



Red Hat Enterprise Linux 9

RHEL 8에서 RHEL 9로 업그레이드

Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로의 인플레이스 업그레이드 방법

Red Hat Enterprise Linux 9 RHEL 8에서 RHEL 9로 업그레이드

Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로의 인플레이스 업그레이드 방법

Enter your first name here. Enter your surname here.

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

Enter your email address here.

법적 공지

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Upgrading_from_RHEL_8_to_RHEL_9.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution-Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

초록

이 문서에서는 Leapp 유틸리티를 사용하여 Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 인플레이스 업그레이드를 수행하는 방법에 대한 지침을 제공합니다. 즉각적 업그레이드 중에 기존 RHEL 8 운영 체제는 RHEL 9 버전으로 교체됩니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체	3
RED HAT 문서에 관한 피드백 제공	4
키 마이그레이션 용어	5
1장. 지원되는 업그레이드 경로	6
2장. 업그레이드 계획	7
3장. 업그레이드 준비	9
3.1. 업그레이드를 위한 RHEL 8 시스템 준비	9
3.2. 업그레이드를 위한 SATELLITE 시스템 준비	12
4장. 사전 업그레이드 보고서 검토	14
4.1. 명령줄에서 UPGRADABILITY 평가	14
4.2. 웹 콘솔을 통해 UPGRADABILITY 평가 및 자동 수정 적용	15
5장. RHEL 8에서 RHEL 9로 업그레이드 수행	20
6장. RHEL 9 시스템의 업그레이드 후 상태 확인	22
7장. 업그레이드 후 작업 수행	23
8장. 보안 정책 적용	24
8.1. SELINUX 모드를 강제 모드로 변경	24
8.2. 시스템 전체 암호화 정책	25
8.3. 보안 기준으로 강화된 시스템 업그레이드	26
8.4. USBGUARD 정책 확인	27
8.5. FAPOLICYD 데이터베이스 업데이트	28
8.6. DBM에서 SQLITE로 NSS 데이터베이스 업데이트	28
8.7. BERKELEY DB 형식에서 GDBM으로 CYRUS SASL 데이터베이스 마이그레이션	29
9장. 문제 해결	31
9.1. 리소스 문제 해결	31
9.2. 문제 해결 팁	31
9.3. 확인된 문제	33
9.4. 지원 받기	35
10장. 관련 정보	36
부록 A. RHEL 8 리포지토리	37
부록 B. RHEL 9 리포지토리	39

보다 포괄적 수용을 위한 오픈 소스 용어 교체

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

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. Red Hat이 어떻게 이를 개선할 수 있는지 알려 주십시오.

- 특정 문구에 대한 간단한 의견 작성 방법은 다음과 같습니다.
 1. 문서가 *Multi-page HTML* 형식으로 표시되는지 확인합니다. 또한 문서 오른쪽 상단에 **피드백** 버튼이 있는지 확인합니다.
 2. 마우스 커서를 사용하여 주석 처리하려는 텍스트 부분을 강조 표시합니다.
 3. 강조 표시된 텍스트 아래에 표시되는 **피드백 추가** 팝업을 클릭합니다.
 4. 표시된 지침을 따릅니다.
- Bugzilla를 통해 피드백을 제출하려면 새 티켓을 생성합니다.
 1. [Bugzilla](#) 웹 사이트로 이동합니다.
 2. 구성 요소로 **문서**를 사용합니다.
 3. **설명** 필드에 문서 개선을 위한 제안 사항을 기입하십시오. 관련된 문서의 해당 부분 링크를 알려주십시오.
 4. **버그 제출**을 클릭합니다.

키 마이그레이션 용어

소프트웨어 업계에서 일반적으로 사용되는 마이그레이션 조건은 다음과 같습니다. 이러한 정의는 RHEL(Red Hat Enterprise Linux)에만 적용됩니다.

update

경우에 따라 소프트웨어 패치라고 하는 업데이트는 현재 버전의 애플리케이션, 운영 체제 또는 실행 중인 소프트웨어에 추가됩니다. 소프트웨어 업데이트는 기술 사용 경험을 개선하기 위해 모든 문제 또는 버그를 해결합니다. RHEL에서 업데이트는 마이너 릴리스(예: RHEL 8.1에서 8.2로 업데이트)와 관련이 있습니다.

업그레이드

업그레이드는 현재 실행 중인 애플리케이션, 운영 체제 또는 소프트웨어를 최신 버전으로 교체할 때입니다. 일반적으로 Red Hat의 지침에 따라 데이터를 백업하십시오. RHEL을 업그레이드할 때 다음 두 가지 옵션이 있습니다.

- **즉각적 업그레이드:** 즉각적 업그레이드 중에 이전 버전을 먼저 제거하지 않고 이전 버전을 새 버전으로 교체합니다. 설치된 애플리케이션 및 유틸리티는 구성 및 기본 설정과 함께 새 버전에 통합되어 있습니다.
- **정리 설치:** 새로 설치한 설치로 이전에 설치한 운영 체제, 시스템 데이터, 구성 및 애플리케이션의 모든 추적을 제거하고 최신 버전의 운영 체제를 설치합니다. 새로 설치하는 것은 시스템에 이전 데이터 또는 애플리케이션이 필요하지 않거나 이전 빌드에 의존하지 않는 새 프로젝트를 개발하는 경우 이상적입니다.

운영 체제 변환

전환은 운영 체제를 다른 Linux 배포판에서 Red Hat Enterprise Linux로 변환하는 경우입니다. 일반적으로 Red Hat의 지침에 따라 데이터를 백업하십시오.

Migration

일반적으로 마이그레이션은 플랫폼(소프트웨어 또는 하드웨어)의 변경을 나타냅니다. Windows에서 Linux로 마이그레이션하는 것은 마이그레이션입니다. 한 컴퓨터에서 다른 노트북으로 또는 한 서버에서 다른 서버로 사용자를 이동하는 것은 마이그레이션입니다. 그러나 대부분의 마이그레이션에는 업그레이드도 포함되므로 용어가 서로 바뀌 사용할 수 있습니다.

- **RHEL로 마이그레이션:** 기존 운영 체제를 RHEL로 변환
- **RHEL에서 마이그레이션:** RHEL의 한 버전에서 다른 버전으로 업그레이드

1장. 지원되는 업그레이드 경로

인플레이스 업그레이드는 시스템의 RHEL 8 운영 체제를 RHEL 9 버전으로 대체합니다.



중요

RHEL 7에서 RHEL 9로 직접 인플레이스 업그레이드를 수행할 수 없습니다. 그러나 RHEL 7에서 RHEL 8로 내부 업그레이드를 수행한 다음 두 번째 즉각적 업그레이드를 RHEL 9로 업그레이드할 수 있습니다. 자세한 내용은 [RHEL 7에서 RHEL 8로](#)의 업그레이드를 참조하십시오.

현재 다음 소스 RHEL 8 마이너 버전에서 다음 대상 RHEL 9 마이너 버전으로 인플레이스 업그레이드를 수행할 수 있습니다.

표 1.1. 지원되는 업그레이드 경로

제품 변형	소스 OS 버전	대상 OS 버전
RHEL	RHEL 8.6	RHEL 9.0

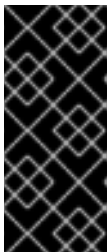
지원되는 업그레이드 경로에 대한 자세한 내용은 [Red Hat Enterprise Linux에 대한 내부 업그레이드 경로를](#) 참조하십시오.

2장. 업그레이드 계획

시스템을 다음 주요 RHEL 버전으로 업그레이드하는 것이 권장되고 지원되는 업그레이드 방법입니다.

RHEL 9로 업그레이드하기 전에 다음을 고려해야 합니다.

- **운영 체제** - 다음과 같은 조건에서 **Leapp** 유틸리티에 의해 운영 체제를 업그레이드 할 수 있습니다.
 - 소스 OS 버전은 다음 지원 아키텍처 중 하나가 있는 시스템에 설치됩니다.
 - 64비트 Intel, AMD 및 ARM
 - IBM POWER (little endian)
 - 64-bit IBM Z
 자세한 내용은 [Red Hat 인증 하드웨어](#) 를 참조하십시오.
 - RHEL 9의 최소 [하드웨어 요구 사항](#) 충족
 - 최신 RHEL 8.6 및 RHEL 9.0 콘텐츠가 제공됩니다. 자세한 내용은 [RHEL 8 시스템 업그레이드를 위한 RHEL 8 시스템 준비](#)를 참조하십시오.
- **애플리케이션** - **Leapp** 을 사용하여 시스템에 설치된 애플리케이션을 마이그레이션할 수 있습니다. 그러나 특정 경우에는 업그레이드 중에 **Leapp** 에서 수행할 작업을 지정하는 사용자 지정 행위자를 생성해야 합니다(예: 애플리케이션 재구성 또는 특정 하드웨어 드라이버 설치). 자세한 내용은 [사용자 지정 및 타사 애플리케이션 마이그레이션](#) 처리를 참조하십시오. 사용자 지정 행위자는 Red Hat에서 지원하지 않습니다.



중요

SHA1 은 RHEL 9에서 더 이상 사용되지 않습니다. 시스템에 **RSA/SHA1** 서명이 있는 패키지가 포함된 경우 업그레이드가 차단됩니다. 업그레이드하기 전에 이러한 패키지를 제거하거나 **RSA/SHA256** 서명이 있는 패키지의 공급 업체에 문의하십시오. 자세한 내용은 [Red Hat Enterprise Linux 9의 SHA-1 사용 중단](#)을 참조하십시오.

- **보안** - 업그레이드하기 전에 이 측면을 평가하고 업그레이드 프로세스가 완료될 때 추가 단계를 수행해야 합니다. 특히 다음을 고려하십시오.
 - 업그레이드하기 전에 시스템이 준수해야 하는 보안 표준을 정의하고 [RHEL 9의 보안 변경 사항](#)을 이해해야 합니다.
 - 업그레이드 프로세스 중에 **Leapp** 유틸리티는 SELinux 모드를 허용으로 설정합니다.
 - FIPS 모드에서 시스템 내부 업그레이드는 지원되지 않습니다.
 - 업그레이드가 완료되면 보안 정책을 다시 평가하고 다시 적용합니다. 보안 정책 적용 및 업데이트에 대한 자세한 내용은 [보안 정책 적용](#)을 참조하십시오.
- **스토리지 및 파일 시스템** - 업그레이드하기 전에 항상 시스템을 백업해야 합니다. 예를 들어 [Relax-and-Recover\(ReaR\)](#) 유틸리티, [LVM 스냅샷](#), [RAID 분할](#) 또는 가상 시스템 스냅샷을 사용할 수 있습니다.
- **고가용성** - **고가용성 애드온** 을 사용한 시스템 업그레이드는 지원되지 않습니다.

- **다운타임** - 업그레이드 프로세스는 몇 분에서 몇 시간까지 걸릴 수 있습니다.
- **Satellite** - Satellite를 통해 호스트를 관리하는 경우 Satellite 웹 UI를 사용하여 RHEL 8에서 RHEL 9으로 여러 호스트를 동시에 업그레이드할 수 있습니다. 자세한 내용은 [RHEL 7에서 RHEL 8로 호스트 업그레이드를 참조하십시오](#).
- **퍼블릭 클라우드** - 인플레이스 업그레이드는 [Red Hat Update Infrastructure\(RHUI\)](#) 를 사용한 AWS(Amazon Web Services)에서 온 디맨드 Pay-As-you-Go(PAYG) 인스턴스에 대해 지원됩니다. AWS 인스턴스와 함께 RHUI를 사용하려면 Red Hat에서 인증된 공식 RHEL High Availability Amazon Machine Image(AMI)가 있어야 합니다. RHEL 서브스크립션의 경우 RHSM을 사용하는 모든 퍼블릭 클라우드에서 Own Subscription 인스턴스 Bring Your Own Subscription 인스턴스도 지원됩니다.
- **언어** - 모든 **Leapp** 보고서, 로그 및 기타 생성된 문서는 언어 구성에 관계없이 영어로 제공됩니다.
- **부트로더** - 부트로더를 RHEL 8 또는 RHEL 9의 UEFI로 전환할 수 없습니다. RHEL 8 시스템에서 BIOS를 사용하고 RHEL 9 시스템이 UEFI를 사용하려면 즉각적 업그레이드 대신 RHEL 9의 새로운 설치를 수행합니다. 자세한 내용은 [BIOS 부팅을 사전 설치된 Red Hat Enterprise Linux 시스템에서 UEFI 부팅으로 전환할 수 있습니까?](#)
- **알려진 제한 사항** - **Leapp**의 알려진 제한 사항은 다음과 같습니다.
 - 전체 디스크 또는 파티션 또는 파일 시스템 암호화의 암호화는 현재 인플레이스 업그레이드를 대상으로 하는 시스템에서 사용할 수 없습니다.
 - 네트워크 기반 다중 경로가 없으며 일종의 네트워크 스토리지 마운트를 시스템 파티션(예: iSCSI 또는 NFS)으로 사용할 수 없습니다.
 - 현재 나머지 퍼블릭 클라우드에서 온 디맨드 PAYG 인스턴스에 대한 인플레이스 업그레이드는 Red Hat Update Infrastructure를 사용하지만 RHEL 서브스크립션 관리자(RHSM)가 아닌 나머지 퍼블릭 클라우드(Microsoft Azure, Huawei Cloud, Alibaba Cloud, Google Cloud) 인스턴스에 대해 지원되지 않습니다.

알려진 문제 ([Known Issues](#))를 참조하십시오.

[Red Hat Insights](#)를 사용하여 Insights에 등록된 시스템 중 RHEL 9에 대한 업그레이드 경로에 있는 시스템을 확인할 수 있습니다. 이렇게 하려면 Insights의 각 [권고 권고](#) 사항으로 이동하여 작업 드롭다운 메뉴에서 권장 사항을 활성화하고 *Affected systems heading* 아래의 목록을 검사합니다. Advisor 권장 사항은 RHEL 8 마이너 버전만 고려하고 시스템의 사전 업그레이드 평가를 수행하지 않는 것이 좋습니다. [Advisor Service Recommendations](#)도 참조하십시오.

3장. 업그레이드 준비

업그레이드 후 문제를 방지하고 시스템을 RHEL의 다음 주요 버전으로 업그레이드하려면 업그레이드하기 전에 필요한 모든 준비 단계를 완료합니다.

모든 시스템의 [업그레이드를 위해 RHEL 8 시스템 준비에 설명된 준비](#) 단계를 수행해야 합니다. 또한 Satellite Server에 등록된 시스템에서 [업그레이드를 위한 Satellite 시스템 준비에 설명된 준비](#) 단계를 수행해야 합니다.

3.1. 업그레이드를 위한 RHEL 8 시스템 준비

이 절차에서는 **Leapp** 유틸리티를 사용하여 RHEL 9으로 인플레이스 업그레이드를 수행하기 전에 필요한 단계를 설명합니다.

업그레이드 프로세스 중에 Red Hat Subscription Manager(RHSM)를 사용하지 않으려면 [Red Hat Subscription Manager 없이 RHEL 9 업그레이드 지침](#)을 따르십시오.

사전 요구 사항

- 시스템은 [업그레이드 플래닝](#)에 나열된 조건을 충족합니다.

절차

1. 이전에 RHEL 7에서 RHEL 8로 인플레이스 업그레이드를 수행한 경우 시스템에 있는 경우 `/root/tmp_leapp_py3` 디렉토리를 제거하십시오.

```
# rm -rf /root/tmp_leapp_py3
```



중요

업그레이드를 수행할 때 `/root/tmp_leapp_py3` 디렉터리가 시스템에 있는 경우 업그레이드 후 시스템이 중단될 수 있습니다.

2. Red Hat Subscription Manager를 사용하여 시스템이 CDN(Red Hat Content Delivery Network) 또는 Red Hat Satellite에 성공적으로 등록되어 있는지 확인합니다.
3. 시스템이 Satellite Server에 등록된 경우 업그레이드할 [Satellite 시스템 준비 단계를 완료하여 시스템이 업그레이드](#) 요구 사항을 충족하는지 확인합니다.
4. [Red Hat Enterprise Linux Server 서브스크립션](#)이 연결되어 있는지 확인합니다. 예를 들어 다음과 같습니다.

```
# subscription-manager list --installed
+-----+
| Installed Product Status |
+-----+
| Product Name:  Red Hat Enterprise Linux x86_64 |
| Product ID:    479 |
| Version:       8.6 |
| Arch:          x86_64 |
| Status:        Subscribed |
```

5. 적절한 리포지토리가 활성화되어 있는지 확인합니다. 다음 명령은 64비트 Intel 아키텍처에 대한 기본 및 Appstream 리포지토리를 활성화합니다. 다른 아키텍처의 경우 [RHEL 8 리포지토리를 참조](#)하십시오.

```
# subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms --enable rhel-8-for-x86_64-appstream-rpms
```



참고

CodeReady Linux Builder 또는 Supplementary 리포지토리가 활성화되어 있습니다. [RHEL 8 리포지토리](#)의 목록을 참조하십시오. 이러한 경우 **Leapp**은 RHEL 8 CodeReady Linux Builder 또는 RHEL 8 보조 리포지토리를 각각 활성화합니다. 자세한 내용은 [패키지 매니페스트](#)를 참조하십시오.

6. RHSM을 사용하여 서브스크립션하는 시스템의 경우 시스템을 RHEL 8.6으로 잠급니다.

```
# subscription-manager release --set 8.6
```

7. 선택 사항: 사용자 지정 리포지토리를 사용하려면 사용자 정의 리포지토리 [구성](#)의 지침에 따라 구성합니다.
8. **dnf versionlock** 플러그인을 사용하여 패키지를 특정 버전으로 잠그면 다음을 실행하여 잠금을 지웁니다.

```
# dnf versionlock clear
```

자세한 내용은 [How to restrict dnf to install or upgrade a package to a fixed specific package version?](#)에서 참조하십시오.

9. AWS에서 RHUI(Red Hat Update Infrastructure)를 사용하여 업그레이드하는 경우 필수 RHUI 리포지토리를 활성화하고 필수 RHUI 패키지를 설치하여 시스템이 업그레이드할 준비가 되었는지 확인합니다.

```
# dnf config-manager --set-enabled rhui-client-config-server-8
# dnf -y install rh-amazon-rhui-client-ha leapp-rhui-aws
```

10. 모든 패키지를 최신 RHEL 8 버전으로 업데이트합니다.

```
# dnf update
```

11. 시스템을 재부팅합니다.

```
# reboot
```

12. **Leapp** 유틸리티를 설치합니다.

```
# dnf install leapp-upgrade
```

현재 you have that you need version 0.14.0 이상 of the shaping **p** package and version 0.16.0 or later of the shaping **p-repository** package, which contains the behind **p-upgrade-el8toel9** RPM 패키지.



참고

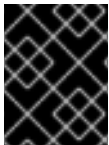
시스템에 인터넷에 액세스할 수 없는 경우 Red Hat [고객 포털](#)에서 Preupgrade Assistant 및 Red Hat Upgrade Tool을 다운로드할 수 있습니다.

13. RPM 패키지 변경 사항, RPM 리포지토리 매핑, 지원되지 않는 드라이버 및 장치를 포함하여 추가 필수 데이터 파일의 최신 버전에 액세스할 수 있는지 확인하십시오.
 - a. 업그레이드에 RHSM을 사용하는 경우 시스템에 cloud.redhat.com에 액세스할 수 있으며, 필요한 데이터 파일의 이전 버전을 다운로드하지 않았으며 추가 작업이 필요하지 않습니다. 데이터 파일은 cloud.redhat.com에서 자동으로 다운로드됩니다. 이는 개발자 서브스크립션에도 적용됩니다.
 - b. 지식 베이스 문서 [Leapp 유틸리티 메타데이터에서 연결이 끊긴 업그레이드를 위해 RHEL의 전체 업그레이드에 연결된 데이터 파일을 다운로드하여 /etc/leapp/files/ 디렉터리에 배치합니다](#). 현재 [yunp-data17.tar.gz](#) 아카이브의 데이터 파일이 필요합니다. 이는 다음과 같은 시나리오에서 업그레이드에 필요합니다.
 - i. RHUI를 사용하여 퍼블릭 클라우드에서 업그레이드 중입니다. Red Hat 서브스크립션 또는 Red Hat 고객 포털 계정이 없는 경우 지식 베이스 문서에 액세스하고 필요한 데이터 패키지를 다운로드할 수 있도록 무료 RHEL 개발자 서브스크립션을 생성하십시오. 자세한 내용은 [How do I get a no-cost Red Hat Enterprise Linux Developer Subscription or renew it?](#)
 - ii. 시스템이 인터넷에 액세스할 수 없습니다.
 - iii. 업그레이드에 RHSM을 사용하고 있으며 이전에 필요한 데이터 파일의 이전 버전을 다운로드했지만 업그레이드를 수행하지 않았습니다(예: 자동화된 스크립트를 생성하기 위해). 이전 버전의 데이터 파일을 삭제하여 최신 파일 버전의 자동 다운로드를 시작할 수도 있습니다.
14. 안티바이러스 소프트웨어를 일시적으로 비활성화하여 업그레이드가 실패하지 않도록 합니다.
15. 구성 관리 시스템이 인플레이스 업그레이드 프로세스를 방해하지 않도록 합니다.
 - Puppet, Salt 또는 Chef 와 같은 클라이언트-서버 아키텍처와 함께 구성 관리 시스템을 사용하는 경우 `yunp preupgrade` 명령을 실행하기 전에 시스템을 비활성화합니다. 업그레이드 중 문제가 발생하지 않도록 업그레이드가 완료될 때까지 구성 관리 시스템을 활성화하지 마십시오.
 - Ansible 과 같은 에이전트 없는 아키텍처가 포함된 구성 관리 시스템을 사용하는 경우 [RHEL 8에서 RHEL 9로의 업그레이드를 수행하는 데](#) 설명된 대로 인플레이스 업그레이드 중에 Ansible 플레이북과 같은 구성 및 배포 파일을 실행하지 마십시오. 구성 관리 시스템을 사용한 사전 업그레이드 및 업그레이드 프로세스의 자동화는 Red Hat에서 지원되지 않습니다. 자세한 내용은 [Using configuration management systems to automate parts of the Leapp pre-upgrade and upgrade process on Red Hat Enterprise Linux](#) 를 참조하십시오.
16. 시스템이 커널(`eth`)에서 사용하는 접두사를 기반으로 이름에 두 개 이상의 NIC(네트워크 인터페이스 카드)를 사용하지 않는지 확인합니다. RHEL 9로 바로 업그레이드하기 전에 다른 명명 스키마로 마이그레이션하는 방법에 대한 자세한 내용은 [RHEL 7에서 커널 NIC 이름을 사용할 때 RHEL 8으로의 내부 업그레이드를 수행하는 방법](#)을 참조하십시오. 이름 지정 체계를 마이그레이션하는 프로세스는 RHEL 7에서 RHEL 8으로 업그레이드하고 RHEL 8에서 RHEL 9 업그레이드 모두에 적용됩니다.

17. NSS 데이터베이스가 RHEL 7 이하에서 생성된 경우 데이터베이스가 DBM 데이터베이스 형식에서 SQLite로 변환되었는지 확인합니다. 자세한 내용은 [DBM에서 SQLite으로 NSS 데이터베이스 업데이트](#)를 참조하십시오.
18. RHEL 9는 RHEL 8에서 더 이상 사용되지 않는 레거시 **network-scripts** 패키지를 지원하지 않습니다. 업그레이드하기 전에 사용자 지정 네트워크 스크립트를 이동하고 기존 사용자 지정 스크립트를 실행하는 NetworkManager 디스패치 스크립트를 작성합니다. 자세한 내용은 [사용자 지정 네트워크 스크립트를 NetworkManager 디스패치 스크립트로 마이그레이션](#)을 참조하십시오.
19. 전체 시스템 백업 또는 가상 머신 스냅샷이 있는지 확인하십시오. 환경 내에서 표준 재해 복구 절차를 따르는 경우 시스템을 pre-upgrade 상태로 만들 수 있습니다. 예를 들어 Relax-and-Recover(ReaR) 유틸리티를 사용할 수 있습니다. 자세한 내용은 [ReaR 문서](#) 및 [What is Relax and Recover \(ReaR\)](#)를 참조하며 [재해 복구에 어떻게 사용할 수 있습니까?](#) 또는 [LVM 스냅샷](#), 또는 [RAID 분할](#)을 사용할 수 있습니다. 가상 머신을 업그레이드하는 경우 전체 VM의 스냅샷을 생성할 수 있습니다.

3.2. 업그레이드를 위한 SATELLITE 시스템 준비

이 절차에서는 RHEL 9으로 업그레이드하기 위해 Satellite에 등록된 시스템을 준비하는 데 필요한 단계를 설명합니다. Satellite 서버에서 수행되는 단계가 있습니다.



중요

Satellite 시스템의 사용자는 이 절차와 [업그레이드를 위한 RHEL 8 시스템 준비](#)에서 설명한 준비 단계를 완료해야 합니다.

사전 요구 사항

- Satellite Server에 대한 관리 권한이 있습니다.

절차

1. Satellite가 전체 버전 또는 유지 관리 지원에 있는지 확인합니다. 자세한 내용은 [Red Hat Satellite 제품 라이프 사이클](#)을 참조하십시오.
2. RHEL 9 리포지토리가 포함된 서브스크립션 매니페스트를 Satellite Server로 가져옵니다. 자세한 내용은 콘텐츠 관리 가이드의 [Red Hat Satellite](#) 특정 버전에 대한 서브스크립션 관리 장(예: [버전 6.10](#))을 참조하십시오.
3. 필요한 모든 RHEL 8 및 RHEL 9 리포지토리를 RHEL 8.6 및 RHEL 9.0의 최신 업데이트와 함께 활성화하고 동기화합니다.



참고

RHEL 9 리포지토리의 경우 각 리포지토리의 버전 9.0을 활성화해야 합니다. 리포지토리의 RHEL 9 버전만 활성화한 경우 인플레이스 업그레이드가 억제되어 있습니다.

예를 들어 EUS (Extended Update Support) 서브스크립션이 없는 Intel 아키텍처의 경우 다음 리포지토리를 최소한으로 활성화하십시오.

- Red Hat Enterprise Linux 8 for x86_64 - AppStream(RPM)
rhel-8-for-x86_64-appstream-rpms

x86_64 8 or 8.6

- Red Hat Enterprise Linux 8 for x86_64 - BaseOS(RPM)
rhel-8-for-x86_64-baseos-rpms

x86_64 8 or 8.6
- Red Hat Enterprise Linux 9 for x86_64 - AppStream(RPM)
rhel-9-for-x86_64-appstream-rpms

x86_64 9.0
- Red Hat Enterprise Linux 9 for x86_64 - BaseOS(RPM)
rhel-9-for-x86_64-baseos-rpms

x86_64 9.0

다른 아키텍처의 경우 [RHEL 8 리포지토리](#) 및 [RHEL 9 리포지토리](#)를 참조하십시오.

자세한 내용은 [콘텐츠 관리 가이드](#)에서 [Red Hat Satellite](#)의 특정 버전에 대한 콘텐츠 가져오기 장(예: [버전 6.10](#))을 참조하십시오.

4. 필요한 RHEL 8 및 RHEL 9 리포지토리가 포함된 콘텐츠 뷰에 콘텐츠 호스트를 연결합니다.
자세한 내용은 [Red Hat Satellite](#)의 특정 버전에 대한 [콘텐츠 관리 가이드](#)의 콘텐츠 뷰 관리 장(예: [버전 6.10](#))을 참조하십시오.

검증

- 최신 RHEL 8 리포지토리가 Satellite Server에서 활성화되었는지 확인합니다. 예를 들어 Library 라이프사이클 환경에서 리포지토리를 확인하려면 다음을 실행합니다.

```
# hammer repository list --search 'content_label ~ rhel-9' --content-view
<content_view_name> --organization <organization> --lifecycle-environment Library
```

`content_view_name` 을 콘텐츠 뷰의 이름으로, `조직`을 `조직`으로 교체합니다.

4장. 사전 업그레이드 보고서 검토

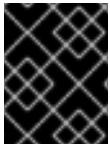
시스템의 업그레이드 가능성을 평가하려면 **yunp preupgrade** 명령을 사용하여 **pre-upgrade** 프로세스를 시작합니다. 이 단계에서 **Leapp** 유틸리티는 시스템에 대한 데이터를 수집하고 upgradability를 평가하고 사전 업그레이드 보고서를 생성합니다.

pre-upgrade 보고서는 **/var/log/leapp/leapp-report.txt** 파일과 웹 콘솔에서 모두 사용할 수 있습니다. 이 보고서는 잠재적인 문제를 요약하고 권장 솔루션을 제안합니다. 이 보고서는 또한 업그레이드를 진행할 수 있는지 여부를 결정하는 데 도움이 됩니다.

특정 구성에서 **Leapp**은 진행 방법을 결정하기 위해 true/false 질문을 생성합니다. 모든 질문은 **/var/log/leapp/answerfile**에 저장되고, **응답 파일 메시지에 필요한 Missing의 pre-upgrade 보고서에 저장됩니다.** **LeApp**은 모든 질문에 대한 답변을 제공하지 않는 경우 업그레이드를 금지합니다.

업그레이드 전 단계에서 upgradability를 평가할 때 다음 두 가지 옵션이 있습니다.

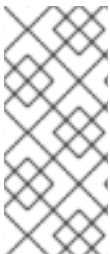
- 생성된 **yunp-report.txt** 파일에서 사전 업그레이드 보고서를 검토하고 명령줄 인터페이스를 사용하여 보고된 문제를 수동으로 해결합니다.
- 웹 콘솔을 사용하여 보고서를 검토하고, 사용 가능한 자동 수정 사항을 적용하고, 제안된 해결 힌트를 사용하여 나머지 문제를 해결합니다.



중요

업그레이드 전 단계에서 **Leapp**은 전체 인플레이스 업그레이드 프로세스를 시뮬레이션하거나 모든 RPM 패키지를 다운로드하지 않습니다.

업그레이드 전 보고서를 검토하면 인플레이스 업그레이드 프로세스 없이 RHEL 8 시스템을 재배치하거나 재배포해야 하는 경우에도 유용합니다.



참고

예를 들어 서로 다른 환경에서 여러 보고서의 결과를 비교하려면 자체 사용자 지정 스크립트를 사용하여 업그레이드 전 보고서를 처리할 수 있습니다. You can process the pre-upgrade report using your own custom scripts, for example, to compare results from multiple reports across different environments. 자세한 내용은 [Red Hat Enterprise Linux 사전 업그레이드 보고서 워크플로 자동화](#)를 참조하십시오.

4.1. 명령줄에서 UPGRADABILITY 평가

명령줄 인터페이스를 사용하여 업그레이드 이전 단계에서 발생할 수 있는 업그레이드 문제를 확인합니다.

사전 요구 사항

- [업그레이드 준비](#)에 나열된 단계가 완료되었습니다.

절차

- RHEL 8 시스템에서 업그레이드 단계를 수행합니다.

```
# leapp preupgrade --target 9.0
```

- 업그레이드에 **/etc/yum.repos.d/** 디렉터리의 [사용자 지정 리포지토리](#)를 사용하려면 다음과 같이 선택한 리포지토리를 활성화합니다.

```
# leapp preupgrade --enablerepo <repository_id1> --enablerepo <repository_id2> ...
```

- **RHSM 없이 업그레이드하거나** RHUI를 사용하려면 **--no-rhsm** 옵션을 추가합니다.
- **EUS (Extended Upgrade Support)**, Advanced Update Support (AUS) 또는 **Update Services for SAP Solutions (E4S)** 서브스크립션이 있는 경우 **--channel** 채널 옵션을 추가합니다. 채널을 채널로 교체합니다(예: **eus,aus,e4s**).

2. 다음 방법 중 하나로 **Leapp**에 필요한 각 질문에 대한 답변을 제공하십시오.

- **ynp** 응답 명령을 실행하여 응답 중인 질문을 지정하고 확인된 응답을 지정합니다.

```
# leapp answer --section <question_section>.<field_name>=<answer>
```

예를 들어 시스템에 VDO 장치가 없는지 질문에 대한 **True** 응답을 확인하려면 다음 명령을 실행합니다.

```
# leapp answer --section check_vdo.no_vdo_devices=True
```

- **/var/log/leapp/answerfile** 파일을 수동으로 편집하고 **#** 기호를 삭제하여 파일의 마지막 줄의 주석을 제거한 다음, **True** 또는 **False**로 답변을 확인합니다. **Leapp 응답file**을 참조하십시오.

3. **/var/log/leapp/leapp-report.txt** 파일의 보고서를 검사하고 인플레이스 업그레이드를 진행하기 전에 보고된 모든 문제를 수동으로 해결합니다.

4.2. 웹 콘솔을 통해 UPGRADABILITY 평가 및 자동 수정 적용

사전 업그레이드 단계에서 발생할 수 있는 문제와 웹 콘솔을 사용하여 자동 수정을 적용하는 방법을 확인합니다.

사전 요구 사항

- **업그레이드 준비에** 나열된 단계가 완료되었습니다.

절차

1. **cockpit-leapp** 플러그인을 설치합니다.

```
# dnf install cockpit-leapp
```

2. 브라우저에서 웹 콘솔로 이동하여 **root** 또는 **/etc/sudoers** 파일에 구성된 사용자로 로그인합니다. 웹 콘솔에 대한 자세한 내용은 **RHEL 8 웹 콘솔을 사용하여 시스템** 관리를 참조하십시오.

3. RHEL 8 시스템에서 명령줄 인터페이스 또는 웹 콘솔 터미널에서 사전 업그레이드 단계를 수행합니다.

```
# leapp preupgrade --target 9.0
```

- 업그레이드에 **/etc/yum.repos.d/** 디렉터리의 **사용자 지정 리포지토리**를 사용하려면 다음과 같이 선택한 리포지토리를 활성화합니다.

```
# leapp preupgrade --target 9.0 --enablerepo <repository_id1> --enablerepo <repository_id2> ...
```

- RHSM 없이 업그레이드하거나 RHUI를 사용하려면 **--no-rhsm** 옵션을 추가합니다.
- EUS (Extended Upgrade Support), Advanced Update Support (AUS) 또는 Update Services for SAP Solutions (E4S) 서브스크립션이 있는 경우 **--channel** 채널 옵션을 추가합니다. 채널을 채널로 교체합니다(예: **eus, aus, e4s**).

4. 웹 콘솔의 왼쪽 메뉴에서 **In-place Upgrade Report** 를 선택합니다.

그림 4.1. 웹 콘솔의 내부 업그레이드 보고서

In-Place Upgrade Report for: localhost.localdomain

Title	Risk Factor	Description	Tags	Time
Repositories map file is invalid (/etc/leapp/files/repomap.csv)	High	⊗ Inhibitor	upgrade process	26.08.2019 15:18:04
OpenSSH configured to use removed ciphers	High	⊗ Inhibitor ⚡ Remediation hint	authentication security network services	26.08.2019 15:23:56
OpenSSH configured to use removed mac	High	⊗ Inhibitor ⚡ Remediation hint	authentication security network services	26.08.2019 15:23:56
Packages not signed by Red Hat found in the system	High	● Remediation command	sanity	26.08.2019 15:23:57
LUKS encrypted partition detected	High	⊗ Inhibitor	boot encryption	26.08.2019 15:23:59
Possible problems with remote login using root account	High	⊗ Inhibitor ⚡ Remediation hint	authentication security network services	26.08.2019 15:23:59
chrony using default configuration	Medium		services time management	26.08.2019 15:23:57
Postfix has incompatible changes in the next major version	Low		services email	26.08.2019 15:23:58
The subscription-manager release is going to be set to 8.0	Low		upgrade process	26.08.2019 15:23:58
Schedule SELinux relabeling	Low		selinux security	26.08.2019 15:23:58

10 per page 1-10 of 16 1 of 2

보고서 테이블은 발견된 문제, 위험 평가 및 수정(사용 가능한 경우)에 대한 개요를 제공합니다.

- 위험 요소:
 - 높음 - 시스템 상태가 저하될 가능성이 높습니다.
 - 중간 - 시스템 및 응용 프로그램에 모두 영향을 줄 수 있습니다.
 - 낮음 - 시스템에 영향을 미치지 않지만 애플리케이션에 영향을 줄 수 있습니다.
 - info - 시스템 또는 애플리케이션에 예상된 영향을 미치지 않는 정보
- Inhibitor - inhibitor - 업그레이드 프로세스를 중단(하드) 그렇지 않으면 시스템이 부팅 가능하거나, 액세스할 수 없거나, 액세스할 수 없거나, 기능이 작동하지 않을 수 있습니다.
- 수정 - 보고된 문제에 대한 실행 가능한 해결 방법:
 - 수정 명령 - 웹 콘솔을 통해 직접 실행할 수 있습니다.
 - 해결 팁 - 문제를 수동으로 해결하는 방법에 대한 지침

5. 보고서의 내용을 검사합니다. 헤더를 클릭하여 테이블을 정렬할 수 있습니다. 세부 정보 창을 열려면 선택한 행을 클릭합니다.

그림 4.2. 세부 정보 창

Title

Packages not signed by Red Hat found in the system

Time

26.08.2019 15:23:57

Risk factor ⓘ

High

Summary

The following packages have not been signed by Red Hat and may be removed in the upgrade process: - leapp - leapp-deps - leapp-repository - leapp-repository-deps - leapp-repository-sos-plugin - python2-leapp - snactor

Links

- [Information about package signatures](#)

Remediations ⓘ

Run Remediation Add to Remediation Plan

Command: yum remove leapp leapp-deps leapp-repository le

Related resources ⓘ

Package

leapp

leapp-deps

leapp-repository

세부 정보 창에는 다음과 같은 추가 정보가 표시됩니다.

- 문제 요약 및 문제를 자세히 설명하는 지식베이스 문서에 대한 링크
 - 수정 - 자동 수정(사용 가능한 경우)을 실행하거나 예약하고 적용 시 결과를 확인할 수 있습니다.
 - 영향을 받는 시스템 리소스: 패키지, 리포지토리, 파일(구성, 데이터), 디스크, 볼륨
6. 선택적으로 결과를 필터링합니다. 보고서의 왼쪽 상단에 있는 **Filters** (필터) 버튼을 클릭하고 기본 설정에 따라 필터를 적용합니다. 필터 카테고리는 서로 함께 적용됩니다.

그림 4.3. 필터

7. 자동 수정을 적용할 문제를 선택합니다. 두 가지 옵션이 있습니다.
 - a. 세부 정보 창에서 **Add to Remediation Plan** 버튼을 클릭하여 개별 항목을 선택합니다. 또는 세부 정보 창에서 **Run Remediation s**(해결 방법 실행)를 클릭하여 직접 개별 수정을 실행할 수 있습니다.
 - b. 보고서 오른쪽 상단에 있는 **Add all remediations to plan** 버튼을 클릭하여 수정을 사용할 수 있는 모든 항목을 선택합니다.
8. 웹 콘솔에서 **Leapp**에 필요한 질문을 검토하고 답변합니다. 응답되지 않은 각 질문은 업그레이드 보고서의 **응답 파일에 필요한 답변**으로 표시됩니다. 질문에 답변할 제목을 선택합니다.
 - a. 기본 **True** 응답을 확인하려면 **Add to Remediation Plan**을 선택하여 나중에 수정 사항을 실행하거나 수정을 즉시 **실행**합니다.
 - b. 대신 기본값이 아닌 대답을 선택하려면 다음 중 하나를 수행합니다.
 - i. **유효p 응답** 명령을 실행하여 응답 중인 질문을 지정하고 확인된 응답을 지정합니다.

```
# leapp answer --section <question_section>.<field_name>=<answer>
```

예를 들어 시스템에 VDO 장치가 없는지 질문에 대한 **True** 응답을 확인하려면 다음 명령을 실행합니다.

```
# leapp answer --section check_vdo.no_vdo_devices=True
```

- ii. `/var/log/leapp/answerfile` 파일을 수동으로 편집하고 **#** 기호를 삭제하여 파일의 마지막 줄의 주석을 제거하고, **True** 또는 **False**로 답변을 확인합니다. [Leapp 응답file 예제](#)를 참조하십시오.

그림 4.4. 답변되지 않은 Leapp 질문이 없습니다.

Upgrade Report for: leapp-20201026142326

Title	Risk Factor	Description	Tags
Upgrade is unsupported	High		upgrade process
Difference in Python versions and support in RHEL 8	High	Remediation hint C* Links	python
Packages not signed by Red Hat found on the system	High		sanity
GRUB core will be updated during upgrade	High		boot
Missing required answers in the answer file	High	inhibitor Remediation hint Remediation command	
Missing required answers in the answer file	High	inhibitor Remediation hint Remediation command	
chrony using default configuration	Medium		services time man
SELinux will be set to permissive mode	Low		selinux security
Profiles has incompatible changes in the next major version	Low	Remediation hint	services email
Dootstools incompatible changes in the next major version	Low	Remediation hint	filesystems tools
Drop has incompatible changes in the next major version	Low	Remediation hint	tools
The subscription-manager release is going to be kept as it is during the upgrade	Low	Remediation hint	upgrade process
Excluded RHEL 8 repositories		C* Links	repository
SELinux relabeling has been scheduled			selinux security
Current PAM and nsswitch.conf configuration will be kept.			authentication

30 - per page

Detail

Title
Missing required answers in the answer file

Time
26.10.2020 15:14:34

Risk factor
High

Summary
One or more sections in answerfile are missing user choices: remove_pam_krb5_module_check.confirm
For more information consult
<https://leapp.readthedocs.io/en/latest/dialogs.html>

Remediations
Please register user choices with leapp answer cli command or by manually editing the answerfile.

Run Remediation | Add to Remediation Plan
Command: leapp answer --section remove_pam_krb5_module_check

Related resources
Dialog
(dialog) = remove_pam_krb5_module_check.confirm

9. 보고서 위의 오른쪽 상단에 있는 해결 계획 링크를 클릭하여 수정 계획을 엽니다. 수정 계획에서는 실행되거나 예약된 모든 수정 목록을 제공합니다.

그림 4.5. 수정 계획

Remediation Plan

Execute Remediation Plan

yum remove leapp leapp-deps leapp-repository leapp-repository-deps leapp-repository-sos-plugin python2-leapp snactor

Remediation-ID	30499418c8169f1a59646cd5910642258411e4cacb6e148e4d89195fb046416c
Status Code	(scheduled)
Runtime	(scheduled)

10. 해결 계획 실행을 클릭하여 예약된 모든 수정을 처리합니다. 각 수정 항목에 다음 정보가 표시됩니다.

- 수정의 고유 ID
- 명령의 종료 상태
- 실행된 수정의 경과 시간
- 표준 출력
- 표준 오류

11. 선택한 수정을 실행한 후 **yp preupgrade** 명령을 사용하여 **pre-upgrade** 보고서를 다시 생성하고 새 보고서를 검사한 후 필요한 경우 추가 수정 단계를 수행합니다.

5장. RHEL 8에서 RHEL 9로 업그레이드 수행

다음 절차에서는 **Leapp** 유틸리티를 사용하여 RHEL 8에서 RHEL 9로의 업그레이드를 수행하는 데 필요한 단계를 나열합니다.

사전 요구 사항

- 전체 시스템 백업을 포함하여 **업그레이드 준비** 단계에 나열된 단계가 완료되었습니다.
- 업그레이드 전 보고서 검토**에 나열된 단계가 완료되었으며 보고된 모든 문제가 해결되었습니다.

절차

1. RHEL 8 시스템에서 업그레이드 프로세스를 시작합니다.

```
# leapp upgrade --target 9.0
```

- 업그레이드에 `/etc/yum.repos.d/` 디렉터리의 **사용자 지정 리포지토리**를 사용하려면 다음과 같이 선택한 리포지토리를 활성화합니다.

```
# leapp upgrade --target 9.0 --enablerepo <repository_id1> --enablerepo <repository_id2> ...
```

- RHSM 없이 업그레이드하거나** RHUI를 사용하려면 **--no-rhsm** 옵션을 추가합니다.
 - EUS (Extended Upgrade Support)**, **Advanced Update Support (AUS)** 또는 **Update Services for SAP Solutions (E4S)** 서브스크립션이 있는 경우 **--channel** 채널 옵션을 추가합니다. 채널을 **yunp preupgrade** 명령과 함께 사용한 값으로 바꿉니다(예: **eus,aus,e4s**). **yunp preupgrade** 및 **leapp upgrade** 명령 둘 다에서 **--channel** 옵션과 함께 동일한 값을 사용해야 합니다.
2. 업그레이드 프로세스 시작 시 **Leapp**은 사전 업그레이드 **보고서 검토**에 설명된 **사전 업그레이드** 단계를 수행합니다.
 - 시스템이 upgradable인 경우 **Leapp**은 필요한 데이터를 다운로드하고 업그레이드를 위해 RPM 트랜잭션을 준비합니다.
 - 시스템이 안정적인 업그레이드의 매개변수를 충족하지 않는 경우 **Leapp**은 업그레이드 프로세스를 종료하고 문제 및 `/var/log/leapp/leapp-report.txt` 파일의 권장 솔루션을 설명하는 레코드를 제공합니다. 자세한 내용은 **문제** 해결을 참조하십시오.
 3. 시스템을 수동으로 재부팅합니다.

```
# reboot
```

이 단계에서는 시스템이 RHEL 9 기반 초기 RAM 디스크 이미지 initramfs로 부팅됩니다. **LeApp**은 모든 패키지를 업그레이드하고 RHEL 9 시스템으로 자동으로 재부팅합니다.

또는 **--reboot** 옵션을 사용하여 **yunp upgrade** 명령을 실행하고 이 수동 단계를 건너뛸 수 있습니다.

오류가 발생하면 **문제** 해결에 설명된 로그 및 알려진 문제를 조사합니다.

4. RHEL 9 시스템에 로그인하고 RHEL 9 시스템의 **업그레이드 후 상태 확인**에 설명된 대로 해당 상태를 확인합니다.

- 업그레이드 후 작업 수행에 설명된 [대로 전체 업그레이드 작업](#). 특히 보안 정책을 다시 평가 및 다시 적용합니다.

6장. RHEL 9 시스템의 업그레이드 후 상태 확인

이 절차에서는 RHEL 9로 인플레이스 업그레이드 후 수행하는 데 권장되는 확인 단계를 나열합니다.

사전 요구 사항

- RHEL 8에서 RHEL 9로의 업그레이드를 수행하는 데 설명된 단계를 따라 시스템이 업그레이드되었으며 RHEL 9에 로그인할 수 있습니다.

절차

업그레이드가 완료되면 시스템이 필수 상태인지 아니면 적어도 다음을 수행합니다.

- 현재 OS 버전이 RHEL 9인지 확인합니다.

```
# cat /etc/redhat-release
Red Hat Enterprise Linux release 9.0 (Plow)
```

- OS 커널 버전을 확인합니다.

```
# uname -r
5.14.0-70.10.1.el9_0.x86_64
```

.el9 는 중요하며 버전이 5.14.0 이전 버전이어야 합니다.

- Red Hat Subscription Manager를 사용하는 경우:

- 올바른 제품이 설치되었는지 확인합니다.

```
# subscription-manager list --installed
+-----+
|          |
| Installed Product Status |
|          |
+-----+
Product Name: Red Hat Enterprise Linux for x86_64
Product ID: 479
Version: 9.0
Arch: x86_64
Status: Subscribed
```

- 업그레이드 직후 릴리스 버전이 9.0으로 설정되어 있는지 확인합니다.

```
# subscription-manager release
Release: 9.0
```

- 예를 들어 네트워크 서비스가 작동하는지 확인합니다. SSH를 사용하여 서버에 연결을 시도합니다.
- 애플리케이션의 업그레이드 후 상태를 확인합니다. 경우에 따라 마이그레이션 및 구성 변경을 수동으로 수행해야 할 수도 있습니다. 예를 들어 데이터베이스 서버를 마이그레이션하려면 [데이터베이스 서버 구성 및 사용](#)의 지침을 따릅니다.

7장. 업그레이드 후 작업 수행

다음 절차에서는 RHEL 9로 인플레이스 업그레이드 후 수행하는 데 권장되는 주요 작업을 나열합니다.

사전 요구 사항

- RHEL 8에서 RHEL 9로의 업그레이드를 수행하는 데 설명된 단계를 따라 시스템이 업그레이드되었으며 RHEL 9에 로그인할 수 있습니다.
- RHEL 9 시스템의 업그레이드 후 상태 확인에 설명된 단계를 따라 인플레이스 업그레이드의 상태가 확인되었습니다.

절차

업그레이드를 수행한 후 다음 작업을 완료합니다.

1. 업그레이드 확장 개발 도구인 **snactor** 패키지를 포함하여 `/etc/dnf/dnf.conf` 구성 파일의 제외 목록에서 나머지 **Leapp** 패키지를 제거합니다. 인플레이스 업그레이드 중에 **Leapp** 유틸리티를 사용하여 설치된 **Leapp** 패키지가 자동으로 제외 목록에 추가되어 중요한 파일이 제거되거나 업데이트되지 않습니다. 인플레이스 업그레이드 후 시스템에서 이러한 **Leapp** 패키지를 제외 목록에서 제거해야 합니다.
 - 제외 목록에서 패키지를 수동으로 제거하려면 `/etc/dnf/dnf.conf` 구성 파일을 편집하고 제외 목록에서 원하는 **Leapp** 패키지를 제거하십시오.
 - 제외 목록에서 모든 패키지를 제거하려면 다음을 수행합니다.

```
# dnf config-manager --save --setopt exclude=
```

2. 나머지 **Leapp** 패키지를 포함하여 나머지 RHEL 8 패키지를 제거합니다.

- a. 나머지 RHEL 8 패키지를 찾습니다.

```
# rpm -qa | grep -e '\.el[78]' | grep -vE '(gpg-pubkey|libmodulemd|katello-ca-consumer)' | sort
```

- b. RHEL 9 시스템에서 이전 커널 패키지를 포함한 나머지 RHEL 8 패키지를 제거합니다.
- c. 나머지 **Leapp** 종속성 패키지를 제거합니다.

```
# dnf remove leapp-deps-el9 leapp-repository-deps-el9
```

3. 보안 정책을 다시 평가 및 다시 적용합니다. 특히 SELinux 모드를 강제로 변경합니다. 자세한 내용은 [보안 정책 적용](#)을 참조하십시오.

8장. 보안 정책 적용

인플레이스 업그레이드 프로세스 중에 SELinux 정책을 허용 모드로 전환해야 합니다. 또한 보안 프로파일에는 주요 릴리스 간 변경 사항이 포함될 수 있습니다. 이 섹션에서는 업그레이드된 RHEL 시스템을 보안할 때 안내하고 보안 관련 구성 요소의 업그레이드 전 단계에 대한 세부 정보를 설명합니다.

8.1. SELINUX 모드를 강제 모드로 변경

인플레이스 업그레이드 프로세스 중에 **Leapp** 유틸리티는 SELinux 모드를 허용으로 설정합니다. 시스템이 성공적으로 업그레이드되면 SELinux 모드를 강제로 수동으로 변경해야 합니다.

사전 요구 사항

- 시스템이 업그레이드되었으며 [RHEL 9 시스템의 업그레이드 후 상태 확인에 설명된 확인](#) 단계를 수행했습니다.

절차

1. 예를 들어 **ausearch** 유틸리티를 사용하여 SELinux 거부가 없는지 확인합니다.

```
# ausearch -m AVC,USER_AVC -ts boot
```

이전 단계에서는 가장 일반적인 시나리오만 다룹니다. 가능한 모든 SELinux 거부를 확인하려면 전체 절차를 제공하는 Using SELinux 제목의 [Identifying SELinux 거부](#) 섹션을 참조하십시오.

2. 선택한 텍스트 편집기에서 **/etc/selinux/config** 파일을 엽니다. 예를 들면 다음과 같습니다.

```
# vi /etc/selinux/config
```

3. **SELINUX=enforcing** 옵션을 구성합니다.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

4. 변경 사항을 저장하고 시스템을 다시 시작하십시오.

```
# reboot
```

검증

1. 시스템을 다시 시작한 후 **getenforce** 명령이 **Enforcing** 을 반환하는지 확인합니다.

```
$ getenforce
Enforcing
```

추가 리소스

- [SELinux 관련 문제 해결](#)
- [SELinux 상태 및 모드 변경](#)

8.2. 시스템 전체 암호화 정책

시스템 전체 암호화 정책은 TLS, IPSec, SSH, DNSSec 및 Kerberos 프로토콜을 다루는 코어 암호화 하위 시스템을 구성하는 시스템 구성 요소입니다.

인플레이스 업그레이드 프로세스는 RHEL 8에서 사용한 암호화 정책을 유지합니다. 예를 들어 RHEL 8에서 **DEFAULT** 암호화 정책을 사용한 경우 시스템은 RHEL 9로 업그레이드된 경우에도 **DEFAULT**를 사용합니다. 사전 정의된 정책의 특정 설정은 다르며 RHEL 9 암호화 정책에는 더 엄격하고 안전한 기본값이 포함되어 있습니다. 예를 들어 RHEL 9 **DEFAULT** 암호화 정책은 서명에 대해 SHA-1 사용을 제한하고 **LEGACY** 정책은 더 이상 2048비트 미만의 DH 및 RSA 암호를 허용하지 않습니다. 자세한 내용은 [보안 강화](#) 문서의 [Strong crypto defaults](#) 섹션을 참조하십시오. 사용자 지정 암호화 정책은 즉각적 업그레이드 전 반에 걸쳐 보존됩니다.

현재 시스템 차원의 암호화 정책을 보거나 변경하려면 update-crypto-policies 도구를 사용합니다.

```
$ update-crypto-policies --show
DEFAULT
```

예를 들어 다음 명령은 시스템 전체 암호화 정책 수준을 **FUTURE** 로 전환합니다. 이 수준은 가까운 미래의 공격에 대응해야 합니다.

```
# update-crypto-policies --set FUTURE
Setting system policy to FUTURE
```

시나리오에 SHA-1을 사용하여 기존 또는 타사 암호화 서명을 확인해야 하는 경우 다음 명령을 입력하여 활성화할 수 있습니다.

```
# update-crypto-policies --set DEFAULT:SHA1
```

또는 시스템 전체 암호화 정책을 LEGACY 정책으로 전환할 수 있습니다. 그러나 **LEGACY** 는 또한 안전하지 않은 다른 많은 알고리즘을 사용할 수 있습니다.



주의

SHA 하위 정책을 활성화하면 기본 RHEL 9 설정보다 시스템에 더 취약합니다. **LEGACY** 정책으로 전환하는 것은 보안 수준이 낮기 때문에 주의해서 사용해야 합니다.

시스템 전체 암호화 정책을 사용자 지정할 수도 있습니다. 자세한 내용은 정책 [수정자를 사용하여 시스템 전체 암호화 정책 사용자 지정](#) 및 [사용자 지정 시스템 차원의 암호화 정책 생성 및 설정](#)을 참조하십시오. 사용자 지정 암호화 정책을 사용하는 경우 정책을 검토하고 업데이트하여 암호화 및 컴퓨터 하드웨어에서 사전에 가져온 위협을 완화하는 것이 좋습니다.

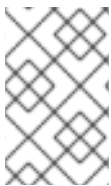
추가 리소스

- [시스템 전체 암호화 정책 사용](#)
- [update-crypto-policies\(8\)](#) 매뉴얼 페이지.

8.3. 보안 기준으로 강화된 시스템 업그레이드

RHEL 9로 업그레이드한 후 완전히 강화된 시스템을 얻으려면 OpenSCAP 제품군에서 제공하는 자동 수정을 사용할 수 있습니다. OpenSCAP 수정을 통해 PCI-DSS, OSPP 또는 ACSC Eight와 같은 보안 기준선에 맞게 시스템을 조정합니다. 보안 제품의 발전으로 인해 구성 컴플라이언스 권장 사항은 RHEL의 주요 버전과 다릅니다.

강화된 RHEL 8 시스템을 업그레이드할 때 **Leapp** 툴은 전체 강화를 유지할 수 있는 직접적인 수단을 제공하지 않습니다. 구성 요소 구성 요소의 변경 사항에 따라 시스템은 업그레이드 중 RHEL 9 권장 사항과 다를 수 있습니다.



참고

RHEL 8 및 RHEL 9을 스캔하는 데 동일한 SCAP 콘텐츠를 사용할 수 없습니다. Red Hat Satellite 또는 Red Hat Insights와 같은 툴에서 시스템 규정 준수를 관리하는 경우 관리 플랫폼을 업데이트합니다.

자동화된 수정 대신 OpenSCAP 생성 보고서를 따라 수동으로 변경할 수 있습니다. 규정 준수 보고서를 생성하는 방법에 대한 자세한 내용은 [보안 규정 준수 및 취약점에 대해 시스템](#) 검사를 참조하십시오.



중요

자동 수정은 기본 구성에서 RHEL 시스템을 지원합니다. 업그레이드 후 시스템 구성이 변경되었으므로 자동 수정을 실행하면 시스템이 필요한 보안 프로필을 완전히 준수하지 않을 수 있습니다. 일부 요구 사항을 수동으로 수정해야 할 수도 있습니다.

다음 예제 절차에서는 PCI-DSS 프로필에 따라 시스템 설정을 강화합니다.

사전 요구 사항

- **scap-security-guide** 패키지는 RHEL 9 시스템에 설치됩니다.

절차

1. 적절한 보안 컴플라이언스 데이터 스트림 **.xml** 파일을 찾습니다.

```
$ ls /usr/share/xml/scap/ssg/content/
...
ssg-rhel9-ds.xml
...
```

자세한 내용은 [규정 준수 프로필 보기](#) 섹션을 참조하십시오.

2. 적절한 데이터 스트림에서 선택한 프로필에 따라 시스템을 교정합니다.

```
# oscap xccdf eval --profile pci-dss --remediate /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
```

--profile 인수의 **pci-dss** 값을 시스템을 강화하려는 프로파일 ID로 교체할 수 있습니다. RHEL 9에서 지원되는 전체 프로필 목록은 [RHEL에서 지원되는 SCAP 보안 프로필](#)을 참조하십시오.



주의

신중하게 사용하지 않으면 **--remediate** 옵션을 사용하여 시스템 평가를 실행하면 시스템이 작동하지 않을 수 있습니다. Red Hat은 보안 강화 수정으로 인한 변경 사항을 되돌릴 수 있는 자동화된 방법을 제공하지 않습니다. 수정은 기본 구성의 RHEL 시스템에서 지원됩니다. 설치 후 시스템이 변경된 경우 수정을 실행하여 필요한 보안 프로필을 준수하지 못할 수 있습니다.

3. 시스템을 다시 시작하십시오.

```
# reboot
```

검증

1. 시스템이 프로필과 호환되는지 확인하고 결과를 HTML 파일에 저장합니다.

```
$ oscap xccdf eval --report pcidss_report.html --profile pci-dss
/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
```

추가 리소스

- [scap-security-guide\(8\)](#) 및 [oscap\(8\)](#) 도움말 페이지
- [보안 규정 준수 및 취약점에 대한 시스템 스캔](#)
- [Red Hat Insights Security Policy](#)
- [Red Hat Satellite 보안 정책](#)

8.4. USBGUARD 정책 확인

USBGuard 소프트웨어 프레임워크를 사용하면 커널의 USB 장치 권한 부여 기능을 기반으로 허용되거나 금지된 장치 목록을 사용하여 시스템을 침입하지 못하도록 보호할 수 있습니다.

사전 요구 사항

- 업그레이드하기 전에 시나리오의 요구 사항을 반영한 USB 장치에 대한 규칙 세트를 생성했습니다.
- **usbguard** 서비스가 RHEL 9 시스템에 설치되어 실행되고 있습니다.

절차

1. **/etc/usbguard/** 디렉터리에 저장된 *.conf 파일을 백업합니다.

2. **usbguard generate-policy**를 사용하여 새 정책 파일을 생성합니다. 명령은 현재 사용 중인 USB 장치에 대한 규칙만 생성합니다.
3. 새로 생성된 규칙을 이전 정책의 규칙과 비교합니다.
 - a. 새 정책을 생성할 때 존재하는 장치의 규칙 및 동일한 장치에 대한 사전 업그레이드 규칙을 확인하는 경우 나중에 삽입할 수 있는 장치에 해당하는 원래 규칙도 수정합니다.
 - b. 새로 생성된 규칙과 사전 업그레이드 규칙에 차이점이 없는 경우 수정 없이 RHEL 8에서 생성된 정책 파일을 사용할 수 있습니다.

추가 리소스

- [침입할 수 없는 USB 장치로부터 시스템 보호](#).

8.5. FAPOLICYD 데이터베이스 업데이트

fapolicyd 소프트웨어 프레임워크는 사용자 정의 정책을 기반으로 애플리케이션 실행을 제어합니다.

드문 경우지만 **fapolicyd** trust 데이터베이스 형식의 문제가 발생할 수 있습니다. 데이터베이스를 다시 빌드하려면 다음을 수행합니다.

1. 서비스를 중지합니다.

```
# systemctl stop fapolicyd
```

2. 데이터베이스를 삭제합니다.

```
# fapolicyd-cli --delete-db
```

3. 서비스를 시작합니다.

```
# systemctl start fapolicyd
```

신뢰 데이터베이스에 사용자 정의 신뢰 파일을 추가한 경우 **fapolicyd-cli -f update < FILE>** 명령을 사용하거나 **fapolicyd-cli -f update -f update**를 사용하여 개별적으로 업데이트합니다. 변경 사항을 적용하려면 **fapolicyd-cli -update** 명령을 사용하거나 **fapolicyd** 서비스를 다시 시작합니다.

또한 사용자 정의 바이너리를 사용하려면 새 RHEL 버전을 다시 빌드해야 할 수 있습니다. **fapolicyd** 데이터베이스를 업데이트하기 전에 이러한 업데이트를 수행합니다.

추가 리소스

- [fapolicyd를 사용하여 애플리케이션을 차단 및 허용](#)

8.6. DBM에서 SQLITE로 NSS 데이터베이스 업데이트

NSS_DEFAULT_DB_TYPE 환경 변수를 시스템의 **sql** 값으로 설정한 후 NSS 데이터베이스 형식을 자동으로 DBM에서 SQLite로 변환합니다. **certutil** 툴을 사용하여 모든 데이터베이스가 변환되었는지 확인할 수 있습니다.



참고

RHEL 9로 업그레이드하기 전에 DBM 형식에 저장된 NSS 데이터베이스를 변환합니다. 즉, RHEL 9로 업그레이드하려는 RHEL 시스템(6, 7, 8)에서 다음 단계를 수행합니다.

사전 요구 사항

- **nss-utils** 패키지가 시스템에 설치되어 있습니다.

절차

1. 시스템에서 **NSS_DEFAULT_DB_TYPE** 을 **sql** 으로 설정합니다.

```
# export NSS_DEFAULT_DB_TYPE=sql
```

2. 모든 디렉터리에서 변환 명령 사용^[1] 여기에는 DBM 형식의 NSS 데이터베이스 파일이 포함됩니다. 예를 들면 다음과 같습니다.

```
# certutil -K -X -d /etc/ipsec.d/
```

데이터베이스 파일이 암호로 보호되는 경우 **-f** 옵션의 값으로 암호 또는 암호 파일의 경로를 제공해야 합니다. 예를 들면 다음과 같습니다.

```
# certutil -K -X -f /etc/ipsec.d/nsspassword -d /etc/ipsec.d/
```

추가 리소스

- **certutil(1)** 도움말 페이지.

8.7. BERKELEY DB 형식에서 GDBM으로 CYRUS SASL 데이터베이스 마이그레이션

RHEL 9 **cyrus-sasl** 패키지는 **libdb** 종속성 없이 구축되며, **sasldb** 플러그인은 Berkeley DB 대신 GDBM 데이터베이스 형식을 사용합니다.

사전 요구 사항

- **cyrus-sasl-lib** 패키지가 시스템에 설치되어 있습니다.

절차

- 이전 Berkeley DB 형식으로 저장된 기존 SASL(Simple Authentication and Security Layer) 데이터베이스를 마이그레이션하려면 다음 구문과 함께 **cyrusbdb2current** 도구를 사용합니다.

```
# cyrusbdb2current <sasldb_path> <new_path>
```

추가 리소스

- **cyrusbdb2current(1)** 매뉴얼 페이지

[1] RHEL에는 **/etc/pki/nssdb** 디렉터리에 시스템 전체 NSS 데이터베이스가 포함되어 있습니다. 다른 위치는 사용하는 애플리케이션에 따라 다릅니다. 예를 들어 Libreswan은 **/etc/ipsec.d/** 디렉토리에 데이터베이스를 저장하고 Firefox는 **/home/<username>/.mozilla/firefox/** 디렉터리를 사용합니다.

9장. 문제 해결

다음 팁을 참조하여 RHEL 8에서 RHEL 9로의 업그레이드 문제를 해결할 수 있습니다.

9.1. 리소스 문제 해결

다음과 같은 문제 해결 리소스를 참조할 수 있습니다.

콘솔 출력

기본적으로 오류 및 심각한 로그 수준 메시지만 **Leapp** 유틸리티에서 콘솔 출력에 출력됩니다. 로그 수준을 변경하려면 **rpm upgrade** 명령과 함께 **--verbose** 또는 **--debug** 옵션을 사용합니다.

- *자세한 정보 표시* 모드에서 **Leapp** 은 정보, 경고, 오류 및 심각한 메시지를 출력합니다.
- *디버그* 모드에서 **Leapp** 은 debug, info, warning, error 및 critical 메시지를 출력합니다.

로그

- **/var/log/leapp/leapp-upgrade.log** 파일은 initramfs 단계에서 발견된 문제를 나열합니다.
- **/var/log/leapp/dnf-debugdata/** 디렉터리에는 트랜잭션 디버그 데이터가 포함되어 있습니다. 이 디렉터리는 **rpm upgrade** 명령이 **--debug** 옵션으로 실행되는 경우에만 존재합니다.
- **/var/log/leapp/answerfile**에는 **Leapp** 에서 답변하는데 필요한 질문이 포함되어 있습니다.
- **journalctl** 유틸리티는 완전한 로그를 제공합니다.

Reports

- **/var/log/leapp/leapp-report.txt** 파일에는 업그레이드 전 단계에서 발견된 문제가 나열됩니다. 웹 콘솔에서도 보고서를 사용할 수 있습니다. 웹 콘솔을 통해 업그레이드 기능 적용 및 자동 수정 적용을 참조하십시오.
- **/var/log/leapp/leapp-report.json** 파일은 머신에서 읽을 수 있는 형식의 사전 업그레이드 단계에서 발견된 문제를 나열하여 사용자 정의 스크립트를 사용하여 보고서를 처리할 수 있습니다. 자세한 내용은 [Red Hat Enterprise Linux 사전 업그레이드 보고서 워크플로 자동화](#)를 참조하십시오.

9.2. 문제 해결 팁

다음 문제 해결 팁을 참조할 수 있습니다.

업그레이드 전 단계

- 시스템이 [업그레이드 계획에 나열된 모든 조건을 충족하는지 확인](#)하십시오.
- [업그레이드](#) 준비에 설명된 모든 단계를 예를 들어 시스템에서 커널(**eth**)에서 사용하는 접두사에 따라 이름 기반의 NIC(네트워크 인터페이스 카드)를 두 개 이상 사용하지 않는지 확인합니다.
- **/var/log/leapp/answerfile** 파일의 **Leapp** 에서 요구하는 모든 질문에 답변했는지 확인하십시오. 응답이 누락된 경우 **Leapp** 이 업그레이드를 금지합니다. 예를 들어 다음과 같습니다.
 - 시스템에 VDO 장치가 있습니까?

- `/var/log/leapp-report.txt`에 있는 사전 업그레이드 보고서에서 확인된 모든 문제를 해결했는지 확인합니다. 이를 위해 확장 가능성에 설명된 대로 웹 콘솔을 사용하고 웹 콘솔을 통해 자동 수정 사항을 적용할 수도 있습니다.

예 9.1. LeApp 응답 파일

다음은 대답되지 않은 질문 하나가 있는 편집되지 않은 `/var/log/leapp/answerfile` 파일의 예입니다.

```
[check_vdo]
# Title:          None
# Reason:         Confirmation
# ===== check_vdo.no_vdo_devices
=====
# Label:          Are there no VDO devices on the system?
# Description:    Enter True if there are no VDO devices on the system and False continue the
upgrade. If the system has no VDO devices, then it is safe to continue the upgrade. If there are
VDO devices they must all be converted to LVM management before the upgrade can proceed.
# Reason:        Based on installed packages it is possible that VDO devices exist on the
system. All VDO devices must be converted to being managed by LVM before the upgrade
occurs. Because the 'vdo' package is not installed, Leapp cannot determine whether any VDO
devices exist that have not yet been converted. If the devices are not converted and the upgrade
proceeds the data on unconverted VDO devices will be inaccessible. If you have any doubts you
should choose to install the 'vdo' package and re-run the upgrade process to check for
unconverted VDO devices. If you are certain that the system has no VDO devices or that all VDO
devices have been converted to LVM management you may opt to allow the upgrade to proceed.
# Type:          bool
# Default:       None
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
# no_vdo_devices =
```

Label 필드는 대답이 필요한 질문을 지정합니다. 이 예에서 문제는 시스템에 VDO 장치가 없다는 것입니다.

질문에 대답하려면 마지막 줄의 주석 처리를 제거하고 **True** 또는 **False** 응답을 입력합니다. 이 예에서 선택한 답변은 **True**입니다.

```
[check_vdo]
...
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
no_vdo_devices = True
```

다운로드 단계

- RPM 패키지를 다운로드하는 동안 문제가 발생하면 `/var/log/leapp/dnf-debugdata/` 디렉터리에 있는 트랜잭션 디버그 데이터를 검사합니다.



참고

`/var/log/leapp/dnf-debugdata/` 디렉터리가 비어 있거나 트랜잭션 디버그 데이터가 생성되지 않은 경우 존재하지 않습니다. 이 문제는 필요한 리포지토리를 사용할 수 없는 경우 발생할 수 있습니다.

initramfs 단계

- 이 단계에서 잠재적인 실패가 Dracut 셸로 리디렉션됩니다. 저널 로그를 확인합니다.

```
# journalctl
```

또는 **reboot** 명령을 사용하여 Dracut 셸에서 시스템을 다시 시작하고 **/var/log/leapp/leapp-upgrade.log** 파일을 확인합니다.

post-upgrade 단계

- 시스템을 성공적으로 업그레이드하고 이전 RHEL 8 커널로 부팅한 것처럼 보이는 경우 시스템을 다시 시작하고 GRUB에서 기본 항목의 커널 버전을 확인합니다.
- RHEL 9 시스템의 업그레이드 후 상태** 확인을 위한 권장 단계를 따르십시오.
- SELinux를 강제 모드로 전환한 후 애플리케이션 또는 서비스가 작동하지 않거나 잘못 작동하는 경우 **ausearch**, **journalctl** 또는 **dmesg** 유틸리티를 사용하여 거부를 검색합니다.

```
# ausearch -m AVC,USER_AVC -ts boot
# journalctl -t setroubleshoot
# dmesg | grep -i -e selinux -e type=1400
```

가장 일반적인 문제는 잘못된 레이블 지정으로 인해 발생합니다. 자세한 내용은 [SELinux 관련 문제 해결](#)을 참조하십시오.

9.3. 확인된 문제

다음은 RHEL 8에서 RHEL 9로 업그레이드할 때 발생할 수 있는 알려진 문제입니다.

- 네트워크 타이밍은 현재 Network Manager가 비활성화되거나 설치되지 않은 상태에서 인플레이스 업그레이드를 수행할 때 작동하지 않습니다.
- HTTP 프록시를 사용하는 경우 이러한 프록시를 사용하도록 Red Hat Subscription Manager를 구성하거나 **--proxy <hostname>** 옵션을 사용하여 **subscription-manager** 명령을 실행해야 합니다. 그러지 않으면 **subscription-manager** 명령의 실행이 실패합니다. 구성 변경 대신 **--proxy** 옵션을 사용하는 경우 **Leapp** 이 프록시를 탐지할 수 없기 때문에 업그레이드 프로세스가 실패합니다. 이 문제가 발생하지 않도록 하려면 [Red Hat 서브스크립션 관리에 대해 HTTP 프록시를 구성하는 방법](#)에 설명된 대로 **rhsm.conf** 파일을 수동으로 편집합니다. (BZ#1689294)
- RHEL 8 시스템에서 Red Hat에서 제공하지만 RHEL 9에서는 사용할 수 없는 장치 드라이버를 사용하는 경우 업그레이드를 수행합니다. 그러나 RHEL 8 시스템에서 **/etc/leapp/files/device_driver_deprecation_data.json** 파일에 있는 데이터가 없는 타사 장치 드라이버를 사용하는 경우 **Leapp** 에서 해당 드라이버를 탐지하지 않고 업그레이드를 진행합니다. 따라서 업그레이드 후 시스템을 부팅하지 못할 수 있습니다.
- 시스템에 설치된 타사 패키지의 이름(Red Hat에서 서명하지 않음)이 Red Hat에서 제공하는 패키지의 이름과 동일한 경우 인플레이스 업그레이드가 실패합니다. 이 문제를 해결하려면 업그레이드하기 전에 다음 옵션 중 하나를 선택하십시오.
 - 타사 패키지 제거
 - 타사 패키지를 Red Hat에서 제공하는 패키지로 교체
- RHEL 8에서는 VDO 관리자 또는 LVM(Logical Volume Manager)을 사용하여 VDO(Virtual Data Optimizer) 볼륨을 관리할 수 있습니다. RHEL 9에서는 LVM을 사용하여 VDO 볼륨만 관리할 수

있습니다. 업그레이드 후 VDO 관리 볼륨을 계속 사용하려면 해당 볼륨을 LVM 관리 VDO 볼륨으로 가져옵니다.

1. RHEL 8 시스템에 VDO 및 LVM의 최신 버전이 설치되어 있는지 확인합니다.
2. 인플레이스 업그레이드를 시작하기 전에 VDO 관리 VDO 볼륨을 LVM 관리 VDO 볼륨으로 가져옵니다.

```
# lvm_import_vdo --name <volume_group_name>/<lvm_name>
/dev/mapper/<vdo_name>
```

volume_group_name 을 새 볼륨 그룹 이름, *lvm_name* 을 LVM-managed VDO 볼륨의 새 이름으로, *VNI_name* 을 가져오는 VDO 관리 볼륨의 이름으로 바꿉니다.



중요

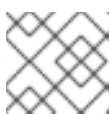
LVM 관리 VDO 볼륨은 VDO로 관리되는 VDO 볼륨으로 가져올 수 없습니다. 따라서 나중에 VDO 관리자를 통해 이러한 VDO 볼륨에 액세스하려는 경우가 저오기 절차를 되돌릴 수 없습니다. LVM 관리 VDO 볼륨에 대한 자세한 내용은 RHEL 가이드의 논리 볼륨 중복 및 압축을 참조하십시오.

- 소프트웨어 RAID(Redundant Array of IRAID)가 있는 시스템에서 인플레이스 업그레이드가 실패합니다. (BZ#1957192)
- 인플레이스 업그레이드 중에 **Leapp** 유틸리티는 일반적으로 RHEL 8과 RHEL 9 간에 NIC(네트워크 인터페이스 컨트롤러) 이름을 유지합니다. 그러나 네트워크 본딩이 있는 시스템(예: 네트워크 본딩이 있는 시스템)에서는 RHEL 8과 RHEL 9 간에 NIC 이름을 업데이트해야 할 수 있습니다. 해당 시스템에서 **LEAPP_NO_NETWORK_RENAMING=1** 환경 변수를 설정하고 내부 업그레이드를 수행한 다음 네트워크가 예상대로 작동하는지 확인합니다. 필요한 경우 네트워크 구성을 수동으로 업데이트합니다. (BZ#1919382)
- NFS 서버에서 실행되는 NSFD 서비스가 있는 시스템에서는 인플레이스 업그레이드 중에 존재하지 않는 NFS 파티션이 잘못 감지되어 업그레이드를 수행할 수 있습니다. 이 문제를 방지하려면 인플레이스 업그레이드를 실행하기 전에 NFSD 서비스를 중지합니다.

```
# systemctl stop /proc/fs/nfsd
```

(BZ#2036069)

- **Leapp** 유틸리티에서 사용 가능한 디스크 공간이 충분하지 않다는 것을 잘못 탐지하기 때문에 업그레이드 전에 인플레이스 업그레이드가 중지될 수 있습니다. 시스템에 *ftype* 속성 없이 XFS 파일 시스템으로 포맷된 파티션이 포함된 경우 **LEAPP_OVL_SIZE** 환경 변수의 기본 크기를 최소한 컨테이너 내부에 누락된 지정된 디스크 공간을 고려하여 이 문제를 해결할 수 있습니다. 반복된 오류 메시지를 방지하기 위해 기본 크기를 지정된 누락된 디스크 공간보다 크게 늘리는 것이 좋습니다. 예를 들어 **Leapp** 유틸리티에서 추가 400MB가 필요하다는 것을 감지하면 기본 크기를 2048MB에서 최소 2500MB로 늘립니다.



참고

이 해결방법은 */var* 파티션에 많은 양의 여유 공간이 필요할 수 있습니다.

이 해결 방법으로 문제가 해결되지 않거나 시스템에 *ftype* 속성없이 이러한 파티션이 포함되어 있지 않은 경우 Red Hat 지원에 문의하십시오. (BZ#1832730)

- 64비트 ARM 아키텍처가 있는 시스템에서는 RHEL 8의 커널 페이지 크기가 64k에서 RHEL 9에서

4k로 변경되었습니다. 따라서 인플레이스 업그레이드 후 스왑 파티션이 자동으로 마운트되지 않습니다. 이 문제를 해결하려면 스왑 파티션을 수동으로 마운트하고 인플레이스 업그레이드를 수행한 후 스왑을 다시 초기화합니다.

```
# swapon -a --fixpgsz
```

(BZ#2040470)

- 인플레이스 업그레이드는 RoCE Express 어댑터를 사용하는 IBM Z의 네트워킹을 분리합니다. RHEL 9.0에서는 RoCE Express 어댑터에 Predictable Interface Name을 사용합니다. RHEL 8.6 배포판에서 사용할 수 있는 이름과 다릅니다. 따라서 RHEL 8에서 RHEL 9로 즉각적 업그레이드를 수행하는 경우 RoCE Express 어댑터의 기존 네트워킹 구성이 현재 RHEL 9 마이너 릴리스와 함께 중단됩니다.
- 즉각적 업그레이드 중에 [RHEL 8에서 RHEL 9로 업그레이드를 수행하는](#) 후 수동 재부팅 후 문제가 발생하면 시스템이 긴급 모드로 전환됩니다. `-debug` 옵션 없이 `stapp upgrade` 명령을 실행하거나 수동 재부팅 후 명령줄 인터페이스에서 키보드를 입력하는 경우 시스템이 긴급 모드를 잘못 입력할 수 있습니다. 이 경우 긴급 모드로 전환해도 업그레이드가 예상대로 진행됩니다. 시스템이 긴급 모드로 전환되면 해결해야 할 문제가 없는지 확인하고 업그레이드가 계속 진행 중인지 확인합니다.

```
# ps -e | grep leapp && echo "The upgrade is still running; do nothing and wait"
```

필요에 따라 이 명령을 여러 번 실행할 수 있습니다. 업그레이드가 계속 진행 중인 경우 추가 작업을 수행할 필요가 없으며 즉각적 업그레이드가 완료되면 업그레이드된 시스템을 부팅할 수 있습니다.

(BZ#2092005)

- RHUI(Red Hat Update Infrastructure)를 사용하는 AWS(Amazon Web Services)의 온 디맨드 Pay-As-You-Go (PAYG) 인스턴스용 인플레이스 업그레이드는 [RHEL High Availability Amazon Machine Image \(AMI\)](#)에서만 가능합니다. 현재 다른 RHEL AMI를 사용하여 업그레이드를 수행할 수 없습니다. (BZ#2106904)

9.4. 지원 받기

지원 사례를 열고 제품으로 *RHEL 7* 을 선택하고 시스템에서 **sosreport** 를 제공할 수 있습니다.

- 시스템에서 **sosreport** 를 생성하려면 다음을 실행합니다.

```
# sosreport
```

사례 ID를 비워 둘 수 있습니다.

sosreport 생성에 대한 자세한 내용은 [What is an sosreport and how to create one in Red Hat Enterprise Linux?](#) 를 참조하십시오.

고객 포털에서 지원 케이스를 열고 관리하는 방법에 대한 자세한 내용은 [How do I open and manage a support case on the Customer Portal](#) 에서 참조하십시오.

10장. 관련 정보

다음과 같은 교육 자료를 참조할 수 있습니다.

- [Red Hat Enterprise Linux 기술 기능 및 제한사항](#)
- [Red Hat Enterprise Linux에서 지원되는 인플레이스 업그레이드 경로](#)
- [RHEL 9 채택 고려 사항](#)
- [Red Hat Enterprise Linux 내부 업그레이드 사용자 정의](#)
- [Red Hat Enterprise Linux 사전 업그레이드 보고서 워크플로 자동화](#)
- [구성 관리 시스템을 사용하여 Red Hat Enterprise Linux에서 Leapp 사전 업그레이드 및 업그레이드 프로세스의 일부를 자동화](#)
- [연결이 끊긴 업그레이드를 위해 RHEL의 인플레이스 업그레이드 인 LeApp 유틸리티 메타데이터](#)
- [RHEL 7에서 RHEL 8로 업그레이드](#)
- [CentOS 또는 Oracle Linux에서 RHEL로 변환하는 방법](#)
- [Red Hat Insights 문서](#)

부록 A. RHEL 8 리포지토리

업그레이드하기 전에 업그레이드를 위한 RHEL 8 시스템 준비 절차의 4단계에 설명된 대로 적절한 리포지토리가 활성화되어 있는지 확인합니다.

업그레이드 중에 Red Hat Subscription Manager를 사용하려면 **subscription-manager repos -- enable repository_id** 명령을 사용하여 업그레이드하기 전에 다음 리포지토리를 활성화해야 합니다.

표 A.1. RHEL 8 리포지토리

아키텍처	리포지토리	리포지토리 ID
64비트 Intel 및 AMD	base	rhel-8-for-x86_64-baseos-rpms
	AppStream	rhel-8-for-x86_64-appstream-rpms
64비트 ARM	base	rhel-8-for-aarch64-baseos-rpms
	엑스트라스	rhel-8-for-aarch64-appstream-rpms
IBM POWER (리틀 endian)	base	rhel-8-for-ppc64le-baseos-rpms
	AppStream	rhel-8-for-ppc64le-appstream-rpmss
IBM Z	base	rhel-8-for-s390x-baseos-rpms
	AppStream	rhel-8-for-s390x-appstream-rpms

subscription-manager repos -- enable repository_id 명령을 사용하여 업그레이드하기 전에 다음 리포지토리를 활성화할 수 있습니다.

표 A.2. 자발적으로 RHEL 8 리포지토리

아키텍처	리포지토리	리포지토리 ID
64비트 Intel 및 AMD	Code Ready Linux Builder	codeready-builder-for-rhel-8-x86_64-rpms
	보조	rhel-8-for-x86_64-supplementary-rpms
64비트 ARM	Code Ready Linux Builder	codeready-builder-for-rhel-8-aarch64-rpms
	보조	rhel-8-for-aarch64-supplementary-rpms
IBM POWER (리틀 endian)	Code Ready Linux Builder	codeready-builder-for-rhel-8-ppc64le-rpms
	보조	rhel-8-for-ppc64le-supplementary-rpms

아키텍처	리포지터리	리포지터리 ID
IBM Z	Code Ready Linux Builder	codeready-builder-for-rhel-8-s390x-rpms
	보조	rhel-8-for-s390x-supplementary-rpms



참고

인플레이스 업그레이드 전에 RHEL 8 Code Ready Linux Builder 또는 RHEL 8 보조 리포지토리를 활성화한 경우, **Leapp** 을 사용하면 RHEL 8 CodeReady Linux Builder 또는 RHEL 8 추가 리포지토리가 각각 활성화됩니다. 자세한 내용은 [패키지 매니페스트](#) 를 참조하십시오.

사용자 정의 리포지토리를 사용하려면 사용자 정의 리포지토리 [구성](#) 의 지침에 따라 활성화합니다.

부록 B. RHEL 9 리포지토리

RHSM(Red Hat Subscription Manager)을 사용하여 시스템을 Red Hat CDN(Content Delivery Network)에 등록한 경우 인플레이스 업그레이드 중에 RHEL 9 리포지토리가 자동으로 활성화됩니다. 그러나 RHSM을 사용하여 Red Hat Satellite에 등록된 시스템에서는 사전 업그레이드 보고서를 실행하기 전에 RHEL 8 및 RHEL 9 리포지토리를 모두 수동으로 활성화하고 동기화해야 합니다.



참고

각 리포지토리의 버전 9.0을 사용하도록 설정합니다. 리포지토리의 RHEL 9 버전만 활성화한 경우 인플레이스 업그레이드가 억제되어 있습니다.

업그레이드 중에 Red Hat Satellite를 사용하려면 Satellite 웹 UI 또는 **hammer repository-set enable** 및 **hammer product synchronize** 명령을 사용하여 업그레이드하기 전에 다음 RHEL 9 리포지토리를 활성화하고 동기화해야 합니다.

표 B.1. RHEL 9 리포지토리

아키텍처	리포지토리	리포지토리 ID	리포지토리 이름	릴리스 버전
64비트 Intel 및 AMD	BaseOS	rhel-9-for-x86_64-baseos-rpms	Red Hat Enterprise Linux 9 for x86_64 - BaseOS(RPM)	x86_64 9.0
	AppStream	rhel-9-for-x86_64-appstream-rpms	Red Hat Enterprise Linux 9 for x86_64 - AppStream(RPM)	x86_64 9.0
64비트 ARM	BaseOS	rhel-9-for-aarch64-baseos-rpms	Red Hat Enterprise Linux 9 for ARM 64 - BaseOS(RPM)	aarch64 9.0
	AppStream	rhel-9-for-aarch64-appstream-rpms	Red Hat Enterprise Linux 9 for ARM 64 - AppStream(RPM)	aarch64 9.0
IBM Power (little endian)	BaseOS	rhel-9-for-ppc64le-baseos-rpms	Red Hat Enterprise Linux 9 for Power, little endian - BaseOS(RPM)	ppc64le 9.0
	AppStream	rhel-9-for-ppc64le-appstream-rpms	Red Hat Enterprise Linux 9 for Power, little endian - AppStream(RPM)	ppc64le 9.0

아키텍처	리포지터리	리포지터리 ID	리포지터리 이름	릴리스 버전
IBM Z	BaseOS	rhel-9-for-s390x-baseos-rpms	Red Hat Enterprise Linux 9 for IBM z Systems - BaseOS(RPM)	s390x 9.0
	AppStream	rhel-9-for-s390x-appstream-rpms	Red Hat Enterprise Linux 9 for IBM z Systems - AppStream(RPM)	s390x 9.0