은 인증 정보에 적합하지 않음

인증 정보 캐시에 인증 정보가 너무 많으면 **klist** 와 같은 **Kerberos** 작업이 **sssd-kcm** 구성 요소와 **sssd-secrets** 구성 요소 간에 데이터를 전송하는 데 사용되는 버퍼의 하드 코딩된 제한으로 인해 실패합니다.

이 문제를 해결하려면 **/etc/sssd/sssd.conf** 파일의 **[kcm]** 섹션에 **ccache_storage = memory** 옵션을 추가합니다. 이렇게 하면 **kcm** 응답자가 자격 증명 캐시를 영구적으로 저장하지 않고 메모리에 저장하도록 지시합니다. 이 작업을 수행하면 시스템을 다시 시작하거나 **sssd-kcm** 가 인증 정보 캐시를 지웁니다. **(BZ#1448094)**

sssd-secrets 구성 요소가 로드 상태에 있을 때 충돌

sssd-secrets 구성 요소에서 많은 요청을 수신하면 상황은 **sssd-secrets** 가 예기치 않게 종료되는 **NNSS(Network Security Services)** 라이브러리에서 버그를 트리거합니다. 그러나 **systemd** 서비스는 다음 요청 시 **sssd-secrets** 를 다시 시작하므로 서비스 거부는 일시적인 것입니다. **(BZ#1460689)**

SSSD는 동일한 우선 순위로 여러 인증서 일치 규칙을 올바르게 처리하지 않습니다.

지정된 인증서가 동일한 우선 순위와 여러 인증서 일치 규칙과 일치하는 경우 **SSSD(System Security Services Daemon)**는 규칙 중 하나만 사용합니다. 이 문제를 해결하려면 **LDAP** 필터가 **|** (또는) **Operator** 와 연결된 개별 규칙의 필터로 구성된 단일 인증서 일치 규칙을 사용합니다. 인증서 일치 규칙의 예는 **sss-certamp(5)** 매뉴얼 페이지를 참조하십시오. **(BZ#1447945)**

SSSD는 **ID** 덮어쓰기에서 고유한 인증서만 조회할 수 있습니다.

여러 **ID** 재정의에 동일한 인증서가 포함된 경우 **SSSD(System Security Services Daemon)**가 인증서와 일치하는 사용자에 대한 쿼리를 확인할 수 없습니다. 이러한 사용자를 검색하려고 하면 사용자를 반환하지 않습니다. 사용자 이름 또는 **UID**를 사용하여 사용자를 조회하는 것은 예상대로 작동합니다. **(BZ#1446101)**

ipa-advise 명령은 스마트 카드 인증을 완전히 구성하지 않습니다.

ipa-advise config-server-for-smart-card-auth 및 **ipa-advise config-client-for-smart-card-auth** 명령은 스마트 카드 인증을 위해 **IdM(Identity Management)** 서버 및 클라이언트를 완전히 구성하지 않습니다. 그 결과 **ipa-advise** 명령이 생성한 스크립트를 실행한 후 스마트 카드 인증이 실패합니다. 이 문제를 해결하려면 **Linux** 도메인 **ID**, 인증 및 정책 가이드의 개별 사용 사례에 대한 수동 단계를 참조하십시오. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/smart-cards.html **(BZ#1455946)**

libwbclient 라이브러리가 **Red Hat Enterprise Linux 7.4**에서 호스팅되는 **Samba** 공유에 연결하지 못했습니다.

Samba와 **SSSD(System Security Services Daemon) Winbind** 플러그인 구현의 인터페이스가 변경되었습니다. 그러나 **SSSD**에서는 이러한 변경 사항이 없습니다. 결과적으로 **Winbind** 데몬 대신 **SSSD libwbclient** 라이브러리를 사용하는 시스템은 **Red Hat Enterprise Linux 7.4**에서 실행되는 **Samba**에서 제공하는 공유에 액세스하지 못합니다. 해결 방법을 사용할 수 없으며 **Winbind** 데몬을 실행하지 않고

libwbclient 라이브러리를 사용하는 경우 **Red Hat Enterprise 7.4**로 업그레이드하지 않는 것이 좋습니다. **(BZ#1462769)**

인증서 시스템 **ubsystems TLS_ECDHE_RSA_*** 암호 및 특정 **HSM**과의 통신 문제가 발생합니다.

TLS_ECDHE_RSA_* 암호화가 활성화된 동안 특정 **HSM**을 사용하면 하위 시스템에서 통신 문제가 발생합니다. 이 문제는 다음 시나리오에서 발생합니다.

- **CA**가 설치되어 있고 두 번째 하위 시스템이 설치되고 보안 도메인으로 **CA**에 연결하려고 하면 설치에 성공할 수 없습니다.
- **CA**에서 인증서 등록을 수행하는 동안 아카이브가 필요한 경우 **CA**는 **KRA**와 동일한 통신 문제가 발생합니다. 이 시나리오는 이전 암호가 설치에 일시적으로 비활성화된 경우에만 발생할 수 있습니다.

이 문제를 해결하려면 가능한 경우 **TLS_ECDHE_RSA_*** 암호를 끕니다. **Perfect Forward Secrecy**는 **TLS_ECDHE_RSA_*** 암호를 사용하여 추가 보안을 제공하지만 각 **SSL** 세션은 설정하는 데 약 **3** 배 더 오래 걸립니다. 또한 기본 **TLS_RSA_*** 암호화는 인증서 시스템 작업에 적합합니다. **(BZ#1256901)**

55장. 컴파일러 및 도구

실행 가능한 스택을 사용하지 않도록 설정하는 경우 **regular** 표현식의 성능은 **qcow** 기술로 향상될 수 없습니다.

SELinux 정책이 실행 가능한 스택을 허용하지 않는 경우 **PCRE** 라이브러리는 정규 표현식의 속도를 높이기 위해 **JIT** 컴파일을 사용할 수 없습니다. 결과적으로 정규식에 대해 **tcpdump** 컴파일을 시도하면 무시되고 성능이 향상되지 않습니다.

이 문제를 해결하기 위해 영향을 받는 **SELinux** 도메인에 대해 **execmem** 작업을 활성화하는 규칙으로 **SELinux** 정책을 수정하여 **1.4** 컴파일을 활성화합니다. 일부 규칙은 이미 제공되며 특정 **SELinux** 부울에서 활성화할 수 있습니다. 이러한 부울을 나열하려면 다음 명령의 출력을 참조하십시오.

```
getsebool -a | grep execmem
```

또 다른 해결 방법은 **PCre_study()** 함수에 대한 호출을 사용하여 **JIT** 컴파일을 요청하지 않도록 애플리케이션 코드를 변경하는 것입니다. **(BZ#1290432)**

Gluster 라이브러리를 언로드한 후 특정 애플리케이션이 종료되지 않으면 메모리 누수가 발생합니다.

Gluster는 기능 및 기능을 구현하는 다양한 내부 구성 요소 및 번역기로 구성됩니다. **Gluster**를 애플리케이션과 긴밀하게 통합하기 위해 **gfapi** 액세스 방법이 추가되었습니다. 그러나 모든 구성 요소와 번역가가 실행 중인 애플리케이션에서 언로드되도록 설계된 것은 아닙니다. 따라서 **Gluster** 라이브러리를 언로드한 후 종료하지 않는 프로그램은 **Gluster**에서 내부적으로 수행하는 일부 메모리 할당을 해제할 수 없습니다.

메모리 누수 양을 줄이기 위해 애플리케이션이 **im fs_init()** 및 **glfs_fini()** 함수를 호출하지 못하도록 합니다. 누수 메모리를 해제하려면 장기 실행 애플리케이션을 다시 시작해야 합니다. **(BZ#1409773)**

DISA SRG에 대한 **URL**이 잘못되었습니다.

SCAP Security Guide(SSG) 규칙은 **Defense Information Systems countries Security Requirement Guides (DISA SRGs)**를 참조하십시오. **404 - not found** 오류와 함께 **URL**에 연결하는 데 실패합니다. 결과적으로 사용자는 **SRG**에 대한 직접 참조가 없습니다. 이 문제를 해결하려면 새 **URL**을 사용하십시오. **http://iase.disa.mil/stig/os/general/Pages/index.aspx/ (BZ#1464899)**

ensure_gpgcheck_repo_metadata 규칙이 실패합니다.

ensure_gpgcheck_repo_metadata 규칙을 수정하는 동안 특정 프로필이 **yum.conf** 파일을 업데이트하여 **repo_gpgcheck** 옵션을 활성화합니다. **Red Hat**은 현재 서명된 리포지터리 메타데이터를 제공하지 않습니다. 그 결과 **yum** 유틸리티는 더 이상 공식 리포지토리에서 패키지를 설치할 수 없습니다. 이 문제를 해결하려면 맞춤형 파일을 사용하여 프로필에서 **ensure_gpgcheck_repo_metadata** 를 제거합니다. 수정을 통해 시스템이 이미 손상되면 **yum.conf** 를 업데이트하고 **repo_gpgcheck** 를 **0** 으로 설정합니다. **(BZ#1465677)**

SSG pam_octets 모듈 사용률 검사에서 default=die를 잘못 허용함

SCAP 보안 가이드 (SSG) pam_octets 모듈 사용률 검사에서 default=die 옵션을 잘못 허용합니다. 그 결과, pam_unix 모듈을 사용한 사용자 인증이 실패하면 pam_octets의 카운터를 늘리지 않고 pam_unix 모듈이 즉시 중지됩니다. 이 문제를 해결하려면 authfail 옵션 앞에 default=die 를 사용하지 마십시오. 이렇게 하면 pam_octets 카운터가 올바르게 증가됩니다. (BZ#1448952)

56장. 데스크탑

totem 만 업데이트 실패

totem 및 **gstreamer1-plugins-bad-free** 패키지 간 명시적 종속성이 없습니다. 결과적으로 **totem** 패키지만 업데이트하려고 하면 작업이 실패합니다. 이 문제를 해결하려면 **totem** 패키지를 자체적으로 업데이트하지 말고 시스템 업데이트에 의존하지 마십시오. (BZ#1451211)

운영 체제는 부팅 시 항상 **Wacom Expresskeys** 원격 모드 **1**로 가정합니다.

Wacom Expresskeys Remote(EKR)는 독립형 장치이므로 **OS(**운영 체제**)**가 부팅될 때 모든 운영 모드로 전환할 수 있습니다. 그러나 현재 **OS**는 부팅 시 **EKR**이 항상 **1** 모드로 설정되어 있다고 가정합니다. 그 결과 **EKR** 모드가 시스템 부팅 전에 **1**로 설정되지 않은 경우 **EKR**이 **OS**와 동기화되지 않습니다. 이 문제를 해결하려면 **OS**를 시작하기 전에 **EKR**을 **1** 모드로 설정합니다. (BZ#1458351)

Multus에서 다운로드한 **RPM** 파일을 설치할 수 없습니다 .

Multus 파일 **manger**에서 **RPM** 파일을 두 번 클릭하면 설치 중인 파일 대신 다음 오류가 반환됩니다.

> Sorry, this did not work, File is not supported

이러한 문제는 **PackageKit** 의 **yum** 백엔드에서 로컬 파일에 대한 세부 정보 가져오기를 지원하지 않기 때문에 발생합니다.

이 문제는 **gnome-packagekit** 을 설치하여 이중 클릭 작업을 처리하거나 **yum** 을 사용하여 파일을 수동으로 설치하여 문제를 해결할 수 있습니다. (BZ#1434477)

Yelp가 **HTML** 형식의 파일을 올바르게 표시하지 않음

이전 버전의 **yelp** 에서는 **HTML** 형식의 파일이 표시될 수 있었습니다. 버전 **3.22**에서는 이 기능이 더 이상 작동하지 않으며 자격이 있는 텍스트 **URL**을 사용하여 알 수 없는 오류 를 반환할 수 없습니다.

문제는 **yelp** 자체의 아키텍처 변경과 관련이 있을 수 있으므로 현재 해결방법은 없습니다.

시스템 관리자는 이 사용 사례를 지원하지 않으며 **Mallard** 또는 **Docbook** 데이터를 입력으로 예상합니다.

HTML 형식의 콘텐츠를 표시하는 대체 방법을 고려해야 합니다. (BZ#1443179)

일부 **AMD** 하드웨어와 모니터를 연결할 때 자동 모드 설정 실패

일부 구성에서는 AMD 하드웨어를 사용하여 시스템에 추가 모니터를 추가하는 경우 새 하드웨어를 자동으로 활성화하지 못할 수 있습니다.

이 문제는 현재 조사 중입니다.

이 문제를 해결하려면 시스템 관리자가 수동으로 xrandr(1)를 호출하여 모니터를 활성화해야 합니다. (BZ#1393951)

종속성이 없기 때문에 Libre office 없이 일부 문서를 설치할 때 GNOME 문서 도 표시할 수 없습니다.

GNOME 문서는 LibreOffice 제품군에서 제공하는 라이브러리를 사용하여 OpenDocument 텍스트 또는 Open Office XML 형식과 같은 특정 유형의 문서를 렌더링합니다. 그러나 필요한 라이브러리 (libreoffice-filters)는 gnome-documents 패키지의 종속성 목록에서 누락되어 있습니다. 따라서 LibreOffice 가 없는 시스템에 Gnome Documents 를 설치하는 경우 앞서 언급한 문서 유형을 렌더링할 수 없습니다.

이 문제를 해결하려면 LibreOffice 자체를 사용하지 않는 경우에도 libreoffice-filters 패키지를 수동으로 설치하십시오. (BZ#1466164)

애플리케이션 설치 관리자 는 큰 endian 아키텍처에 설치할 수 없는 경우에도 패키지를 표시합니다.

IBM Power Systems 또는 IBM z Systems와 같은 big-endian 시스템에서 Application Installer 그래픽 패키지 설치 프로그램(gnome-software 패키지)을 사용하는 경우 사용 가능한 패키지 중 일부는 설치할 수 없으며 이로 인해 설치 중 오류 메시지가 표시됩니다. 이는 현재 64비트 AMD 및 Intel 호환 (little-endian) 시스템용으로만 생성되는 패키지 메타데이터로 인해 발생하는 알려진 문제이며, 모든 패키지가 big-endian 아키텍처에서도 제공된다고 가정하면 그렇지 않습니다.

이 문제에 대한 해결 방법은 없지만, 오류 메시지는 설치할 수 없는 패키지 이외의 다른 결과는 없습니다. (BZ#1464139)

소프트웨어 추가/제거 도구(gpk-application)는 첫 번째 시도에서 새로 가져온 키를 사용하지 않습니다.

GNOME 에서 소프트웨어 추가/제거 그래픽 인터페이스를 사용하여 아직 가져오지 않은 키로 서명된 패키지를 설치할 때 툴에 키를 가져올 수 있는 프롬프트가 표시됩니다. 그러나 키를 가져오는 경우에도 즉시 키를 사용하지 못하게 하는 버그로 인해 설치에 실패합니다. 문제를 해결하려면 동일한 패키지를 다시 설치하십시오. 이 시점에서 키가 이미 이전 시도에서 가져온 후 설치에 성공합니다. (BZ#1387181)

여러 PCI 장치를 사용하여 여러 개의 디스플레이가 있는 가상 머신 표시 크기를 조정하면 X 가 충돌합니다.

QXL 드라이버(xorg-x11-drv-qxl)의 버그로 인해 가상 머신에 여러 PCI 장치를 사용하도록 구성된 경우 디스플레이 크기 조정 시 X.Org 표시 서버가 충돌합니다. 단일 PCI 장치를 사용하도록 여러 모니터가

있는 **Red Hat Enterprise Linux**를 실행하는 게스트 가상 머신이 구성되어 있는지 확인합니다. **Red Hat Virtualization**에서 이 설정은 **Edit -> Console** 아래의 **Single PCI** 장치 확인란을 통해 제어되며 기본적으로 활성화되어 있습니다. (**BZ#1428340**)

RHEA는 **GNOME classic** 세션에서 아이콘을 숨기지 않습니다.

GNOME Tweak Tool은 기본적으로 아이콘이 숨겨져 있는 **gnome** 세션에서 아이콘을 표시하거나 숨길 수 있으며 **GNOME classic** 세션에서는 무시됩니다. 결과적으로 **GNOME Tweak** 도구가 이 옵션을 표시하더라도 **GNOME classic** 세션에서 아이콘을 숨길 수 없습니다. (**BZ#1474852**)

잘못된 종속성 **flatpak**

flatpak 패키지의 잘못된 종속성으로 인해 사용자에게 다음 오류가 발생할 수 있습니다.

```
flatpak: error while loading shared libraries: libostree-1.so.1: cannot open shared object file: No such file or directory
```

이 문제를 해결하려면 **flatpak-libs** 패키지를 설치하십시오. 또는 처음에 **flatpak** 을 설치하는 대신 다음을 실행하여 두 패키지를 모두 설치합니다.

```
sudo yum -y install flatpak flatpak-libs
```

(**BZ#1476905**)

업데이트 후 **Firefox**가 시작되지 않음

fire Firefox-52.1.2-.el7.x86_64로 업그레이드한 후 일부 경우에는 브라우저가 시작되지 않습니다. 이는 **nspr** 및 **nss** 패키지가 **Red Hat Enterprise Linux 7.4** 배치에서 업데이트되지 않기 때문입니다. 이 문제를 해결하려면 **Red Hat Enterprise 7.4** 릴리스에서 **nspr** 및 **nss** 패키지를 업데이트하십시오. 가능한 또 다른 해결방법은 **Firefox**를 다운그레이드하는 것입니다. 하지만 이 옵션은 권장되지 않습니다. 그 결과 **Firefox** 웹 브라우저를 다시 시작할 수 있습니다. (**BZ#1455798**)

Xorg의 시각적 개체에 대한 제한적인 지원

Xorg 서버에서는 하드웨어 드라이버에 대해 **TrueColor** 및 **Direct colors** 시각적 개체만 깊이 **16** 이상에서 지원됩니다. **Pseudo adoption** 시각적 개체가 필요한 레거시 애플리케이션을 실행할 수 있습니다. **Xephyr** 중첩된 **X** 서버에 대해 실행할 수 있습니다. (**BZ#1185690**)

57장. 파일 시스템

NFSv4를 제공하는 **NetApp** 스토리지 어플라이언스가 구성을 확인하는 것이 좋습니다.

NFSv4를 제공하는 **NetApp** 스토리지 어플라이언스를 사용할 때 마이너 버전에서 기능을 활성화하거나 비활성화할 수 있습니다.

다음과 같은 **Data ONTAP** 명령을 사용하여 적절한 기능을 원하는 대로 사용하도록 설정할 수 있도록 구성을 확인하는 것이 좋습니다.

```
vserver nfs show -vserver <vserver-name> -fields v4.0-acl,v4.0-read-delegation,v4.0-write-
delegation,v4.0-referrals,v4.0-migration,v4.1-referrals,v4.1-migration,v4.1-acl,v4.1-read-
delegation,v4.1-write-delegation
```

(BZ#1450447)

58장. 하드웨어 활성화

i40e 드라이버는 가장 일반적인 **HWTSTAMP** 필터를 거부합니다.

INTEL-SA-00063 권고에 설명된 **Intel** 이더넷 컨트롤러 **X710** 및 **XL710** 제품군의 보안 수정에서 **L4** 타임스탬프링**(UDP)**을 비활성화하기 때문에 **i40e** 장치 드라이버는 가장 일반적인 **HWTSTAMP** 필터를 거부합니다. 이 문제는 최신 **X722** 장치가 아닌 **Intel X710** 장치에만 영향을 미칩니다. **(BZ#1431964)**

59장. 설치 및 부팅

HTTPS kickstart 소스에서 설치할 때 FIPS 모드 지원되지 않음

설치 이미지는 **HTTPS kickstart** 소스를 사용하여 설치 중에 **FIPS** 모드를 지원하지 않습니다. 결과적으로 현재 **fips=1** 및 **inst.ks=https://<location>/ks.cfg** 옵션을 사용하여 시스템을 설치할 수 없습니다. **(BZ#1341280)**

UEFI 및 IPv6로 PXE 부팅은 운영 체제 선택 메뉴 대신 GRUB2 쉘을 표시합니다.

UEFI 및 IPv6로 구성된 클라이언트에서 **Pre-Boot Execution Environment(PXE)** 가 시작되면 **/boot/grub/grub.cfg** 파일에 구성된 부팅 메뉴가 표시되지 않습니다. 제한 시간이 지나면 구성된 운영 체제 선택 메뉴 대신 **GRUB2** 쉘이 표시됩니다. **(BZ#1154226)**

비**alphanumeric** 문자가 있는 드라이버**disk** 파티션을 지정하면 잘못된 출력 **Kickstart** 파일이 생성됩니다.

Anaconda 설치 프로그램을 사용하여 **Red Hat Enterprise Linux**를 설치할 때 **Kickstart** 파일에 드라이버 디스크가 포함된 파티션의 경로를 포함하여 드라이버 디스크를 추가할 수 있습니다. 현재 **LABEL** 또는 **CDLABEL**으로 파티션을 지정하는 경우**alphanumeric** 문자가 있는 경우 예를 들면 다음과 같습니다.

```
driverdisk "CDLABEL=Fedora 23 x86_64:/path/to/rpm"
```

Anaconda 설치 중에 생성된 출력 **Kickstart** 파일에는 잘못된 정보가 포함됩니다. 이 문제를 해결하려면 **LABEL** 또는 **CDLABEL**으로 파티션을 지정할 때 영숫자만 사용하십시오. **(BZ#1452770)**

ology Computing 변형은 특정 보안 프로파일에 필요한 누락된 패키지입니다.

컴퓨팅 노드라고도 하는 **related Computing** 변형용 **Red Hat Enterprise Linux** 를 설치할 때 다른 변형의 설치 프로세스와 마찬가지로 보안 프로필을 선택할 수 있습니다. 그러나 이 변형은 최소이므로 미국 정부 구성 기준선 과 같은 특정 프로필에 필요한 패키지가 누락되어 있습니다. 이 프로필을 선택하면 설치 프로그램에 일부 패키지가 누락되었음에 대한 경고가 표시됩니다.

경고는 누락된 패키지라도 설치를 계속할 수 있습니다. 이 패키지는 문제를 해결하는 데 사용할 수 있습니다. 그러나 설치가 정상적으로 완료되지만 경고에도 불구하고 시스템을 설치한 다음 설치 후 보안 검사를 시도하면 검사에서 이러한 누락된 패키지로 인해 실패한 규칙을 보고합니다. 이 동작은 예상됩니다. **(BZ#1462647)**

60장. 커널

보조 코어가 오프라인이 아닌 경우 **kexec** 가 실패합니다.

특정 상황에서 **secondary-core offlining**은 **HP vGPU m400** 및 **AppliedMicro Mustang**과 같은 **AppliedMicro X-Gene** 플랫폼에서 실패합니다. 결과적으로 커널 패닉이 발생할 때 커널이 **kexec**를 통해 **kdump** 크래시 덤프 메커니즘 을 트리거하지 못하는 경우가 있습니다. 따라서 커널 크래시 덤프 파일이 저장되지 않습니다. **(BZ#1218374)**

캐시 플러시가 잘못되어 파일 시스템 손상이 수정되었지만 **I/O** 작업 속도가 느려질 수 있습니다.

megaraid_sas 드라이버의 버그로 인해 파일 시스템 손상은 시스템 종료, 재부팅 또는 정전 중에 파일 시스템이 디스크-쓰기 백 캐시와 함께 사용되었을 때 이전에 발생했습니다. 이번 업데이트에서는 **megaraid_sas** 가 플러시 캐시 명령을 **raid** 카드에 올바르게 전송합니다. 결과적으로 **raid** 카드 펌웨어도 업데이트하는 경우 설명된 상황에서 파일 시스템 손상이 더 이상 발생하지 않습니다.

Broadcom megaraid_sas raid 어댑터를 사용하면 시스템 로그 **(dmesg)**에서 기능을 확인할 수 있습니다. 적절한 기능은 다음 텍스트 문자열로 표시됩니다.

```
FW supports sync cache Yes
```

이 수정으로 인해 캐시가 올바르게 플러시되므로 **I/O** 작업이 느려질 수 있습니다. **(BZ#1380447)**

핫플러그되지 않고 신속하게 연결할 때 **Wacom Cintiq 12WX**가 다시 탐지되지 않습니다.

동일한 **USB** 포트 내에서 **Wacom Cintiq 12WX**에서 연결 해제 및 빠르게 연결 해제할 때, 불타일러는 현재 인식되지 않습니다. 이 문제를 해결하려면 알레일을 다시 연결하기 전에 **3~5~5**초 동안 기다립니다. **(BZ#1458354)**

GUI를 시작할 때 가상 **DVD**를 사용하여 일부 **IBM POWER8** 머신에 설치할 수 없습니다.

Red Hat Enterprise Linux 7.4는 **Anaconda GUI**를 시작하는 동안 일부 **IBM POWER8** 하드웨어 **(S822LC** 시스템 포함)에 설치되지 않을 수 있습니다.

이 문제는 **X11**을 시작하는 동안 오류가 발생하고 **Pane**이 **Anaconda** 화면에서 사라진 메시지가 있다는 것입니다.

해결방법은 **inst.text** 를 커널 명령줄에 추가하고 텍스트 모드로 설치하는 것입니다.

이 문제는 가상 **DVD** 설치로 제한되며 **netboot** 이미지를 사용한 추가 테스트를 통해 **GUI**를 설치할 수 있습니다. **(BZ#1377857)**

키보드 바로 가기를 사용하여 전체 화면 모드를 입력하면 VMWare ESXi 5.5에서 표시 문제가 발생합니다.

Red Hat Enterprise Linux 7.4를 VMWare ESXi 5.5 호스트에서 실행 중인 가상 머신 게스트로 사용하는 경우 Ctrl+Alt+Enter 를 눌러 콘솔에서 전체 화면 모드로 전환하면 디스플레이를 사용할 수 없게 됩니다. 동시에 다음 예제와 같은 오류는 시스템 로그(dmesg)에 저장됩니다.

```
[drm:vmw_cmdbuf_work_func [vmwgfx]] *ERROR* Command buffer error.
```

이 문제를 해결하려면 가상 머신을 종료하고 .vmx 구성 파일을 열고 다음 매개변수를 추가하거나 수정합니다.

```
svga.maxWidth = X
svga.maxHeight = Y
svga.vramSize = "X * Y * 4"
```

위의 경우 X 및 Y를 화면의 수평 및 수직 해상도로 바꿉니다. svga.vramSize 매개변수는 X times Y times 4와 같은 값을 사용합니다. 따라서 1920x1080의 해상도가 있는 화면의 예제 설정은 다음과 같습니다.

```
svga.maxWidth = 1920
svga.maxHeight = 1080
svga.vramSize = "8294400"
```

VMWare ESXi 5.5는 이 버그가 발생하는 것으로 보고된 유일한 버전입니다. 다른 버전은 문제없이 전체 화면 모드로 전환할 수 있습니다. (BZ#1451242)

KSC는 현재 xz 압축을 지원하지 않습니다.

커널 모듈 소스 검사기(ks c 툴)는 현재 xz 압축 방법을 처리할 수 없으며 다음 오류를 보고합니다.

```
Invalid architecture, supported architectures are x86_64, ppc64, s390x
```

이러한 제한 사항이 해결될 때까지 시스템 관리자는 ksc 도구를 실행하기 전에 xz 압축을 사용하여 타사 모듈을 수동으로 압축 해제해야 합니다. (BZ#1463600)

61장. 네트워킹

MD5 해시 알고리즘을 사용한 서명 확인은 **Red Hat Enterprise Linux 7**에서 비활성화되어 있습니다.

MD5 서명된 인증서가 필요한 모든 **WPA(Enterprise Access Point)**에 연결하는 것은 불가능합니다. 이 문제를 해결하려면 **/usr/lib/systemd/system/** 디렉터리에서 **/etc/systemd/system/** 디렉터리로 **wpa_supplicant.service** 파일을 복사하고 파일의 서비스 섹션에 다음 행을 추가합니다.

```
Environment=OPENSSL_ENABLE_MD5_VERIFY=1
```

그런 다음 **systemctl daemon-reload** 명령을 **root**로 실행하여 서비스 파일을 다시 로드합니다.

중요: **MD5** 인증서는 매우 안전하지 않으며 **Red Hat**은 사용하지 않는 것이 좋습니다. **(BZ#1062656)**

RHEL 7.3에서 업그레이드할 때 **freeradius** 가 실패할 수 있습니다.

/etc/raddb/radiusd.conf 파일의 새 구성 속성 **correct_escapes** 은 **RHEL 7.4** 이후 배포된 **freeradius** 버전에서 도입되었습니다. 관리자가 **correct_escapes** 를 **true** 로 설정하면 백슬래시 이스케이프에 대한 새 정규식 구문이 예상됩니다. **correct_escapes** 이 **false** 로 설정된 경우 이전 구문에서 백슬래시도 이스케이프해야 합니다. 이전 버전과의 호환성을 위해 **false** 는 기본값입니다.

업그레이드할 때 관리자가 수정하지 않는 한 **/etc/raddb/** 디렉토리의 구성 파일을 덮어쓰므로 **correct_escapes** 값이 모든 구성 파일에서 사용되는 구문 유형과 일치하지 않을 수 있습니다. 결과적으로 **freeradius** 의 인증이 실패할 수 있었습니다.

문제가 발생하지 않도록 하려면 **freeradius** 버전 **3.0.4 (RHEL 7.3**으로 배포) 및 이전 버전에서 업그레이드 한 후 **/etc/raddb/** 디렉토리에 있는 모든 설정 파일이 새로운 **escaping** 구문을 사용합니다(더 이상 백슬래시 문자를 찾을 수 없음) **/etc/raddb/radiusd.conf** 의 **correct_escapes** 값이 **true** 로 설정되어 있는지 확인합니다.

자세한 내용은 다음 주소에 있는 솔루션을 참조하십시오 https://access.redhat.com/solutions/3241961. **(BZ#1489758)**

certutil 은 FIPS 모드에서 NSS 데이터베이스 암호 요구 사항을 반환하지 않습니다.

certutil 툴을 사용하여 새 **NNSS(Network Security Services)** 데이터베이스를 생성할 때 사용자는 **FIPS** 모드에서 실행할 때 데이터베이스 암호 요구 사항이 무엇인지 확인할 수 없습니다. 프롬프트 메시지는 암호 요구 사항을 제공하지 않으며 **certutil** 은 일반적인 오류 메시지만 반환합니다.

```
certutil: could not authenticate to token NSS FIPS 140-2 Certificate DB.: SEC_ERROR_IO: An I/O error occurred during security authorization.
```

(BZ#1401809)

systemd-importd runs as init_t

systemd-importd 서비스는 **systemd** 장치 파일에서 **NoNewPrivileges** 보안 플래그를 사용합니다. 이렇게 하면 **init_t** 에서 **systemd_importd_t** 도메인으로 **SELinux** 도메인 전환이 차단됩니다. **(BZ#1365944)**

kickstart 설치에서 SCAP 암호 길이 요구 사항이 무시됩니다.

대화형 **Kickstart** 설치에서는 **SCAP** 규칙에 의해 정의된 암호 길이 검사를 적용하고 더 짧은 루트 암호를 허용하지 않습니다. 이 문제를 해결하려면 **Kickstart** 파일의 **pwpolicy root** 명령과 함께 **--strict** 옵션을 사용합니다. **(BZ#1372791)**

rhnsd.pid 는 그룹 및 다른 사람이 쓸 수 있습니다.

Red Hat Enterprise Linux 7.4에서 **/var/run/rhnsd.pid** 파일의 기본 권한이 **-rw-rw-rw-.. .** 이 설정은 안전하지 않습니다. 이 문제를 해결하려면 소유자만 쓸 수 있도록 이 파일의 권한을 변경합니다.

```
# chmod go-w /var/run/rhnsd.pid
```

(BZ#1480306)

63장. 스토리지

클러스터의 RAID 상단에서 씬 프로비저닝 지원 없음

RAID 논리 볼륨 및 씬 프로비저닝된 논리 볼륨은 독점적으로 활성화될 때 클러스터에서 사용할 수 있지만 현재 클러스터의 RAID 상단에서 씬 프로비저닝을 지원하지 않습니다. 이 경우는 조합이 독점적으로 활성화되더라도 발생합니다. 현재 이 조합은 LVM의 단일 시스템 비 클러스터 모드에서만 지원됩니다. (BZ#1014758)

LVM 또는 md 장치에 이전 설치의 메타데이터가 있는 경우 Anaconda 설치에 실패할 수 있습니다.

Red Hat Enetrprise Linux 7 설치 중에 이전 설치에서 이미 LVM 또는 md 메타데이터로 시작하는 시스템의 Red Hat Enetrprise Linux 7 설치 중에 다중패스가 장치에 설정되지 않으며 Anaconda가 시작되는 동안 LVM/md가 경로 장치 중 하나에 설정됩니다. 그러면 Anaconda에 문제가 발생하여 설치에 실패할 수 있습니다. 이 문제의 해결방법은 설치를 위해 부팅할 때 mpath.wwid=<WWID >를 커널 명령 줄에 추가하는 것입니다. <WWID >는 다중 경로가 요청하는 장치의 wwid입니다. 이 값은 DASD 장치의 경우 scsi 장치 및 ID_UID 의 ID_SERIAL udev 데이터베이스 값과도 동일합니다. (BZ#1378714)

64장. 시스템 및 서브스크립션 관리

시스템 업그레이드로 인해 **rdma-core** 이 설치된 경우 **yum**이 불필요한 **32**비트 패키지를 설치할 수 있습니다.

Red Hat Enterprise Linux 7.4에서 **rdma-core.noarch** 패키지는 **rdma-core.i686** 및 **rdma-core.x86_64** 에서 더 이상 사용되지 않습니다. 시스템 업그레이드 중에 **YUM** 은 원래 패키지를 새 패키지로 교체하고 필요한 모든 종속 항목을 설치합니다. 즉, **32** 비트 패키지뿐만 아니라 잠재적으로 많은 양의 **32** 비트 종속성이 필요하지 않은 경우에도 기본적으로 설치됩니다.

이 문제를 해결하려면 **--exclude=*.i686** 옵션과 함께 **yum update** 명령을 사용하거나 **32**비트 패키지를 제거하려면 업그레이드 후에 **yum remove rdma-core.i686** 을 사용할 수 있습니다. **(BZ#1458338)**

65장. 가상화

OVMF 게스트 부팅 실패

현재 qemu-kvm 패키지를 사용하여 Red Hat Enterprise Linux 호스트에서 OVMF(Open Virtual Machine Firmware)를 사용하는 게스트 가상 머신을 부팅하려고 하면 게스트가 응답하지 않고 빈 화면이 표시됩니다. (BZ#1174132)

virsh iface-bridge 를 사용하여 브리지 생성에 실패합니다.

네트워크 이외의 다른 소스에서 Red Hat Enterprise Linux 7을 설치할 때 인터페이스 구성 파일에서 네트워크 장치 이름이 기본적으로 지정되지 않습니다(이는 DEVICE= 줄로 수행됨). 그 결과 virsh iface-bridge 명령을 사용하여 네트워크 브리지를 생성하면 오류 메시지가 표시되고 실패합니다. 이 문제를 해결하려면 /etc/sysconfig/network-scripts/ifcfg-* 파일에 DEVICE= 행을 추가합니다.

자세한 내용은 Red Hat Knowledgebase https://access.redhat.com/solutions/2792701 (BZ#1100588)을 참조하십시오.

게스트가 ESXi 5.5에서 부팅되지 않는 경우도 있습니다.

VMware ESXi 5.5 하이퍼바이저에서 12GB 이상의 RAM이 있는 Red Hat Enterprise Linux 7 게스트를 실행하는 경우 현재 특정 구성 요소는 잘못된 메모리 유형 레지스터(MTRR) 값으로 초기화하거나 부팅 시 MTRR 값을 잘못 재구성합니다. 이로 인해 부팅 중에 게스트 커널이 패닉 상태이거나 게스트가 응답하지 않는 경우가 있습니다.

이 문제를 해결하려면 게스트의 커널 명령줄에 disable_mtrr_trim 옵션을 추가하여 MTRRs가 잘못 구성된 경우 게스트를 계속 부팅할 수 있습니다. 이 옵션을 사용하면 게스트가 부팅 중에 BIOS 버그 메시지가 표시되고 안전하게 무시할 수 있습니다. (BZ#1429792)

Red Hat Virtualization Hypervisor 프로파일의 RuntimeClass가 Anaconda에 표시되지 않습니다.

oscap-anaconda-addon 모듈은 현재 Red Hat Virtualization Hypervisor 보안 강화 프로파일의 Replicas를 올바르게 구문 분석할 수 없습니다. 결과적으로 프로파일 이름은 Red Hat Enterprise Linux 7 또는 미국 정부 구성 기준선 (USGCB / RuntimeClass) - Anaconda 인터페이스 선택에서 DRAFT 로 표시됩니다. 그러나 이는 디스플레이 문제일 뿐이며 Red Hat Virtualization Hypervisor 프로파일 용 rhcos 대신 Red Hat Enterprise Linux 7 프로파일에 DISAReplicas를 안전하게 사용할 수 있습니다. (BZ#1437106)

부록 A. 구성 요소 버전

이 부록은 **Red Hat Enterprise Linux 7.4** 릴리스의 주요 구성 요소 및 버전 목록을 제공합니다.

표 A.1. 구성 요소 버전

구성 요소	버전
커널	3.10.0-693
Qlogic **qla2xxx** 드라이버	8.07.00.38.07.4-k1
Qlogic **qla4xxx** 드라이버	5.04.00.00.07.02-k0
Emulex **lpfc** 드라이버	0:11.2.0.6
iSCSI 이니시에이터 utils	iscsi-initiator-utils-6.2.0.874-4
DM-Multipath	device-mapper-multipath-0.4.9-111
LVM	lvm2-2.02.171-8

부록 B. 구성 요소별 BUGZILLA 목록

이 부록에서는 이 책에 포함된 모든 구성 요소와 관련 Bugzilla 목록을 제공합니다.

표 B.1. 구성 요소별 Bugzilla 목록

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
389-ds-base	BZ#1394000, BZ#1395940, BZ#1425907	BZ#1378209		
doc-administration-guide	BZ#1426286, BZ#1426289			
doc-release-notes	BZ#1426275, BZ#1426278, BZ#1426283, BZ#1436973			
NetworkManager	BZ#1337997, BZ#1353612, BZ#1373698, BZ#1394344, BZ#1394579, BZ#1398934, BZ#1404594, BZ#1404598, BZ#1414103, BZ#1420708	BZ#1391170, BZ#1393997		
AIDE		BZ#1377215		
anaconda	BZ#663099, BZ#1113207, BZ#1131247, BZ#1255659, BZ#1315160, BZ#1332316, BZ#1366935, BZ#1377233, BZ#1391724, BZ#1412538	BZ#1317370, BZ#1327439, BZ#1356975, BZ#1358778, BZ#1373360, BZ#1380224, BZ#1380277, BZ#1404158, BZ#1412022, BZ#1441337		BZ#1378714
Ansible			BZ#1313263	
audit	BZ#1381601			
authconfig	BZ#1334449, BZ#1378943			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
EgressIP	BZ#1367576, BZ#1382093	BZ#1101782, BZ#1383194, BZ#1383910, BZ#1420574, BZ#1420584, BZ#1320588		
bind	BZ#1388534, BZ#1393886			
bind-dyndb-ldap	BZ#1393889			
binutils	BZ#1366052	BZ#1326710, BZ#1406498		
bison	BZ#1306000			
booth	BZ#1302087			
ca-certificates	BZ#1444414			
chrony	BZ#1387223			
chrpath		BZ#1271380		
Clevis	BZ#1300697			
cloud-init	BZ#1427280			
clufter	BZ#1387424			
crash	BZ#1368711, BZ#1384944, BZ#1393534			
criu			BZ#1400230	
custodia			BZ#1403214	
cyrus-sasl		BZ#1421663		
dbxtool	BZ#1078990			
dconf-editor	BZ#1388931			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
device-mapper-multipath	BZ#1169168, BZ#1279355, BZ#1359510, BZ#1362409, BZ#1368211, BZ#1372032, BZ#1394059, BZ#1406226, BZ#1416569, BZ#1430097	BZ#1239173, BZ#1362120, BZ#1380602, BZ#1402092, BZ#1403552, BZ#1431562		
dhcp	BZ#1374119			
distribution				BZ#1062656
dmidecode	BZ#1385884			
dnsmasq	BZ#1375527, BZ#1375569			
ecj	BZ#1379855			
elfutils	BZ#1400302			
empathy		BZ#1386616		
ethtool	BZ#1402701			
fcoe-utils		BZ#1384707		
firefox				BZ#1455798
firewalld	BZ#1006225, BZ#1409544, BZ#1419058	BZ#1401978		
flatpak				BZ#1476905
freeradius				BZ#1489758
genwqe-tools	BZ#1275663			
gfs2-utils	BZ#1413684			
Ghostscript		BZ#1390847, BZ#1411725, BZ#1424752		

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
Git		BZ#1369173		
glibc	BZ#841653, BZ#1298975, BZ#1320947, BZ#1421155	BZ#1324568, BZ#1326739		
glusterfs				BZ#1409773
gnome-initial-setup		BZ#1226819		
gnome-packagekit				BZ#1387181
gnome-shell	BZ#1383353			
gnome-software				BZ#1434477, BZ#1464139
gnu-efi	BZ#1310782			
gnutls	BZ#1399232			
grep	BZ#1297441			
grub2				BZ#1154226
gstreamer1-plugins-good				BZ#1451211
http-parser	BZ#1393819			
hwdata	BZ#1386133			
initial-setup		BZ#1378082		

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
initscripts	BZ#1260552, BZ#1428935	BZ#1278521, BZ#1367554, BZ#1369790, BZ#1374837, BZ#1385272, BZ#1392766, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ##150, BZ##150, BZ##150, BZ##150, BZ##HIERA, BZ##150, BZ#HIERA, BZ##150139419 1 1398671 1398678 1398679 1398683 1398686 1406254 1408219 1428574143407 5		
intel-cmt-cat	BZ#1315489			
IPA	BZ#872671, BZ#1125174, BZ#1200767, BZ#1366572, BZ#1402959, BZ#1404750, BZ#1409628, BZ#1459153		BZ#1115294, BZ#1298286	BZ#1455946
ipa-server-docker			BZ#1405325	
iperf3	BZ#913329			
ipmitool	BZ#1398658			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
iproute	BZ#1063934, BZ#1422629	BZ#1375215		
iprutils	BZ#1384382			
jansson	BZ#1389805			
java-1.7.0-openjdk	BZ#1373986			
java-1.8.0-openjdk			BZ#1400306	
kernel	BZ#437984, BZ#950243, BZ#1072503, BZ#1138782, BZ#1155732, BZ#1241990, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA1270982 1273401 1297841 1297929 1298643 1299527 1302147 1306396 1306453 1308632 1314179 1326309 1326318 1326353 BZ#1330457,	BZ#1084802, BZ#1213119, BZ#1217546, BZ#1324918, BZ#1351098, BZ#1353218, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#1363661, BZ######HIERA1370638 1379787 1385149 1386923 1387485 1406885 14083301412898	BZ#916382, BZ#947163, BZ#1109348, BZ#1111712, BZ#1206277, BZ#1230959, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ##150, BZ##150, BZ##150, BZ##150, BZ##HIERA, BZ##150, BZ#HIERA, BZ##1501274456 1274459 1299662 1305092 1348508 1349668 1350553 1393375 1414957 1449762 14608491288964	BZ#1377857, BZ#1380447, BZ#1429792, BZ#1431964, BZ#1451242, BZ#1458354

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
	BZ#1339127, BZ#1339791, BZ#1340238, BZ#1346348, BZ#1352289, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA13559 19 1356122 1357491 1365002 1366564 1369158 1373606 1373971 1374498 1377710 1377767 1379590 1382101 1382494 BZ#1382500, BZ#1382504, BZ#1382508, BZ#1382849, BZ#1383280, BZ#1383827, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA,			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
	BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA1383834 1384456 1384648 1385026 1385757 1388467 1388646 1388716 1391219 1391243 1391413 1391668 1394197 1400501 BZ#1401797, BZ#1402102, BZ#1406197, BZ#1416924, BZ#1432218, BZ#1432897, BZ#TEKTON, BZ##13834891626527			
kernel-aarch64				BZ#1218374
kernel-rt	BZ#1391779	BZ#1443711	BZ#1297061	
kexec-tools	BZ#1384945			
keycloak-httpd-client-install	BZ#1401781			
libcgroup		BZ#1406927		
libdb		BZ#1277887		
libfastjson	BZ#1395145			
libguestfs	BZ#1233093, BZ#1359086, BZ#1362649, BZ#1367738, BZ#1400205, BZ#1404182	BZ#1161019, BZ#1265588, BZ#1311890, BZ#1354507, BZ#1374232, BZ#1374405, BZ#1383517, BZ#1392798, BZ#1401474, BZ#1402301, BZ#1431579	BZ#1387213, BZ#1441197	

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
libica	BZ#1391558			
libnfsidmap	BZ#980925			
libnftnl		BZ#1418967	BZ#1332585	
libreoffice				BZ#1466164
libreswan	BZ#1324458, BZ#1399883			
librtas	BZ#1380656			
libseccomp	BZ#1425007			
libstoragemgmt	BZ#1403142		BZ#1119909	
libusnic_verbs			BZ#916384	
libvirt	BZ#1349696, BZ#1382640, BZ#1414627		BZ#1283251	
libwacom	BZ#1342990			BZ#1458351
linuxptp	BZ#1359311			
logrotate	BZ#1381719			
lorax	BZ#1310775, BZ#1430483			BZ#1341280
lshw	BZ#1368704			
lvm2	BZ#1189108, BZ#1191935, BZ#1346280, BZ#1366296, BZ#1378956, BZ#1394048, BZ#1436748, BZ#1442992	BZ#1380521, BZ#1380532, BZ#1382688, BZ#1386184, BZ#1434054		BZ#1014758
mariadb		BZ#1356897		
mdadm	BZ#1380017			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
memkind	BZ#1384549			
mod_nss	BZ#1382102, BZ#1392582			
대해 알아보기	BZ#1388511	BZ#1388512		
DomainMappinger				BZ#1393951
nautilus				BZ#1474852
net-snmp		BZ#1286693, BZ#1324306		
NetCF				BZ#1100588
nfs-utils	BZ#1375259, BZ#1418041			BZ#1450447
nss	BZ#1309781, BZ#1316546, BZ#1444413	BZ#1220573		BZ#1401809
nss-softokn	BZ#1369055			
nvme-cli	BZ#1382119			
nvmetcli	BZ#1383837			
opencryptoki	BZ#1391559			
openldap	BZ#1386365, BZ#1428740			
opensc	BZ#1081088			
openscap	BZ#1363826	BZ#1420038, BZ#1440192, BZ#1447341		
openssh	BZ#1322911, BZ#1341754	BZ#1418062		
OpenSSL	BZ#1276310			
openssl-ibmca	BZ#1274385			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
openvswitch	BZ#1368043, BZ#1390938			
openwsman	BZ#1190689			
OProfile		BZ#1380809		
oscap-anaconda-addon				BZ#1372791, BZ#1437106, BZ#1462647
기타	BZ#1432080, BZ#1444937, BZ#1457907, BZ#1459948, BZ#1467260	BZ#1408694	BZ#1062759, BZ#1072107, BZ#1259547, BZ#1464377, BZ#1467338, BZ#1477977	BZ#1174132, BZ#1458338, BZ#1463600
OVMF			BZ#653382	
pacemaker	BZ#1289662	BZ#1388489		
pcp	BZ#1422263, BZ#1423020			
pcre		BZ#1400267		BZ#1290432
pcs	BZ#1158805, BZ#1165821, BZ#1176018, BZ#1261116, BZ#1303969, BZ#1362493, BZ#1373614, BZ#1413958	BZ#1386114, BZ#1378107	BZ#1433016	
perl-IO-Socket-SSL	BZ#1335035			
perl-Net-SSLeay	BZ#1335028			
perl-Perl4-CoreLibs	BZ#1366724			
perl-local-lib		BZ#1122993		

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
pki-core	BZ#1303683, BZ#1305993, BZ#1325071, BZ#1388622, BZ#1391737, BZ#1392068, BZ#TEKTON, BZ#OCTETS, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ######1409946 1413132 1426754 1445535 1447144 14501431458055	BZ#1238684, BZ#1246635, BZ#1249400, BZ#1282504, BZ#1330800, BZ#1372052, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#TEKTON, BZ#TEKTON, BZ#TEKTON, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA, BZ#HIERA1376226 1376488 1378275 1378277 1381084 1382066 1385208 1386303 1395817 1397200 1400149 14048811411428 1412681 BZ#1413136, BZ#1445088, BZ#1446364, BZ#1447762, BZ#1452250, BZ#1452344, BZ#HIERA, BZ##1454450 14544711458429		BZ#1256901
procps-ng		BZ#1373246		
psacct	BZ#1255183			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
pykickstart				BZ#1452770
python	BZ#1219110			
python-blivet		BZ#1214407, BZ#1327463		
python-tornado	BZ#1158617			
qemu-kvm			BZ#1103193	
rdma-core	BZ#1404035			
Rear	BZ#1355667	BZ#1343119		
resource-agents	BZ#1077888, BZ#1336847, BZ#1430304			
rhino	BZ#1350331			
rhnsd				BZ#1480306
rpm		BZ#1378307	BZ#1278924	
rsyslog	BZ#1313490, BZ#1431616			
ruby	BZ#1397390	BZ#1308992		
rubygem-abrt	BZ#1418750			
samba	BZ#1391954			
sapconf		BZ#1391881		
sbd	BZ#1413951			
sblim-cmpi-fsvol		BZ#1136116		
scap-security-guide	BZ#1404392, BZ#1410914	BZ#1450731		BZ#1448952, BZ#1464899, BZ#1465677
해비아		BZ#1020622		

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
selinux-policy		BZ#1368057, BZ#1386916		BZ#1365944
sendmail	BZ#1124827			
sg3_utils		BZ#1380744		
shim	BZ#1310766			
shim-signed	BZ#1310764			
sos	BZ#1414879			
sssd	BZ#1214491, BZ#1311056, BZ#1330196, BZ#1340711, BZ#1396012, BZ#1414023, BZ#1425891		BZ#1068725	BZ#1446101, BZ#1447945, BZ#1448094, BZ#1460689, BZ#1462769
strace		BZ#1377847		
strongimcv			BZ#755087	
sudo				BZ#1293306
system-config-language		BZ#1304223		
systemd		BZ#1353028	BZ#1284974	
systemtap	BZ#1398393			
tar	BZ#1350640	BZ#1184697, BZ#1319820, BZ#1341786		
targetcli	BZ#1243410			
targetd	BZ#1162381			
tboot	BZ#1384210			
tcpdump	BZ#1292056, BZ#1422473			

구성 요소	새로운 기능	주요 버그 수정	기술 프리뷰	알려진 문제
tcsh		BZ#1388426		
텔넷	BZ#1367415			
tpm2-tss	BZ#1275027			
tss2	BZ#1384452			
tuned	BZ#1388454, BZ#1414098			
unbound	BZ#1382383			
usbguard	BZ#1395615		BZ#1467369	
valgrind	BZ#1391217			
virt-who	BZ#1299643, BZ#1369107, BZ#1405967, BZ#1426058, BZ#1436811			
wget	BZ#1439811			
wpa_supplicaant	BZ#1404793			
xorg-x11-drv-libinput	BZ#1413811			
xorg-x11-drv-qxl				BZ#1428340
xorg-x11-server	BZ#1404868			BZ#1185690
elp				BZ#1443179
YP-tools		BZ#1401432		
ypbind		BZ#1217435, BZ#1382804		
yum	BZ#1343690	BZ#1352585, BZ#1370134		
yum-utils		BZ#1406891		

부록 C. 개정 내역

고침 0.5-0 Wed Feb 12 2020 Jaroslav Klech
아키텍처 및 새로운 기능에 대한 전체 커널 버전이 제공됩니다.

고침 0.4-9 Mon Oct 07 2019 Jiří Herrmann
OVMF와 관련된 기술 프리뷰 노트를 명확히 합니다.

고침 0.4-8 Mon May 13 2019 Lenka Špačková
freeradius upgrade (Networking)와 관련된 알려진 문제가 추가되었습니다.

고침 0.4-7 Sun Apr 28 2019 Lenka Špačková
기술 프리뷰 기능 설명(File Systems)의 개선된 용어입니다.

고침 0.4-6 Mon Feb 04 2019 Lenka Špačková
더 나은 책의 구조

고침 0.4-5 Thu Sep 13 2018 Lenka Špačková
CephFS 를 기술 프리뷰에서 완전히 지원되는 기능(File Systems)으로 이동.

고침 0.4-4 Tue Apr 17 2018 Lenka Špačková
sslwrap() 사용 중단과 관련된 권장 사항을 업데이트했습니다.

고침 0.4-3 Tue Apr 10 2018 Lenka Špačková
rsyslog **imudp** 모듈의 **inputname** 옵션과 관련된 사용 중단 노트가 추가되었습니다.

고침 0.4-2 Thu Apr 05 2018 Lenka Špačková
CAT를 기술 프리뷰(Kernel)로 이동.

고침 0.4-1 Thu Mar 22 2018 Lenka Špačková
openldap-servers 패키지 이름(더 이상 사용되지 않는 기능)을 수정했습니다.

고침 0.4-0 Fri Mar 16 2018 Lenka Špačková
pcs-related 버그 수정(클러스터링)이 추가되었습니다.

고침 0.3-9 Mon Feb 19 2018 Mirek Jahoda
TPM 관련 기능이 Technnology Preview 섹션으로 잘못 배치되었습니다.

고침 0.3-8 Tue Feb 06 2018 Lenka Špačková
누락된 기술 프리뷰 - OVMF(가상화)가 추가되었습니다.
libvirt-lxc 툴링을 사용하여 컨테이너 사용 중단에 대한 정보가 추가되었습니다.

고침 0.3-7 Wed Jan 17 2018 Lenka Špačková
FCoE 사용 중단 알림을 업데이트했습니다.

고침 0.3-6 Wed Jan 10 2018 Lenka Špačková
NVDIMM 장치의 장치 DAX 상태를 기술 프리뷰에서 완전히 지원되는 (Storage)로 변경했습니다.

고침 0.3-5 Thu Dec 14 2017 Lenka Špačková
더 이상 사용되지 않는 드라이버의 구조를 통합합니다.

고침 0.3-4 Tue Dec 12 2017 Lenka Špačková

qla2xxx 드라이버에서 더 이상 사용되지 않는 어댑터를 업데이트했습니다.

고침 0.3-3 Wed Nov 22 2017 Lenka Špačková
pam_krb5 에서 sssd 마이그레이션(더 이상 사용되지 않는 기능)에 대한 추가 정보.

고침 0.3-2 Wed Nov 15 2017 Lenka Špačková
오타를 수정했습니다.

고침 0.3-1 Tue Oct 31 2017 Lenka Špačková
LVM 관련 버그 수정 설명(Storage)을 추가했습니다.

고침 0.3-3 Mon Oct 30 2017 Lenka Špačková
EgressIP 버그 **수정** 설명 (File Systems)을 추가했습니다.
더 이상 사용되지 않는 기능에 대한 **ld** 링커 동작의 변경 사항에 대한 정보가 추가되었습니다.

고침 0.3-2 Wed Sep 13 2017 Lenka Špačková
Xorg 서버의 시각적 개체에 대한 제한된 지원에 대한 정보가 추가되었습니다.

고침 0.3-1 Mon Sep 11 2017 Lenka Špačková
기술 프리뷰(커널)에 CUIR의 범위 탐지 기능이 추가되었습니다.
새 기능(보안)의 업데이트 openssh 재베이스 설명.

고침 0.3-0 Mon Sep 04 2017 Lenka Špačková
알려진 두 가지 문제(보안 데스크탑)를 추가했습니다.

고침 0.2-9 Mon Aug 21 2017 Lenka Špačková
더 이상 사용되지 않는 기능에 tcp_wrappers 를 추가했습니다.

고침 0.2-8 Tue Aug 15 2017 Lenka Špačková
몇 가지 새로운 기능과 알려진 문제가 추가되었습니다.

고침 0.2-7 Mon Aug 14 2017 Lenka Špačková
중복 노트 삭제

고침 0.2-6 Thu Aug 10 2017 Lenka Špačková
몇 가지 알려진 문제가 업데이트되었습니다.

고침 0.2-5 Tue Aug 08 2017 Lenka Špačková
알려진 두 가지 문제가 추가되었습니다.

고침 0.2-4 Mon Aug 07 2017 Lenka Špačková
FCoE 사용 중단 알림이 업데이트되었습니다.
마이너 업데이트 및 추가

고침 0.2-3 Fri Aug 04 2017 Lenka Špačková
가상화에서 시스템 및 서브스크립션 관리로 몇 가지 새로운 기능을 도입했습니다.

고침 0.2-2 Thu Aug 03 2017 Lenka Špačková
RuntimeClass에 대한 **업데이트된** 정보; 이제 기술 프리뷰 및 더 이상 사용되지 않는 기능성에 있습니다.
마이너 업데이트 및 추가

고침 0.2-1 Tue Aug 01 2017 Lenka Špačková
Red Hat Enterprise Linux 7.4 릴리스 노트.

고침 0.0-4 Tue May 23 2017 Lenka Špačková
Red Hat Enterprise Linux 7.4 베타 릴리스 노트.