



# Red Hat Enterprise Linux 8

## RHEL 7에서 RHEL 8로 업그레이드

Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8으로의 인플레이스(In-Place) 업그레이드 방법



# Red Hat Enterprise Linux 8 RHEL 7에서 RHEL 8로 업그레이드

---

Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8으로의 인플레이스(In-Place) 업그레이드 방법

## 법적 공지

Copyright © 2024 Red Hat, Inc.

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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 7에서 Red Hat Enterprise Linux 8로의 인플레이스(In-Place) 업그레이드를 수행하는 방법에 대해 설명합니다. 인플레이스 업그레이드 중에 기존 RHEL 7 운영 체제는 RHEL 8 버전으로 교체됩니다.

## 차례

RED HAT 문서에 관한 피드백 제공 .....	3
주요 마이그레이션 용어 .....	4
1장. 지원되는 업그레이드 경로 .....	5
2장. 업그레이드 프로세스 개요 .....	6
3장. 업그레이드 계획 .....	7
4장. 업그레이드 준비 .....	10
4.1. 업그레이드를 위한 RHEL 7 시스템 준비 .....	10
4.2. 업그레이드를 위한 SATELLITE 등록 시스템 준비 .....	14
5장. 업그레이드 전 보고서 검토 .....	17
5.1. 명령줄에서 업그레이드 가능성 평가 .....	17
5.2. 웹 콘솔을 통해 업그레이드 가능성 평가 및 자동 복구 적용 .....	19
6장. RHEL 7에서 RHEL 8로의 업그레이드 수행 .....	23
7장. RHEL 8 시스템의 업그레이드 후 상태 확인 .....	25
8장. 업그레이드 후 작업 수행 .....	27
9장. 보안 정책 적용 .....	30
9.1. SELINUX 모드를 강제 모드로 변경 .....	30
9.2. 시스템 전체 암호화 정책 설정 .....	31
9.3. 시스템 업그레이드에 보안 기준 개선 .....	31
10장. 문제 해결 .....	34
10.1. 리소스 문제 해결 .....	34
10.2. 문제 해결 팁 .....	34
10.3. 확인된 문제 .....	36
10.4. 지원 받기 .....	40
11장. 관련 정보 .....	41
부록 A. RHEL 7 리포지토리 .....	42
부록 B. RHEL 8 리포지토리 .....	43
부록 C. RHEL 8의 암호화 키 위치 .....	45



## RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

### Jira를 통해 피드백 제출 (등록 필요)

1. [Jira](#) 웹 사이트에 로그인합니다.
2. 상단 탐색 모음에서 **생성** 을 클릭합니다.
3. **요약** 필드에 설명 제목을 입력합니다.
4. **설명** 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

## 주요 마이그레이션 용어

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

### 업데이트

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 교체하는 것입니다. 일반적으로 Red Hat의 지침에 따라 데이터를 백업하십시오. RHEL을 업그레이드할 때 다음 두 가지 옵션이 있습니다.

- **인플레이스(In-Place) 업그레이드:** 인플레이스 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.
- **새로 설치:** 새로 설치하면 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 전환

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 전환하는 것은 마이그레이션입니다. 한 컴퓨터에서 다른 노트북으로 또는 한 서버에서 다른 서버로 사용자를 이동하는 것은 마이그레이션입니다. 그러나 대부분의 마이그레이션에는 업그레이드가 수반되며 때로는 이 용어가 상호 교환적으로 사용됩니다.

- **RHEL로 마이그레이션:** 기존 운영 체제를 RHEL로 변환
- **RHEL 간 마이그레이션:** 한 버전의 RHEL에서 다른 RHEL 버전으로 업그레이드



## 1장. 지원되는 업그레이드 경로

인플레이스 업그레이드는 시스템의 RHEL 7 운영 체제(OS)를 RHEL 8 버전으로 대체합니다.

현재 RHEL 7에서 다음 대상 RHEL 8 마이너 버전으로의 인플레이스 업그레이드를 수행할 수 있습니다.

표 1.1. 지원되는 업그레이드 경로

시스템 구성	소스 OS 버전	대상 OS 버전
RHEL	RHEL 7.9	RHEL 8.8
		RHEL 8.10 (기본값)
RHEL with SAP HANA	RHEL 7.9	RHEL 8.8 (기본값)
		RHEL 8.10

지원되는 업그레이드 경로에 대한 자세한 내용은 [Red Hat Enterprise Linux의 지원되는 인플레이스 업그레이드 경로 및 인플레이스 업그레이드 지원 정책을](#) 참조하십시오.

## 2장. 업그레이드 프로세스 개요

RHEL 7에서 RHEL 8로의 인플레이스 업그레이드 프로세스는 다음과 같이 요약할 수 있습니다.

### 1. 업그레이드 계획

시스템 요구 사항 및 제한 사항을 검토합니다. 시스템이 인플레이스 업그레이드에 적합한 후보인지 또는 대신 RHEL 8을 새로 설치해야 하는지 확인합니다.

### 2. 업그레이드 준비

업그레이드 프로세스를 시작하기 전에 RHEL 7 시스템의 백업 생성을 포함하여 필요한 준비 단계를 완료합니다.

### 3. 업그레이드 전 보고서를 실행하고 검토

업그레이드 전 유틸리티를 실행하여 업그레이드 전에 해결해야 하는 잠재적인 문제를 요약하는 보고서를 생성합니다. 발견된 문제의 심각도 및 영향에 따라 문제를 해결하는 데 필요한 작업 양에 따라 다음 결과 중 하나를 진행합니다.

- 발견된 문제를 해결하고 권장 솔루션을 적용합니다. 업그레이드 전 유틸리티를 다시 실행하여 모든 심각한 문제가 해결되었는지 확인합니다. 시스템이 업그레이드를 준비하기 전에 업그레이드 전 보고서를 실행하고 발견된 문제를 여러 번 해결해야 할 수 있습니다.
- 인플레이스 업그레이드를 수행하는 대신 RHEL 8의 새로 설치로 전환합니다.

### 4. 인플레이스 업그레이드를 수행합니다.

RHEL 8로 업그레이드를 수행하고 업그레이드가 올바르게 완료되었는지 확인합니다. 업그레이드할 수 없는 문제가 발생하면 RHEL 7 백업으로 롤백하십시오.

### 5. 업그레이드 후 단계 수행

필요한 업그레이드 후 단계를 수행하여 RHEL 8 시스템이 올바르게 설정되었는지 확인합니다.

## 3장. 업그레이드 계획

인플레이스 업그레이드는 시스템을 다음 주요 RHEL로 업그레이드할 수 있는 권장 및 지원되는 방법입니다.

RHEL 8로 업그레이드하기 전에 다음을 고려하십시오.

- **운영 체제** - 운영 체제는 다음과 같은 조건에서 **Leapp** 유틸리티에 의해 업그레이드됩니다.
  - 64비트 Intel, IBM POWER 8(little endian) 및 64비트 IBM Z 아키텍처의 **RHEL 7.9** 가 64비트 Intel 아키텍처에 설치되어 있습니다.  
자세한 내용은 [Red Hat Enterprise Linux의 인플레이스 업그레이드 경로 지원](#) 을 참조하십시오.
  - RHEL 8의 최소 **하드웨어 요구 사항**을 충족합니다.
  - 최신 RHEL 7.9 및 대상 운영 체제(OS) 버전(예: RHEL 8.10) 콘텐츠에 액세스할 수 있습니다.  
자세한 내용은 [RHEL 7 시스템 업그레이드 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 행위를 생성해야 합니다(예: 애플리케이션 재구성 또는 특정 하드웨어 드라이버 설치). 자세한 내용은 [사용자 지정 및 타사 애플리케이션 마이그레이션 처리](#) 를 참조하십시오. Red Hat은 사용자 정의 서비스를 지원하지 않습니다.
- **보안** - 업그레이드하기 전에 이 측면을 평가하고 업그레이드 프로세스가 완료될 때 추가 단계를 수행해야 합니다. 특히 다음 사항을 고려하십시오.
  - 업그레이드하기 전에 시스템이 **RHEL 8의 보안 변경 사항** 을 준수하고 이해하는 데 필요한 보안 표준을 정의합니다.
  - 업그레이드 프로세스 중에 **Leapp** 유틸리티는 SELinux 모드를 허용으로 설정합니다.
  - 연방 정보 처리 표준 (FIPS) 모드에서 시스템의 인플레이스 업그레이드는 **Leapp** 에 의해 완전히 자동화 될 수 없습니다. 시나리오에서 **FIPS 모드에서** 실행되는 RHEL 7 시스템을 업그레이드해야 하는 경우 다음을 수행해야 합니다.



### 중요

모든 암호화 키가 FIPSECDHE 표준을 준수하도록 하려면 이미 배포된 시스템의 인플레이스 업그레이드를 수행하는 대신 **FIPS 모드에서 새 설치**를 시작합니다. 회사의 보안 정책이 이러한 대체 업그레이드 프로세스를 허용하는 경우에만 다음 단계를 사용하고 업그레이드된 시스템의 모든 암호화 키의 재생 및 평가를 보장할 수 있는 경우에만 다음 단계를 사용하십시오.

1. RHEL 7에서 **FIPS 모드**를 비활성화합니다.
2. **Leapp** 을 사용하여 시스템을 업그레이드합니다. 다른 인플레이스 업그레이드와 같이 사전 업그레이드, 업그레이드 후 지침을 따라야 합니다.
3. RHEL 8에서 FIPS 모드를 활성화합니다. 자세한 내용은 [RHEL 8 보안 강화 문서에서 시스템을 FIPS 모드로 전환](#)에서 참조하십시오.
4. 시스템에서 암호화 키를 다시 생성합니다. 자세한 내용은 [부록 C. RHEL 8의 암호화 키 위](#) [치를](#) 참조하십시오.

- 업그레이드가 완료되면 보안 정책을 다시 평가하고 다시 적용합니다. RHEL 8에서 업그레이드 또는 새로 도입된 보안 정책 적용에 대한 자세한 내용은 [보안 정책 적용](#)을 참조하십시오.
- **스토리지 및 파일 시스템** - 업그레이드하기 전에 항상 시스템을 백업합니다. 예를 들어 [Relax-and-Recover\(Rear\)](#) 유틸리티, [LVM 스냅샷](#), [RAID 분할](#) 또는 가상 시스템 스냅샷을 사용할 수 있습니다.



**참고**

파일 시스템 형식은 그대로 유지됩니다. 결과적으로 파일 시스템에는 원래 생성된 것과 동일한 제한 사항이 있습니다.

- **고가용성** - **고가용성** 애드온을 사용하는 경우 [RHEL 고가용성 또는 탄력적 스토리지 클러스터 지식 베이스](#)에 [소프트웨어 업데이트 적용 권장 사례](#)를 따르십시오.
- **다운타임** - 업그레이드 프로세스는 몇 분에서 몇 시간까지 걸릴 수 있습니다.
- **Satellite** - Satellite를 통해 호스트를 관리하는 경우 Satellite 웹 UI를 사용하여 RHEL 7에서 RHEL 8로 여러 호스트를 동시에 업그레이드할 수 있습니다. 자세한 내용은 [Upgrading Hosts to Next Major Red Hat Enterprise Linux 릴리스](#)를 참조하십시오.
- **SAP HANA** - SAP HANA를 사용하는 경우 대신 [SAP 환경을 RHEL 7에서 RHEL 8로 인플레이스 업그레이드하는 방법](#)을 따르십시오. SAP HANA를 사용하는 RHEL의 업그레이드 경로는 다를 수 있습니다.
- **RHEL for Real Time** - 실시간 시스템의 업그레이드가 지원됩니다.
- **Red Hat OpenStack Platform의 NFV(Network Functions Virtualization)실시간** - 실시간 시스템에서 업그레이드가 지원됩니다.
- **RHSC(Red Hat Software Collections)**- 인플레이스 업그레이드 중에 RHSC가 완전히 마이그레이션되지 않습니다. RHEL 8 패키지는 일반적으로 RHSC 패키지를 자동으로 대체하지만 사용자 지정 구성 및 데이터를 수동으로 마이그레이션하고 구성해야 합니다. 예를 들어 RHSC에서 데이터베이스를 설치한 경우 RHSC 패키지를 제거하는 동안 데이터 손실을 방지하기 위해 업그레이드 전에 모든 데이터를 덤프한 다음 시스템 업그레이드 후 필요에 따라 데이터를 복원해야 합니다. Red Hat Satellite 서버를 업그레이드할 때 프로젝트에 필요한 RHSC 패키지가 자동으로 마이그레이션됩니다.
- **Red Hat JBoss EAP(Enterprise Application Platform)**- RHEL 9로의 업그레이드에는 JBoss EAP가 지원되지 않습니다. 업그레이드 후 시스템에 JBoss EAP를 수동으로 설치하고 구성해야 합니다. 자세한 내용은 [leapp 유틸리티를 사용하여 Linux와 함께 Jboss EAP 및 websphere 서버의 내부 마이그레이션](#)을 참조하십시오.
- **퍼블릭 클라우드** - 인플레이스 업그레이드는 AWS(Amazon Web Services), Microsoft Azure 및 Google Cloud Platform에서만 [RHUI\(Red Hat Update Infrastructure\)](#) 를 사용하는 온디맨드 Pay-As-You-Go(PAYG) 인스턴스에 대해 지원됩니다. RHEL 서브스크립션 전에 Red Hat Subscription Manager(RHSM)를 사용하는 모든 퍼블릭 클라우드에서 Bring Your Own Subscription 인스턴스에 인플레이스 업그레이드도 지원됩니다.
- **언어** - 모든 **Leapp** 보고서, 로그 및 기타 생성된 문서는 언어 구성에 관계없이 영어로 제공됩니다.
- **부트로더** - 부트로더를 RHEL 7 또는 RHEL 8의 BIOS에서 UEFI로 전환할 수 없습니다. RHEL 7 시스템에서 BIOS를 사용하고 RHEL 8 시스템이 UEFI를 사용하려면 인플레이스 업그레이드 대신 RHEL 8의 새로운 설치를 수행합니다. 자세한 내용은 [BIOS 부팅을 사전 설치된 Red Hat Enterprise Linux 시스템에서 UEFI 부팅으로 전환할 수 있습니까?](#)에서 참조하십시오.
- **알려진 제한 사항** - **Leapp**의 알려진 제한 사항은 다음과 같습니다.

- 전체 디스크 또는 파티션 또는 파일 시스템 암호화는 현재 인플레이스 업그레이드를 대상으로 하는 시스템에서 사용할 수 없습니다.
- 이더넷 또는 Infiniband를 사용하는 네트워크 기반 다중 경로 및 네트워크 스토리지는 업그레이드에 지원되지 않습니다. 여기에는 FCoE를 사용하는 SAN 및 FC를 사용하는 SAN에서 부팅이 포함됩니다. FC를 사용하는 SAN이 지원됩니다.
- 현재 인플레이스 업그레이드는 Red Hat Update Infrastructure를 사용하지만 RHEL 서브스크립션에는 RHSM이 아닌 나머지 퍼블릭 클라우드의 온 디맨드 PAYG 인스턴스에 지원되지 않습니다.
- Ansible Tower를 포함한 Ansible 제품이 설치된 시스템에서는 인플레이스 업그레이드가 지원되지 않습니다. RHEL 8에서 RHEL 7 Ansible Tower 설치를 사용하려면 [How do I migrate my Ansible Automation Platform installation from one environment to another?](#)를 참조하십시오. 지식 베이스 솔루션.

알려진 문제를 참조하십시오.

**Red Hat Insights**를 사용하여 Insights에 등록된 시스템 중 RHEL 8에 대한 업그레이드 경로에 있는 시스템을 확인할 수 있습니다. 이렇게 하려면 Insights의 각 [권고 권장 사항](#)으로 이동하여 작업 드롭다운 메뉴에서 권장 사항을 활성화한 다음 영향을 받는 시스템 제목 아래 목록을 검사합니다. Advisor 권장 사항은 RHEL 7 마이너 버전만 고려하며 시스템에 대한 사전 업그레이드 평가를 수행하지 않습니다. [Advisor-service 권장 사항 개요](#)도 참조하십시오.

#### 추가 리소스

- [Leapp](#)을 사용하여 RHEL 업그레이드 수행을 위한 모범 사례 및 권장 사항
- [Leapp 업그레이드 FAQ \(Frequently Asked Questions\)](#)

## 4장. 업그레이드 준비

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

모든 시스템에서 **업그레이드를 위해 RHEL 7 시스템 준비**에 설명된 준비 단계를 수행해야 합니다. 또한 Satellite Server에 등록된 시스템에서 **업그레이드용 Satellite 등록 시스템 준비에 설명된 준비** 단계도 수행해야 합니다.

### 4.1. 업그레이드를 위한 RHEL 7 시스템 준비

다음 절차에서는 **Leapp** 유틸리티를 사용하여 RHEL 8로 인플레이스 업그레이드를 수행하기 전에 필요한 단계를 설명합니다.

업그레이드 프로세스 중에 Red Hat Subscription Manager를 사용하지 않으려는 경우 [Red Hat Subscription Manager 없이 RHEL 8로 업그레이드 지침](#)을 따르십시오.

#### 사전 요구 사항

- 시스템은 **업그레이드 계획**에 나열된 조건을 충족합니다.
- 이전에 RHEL 6에서 RHEL 7로 업그레이드한 경우 필요한 수동 후 업그레이드 단계를 모두 완료했습니다. 여기에는 RHEL 7 시스템의 GRUB2 부트로더로 수동 마이그레이션이 포함됩니다. 자세한 내용은 [GRUB Legacy에서 GRUB 2로 업그레이드](#)를 참조하십시오.

#### 절차

1. 선택 사항: [Leapp 지식 베이스를 사용하여 RHEL 업그레이드 수행에 대한 모범 사례 및 권장 사항](#)을 검토하십시오.
2. Red Hat Subscription Manager를 사용하여 시스템이 Red Hat CDN(Content Delivery Network) 또는 Red Hat Satellite에 성공적으로 등록되어 있는지 확인합니다.
3. 시스템이 Satellite Server에 등록된 경우 업그레이드를 위해 [Satellite 등록 시스템 준비 단계](#)를 완료하여 **시스템이 업그레이드 요구 사항을 충족하는지** 확인합니다.



#### 중요

시스템이 Satellite Server에 등록된 경우 문제가 발생하지 않도록 이 절차의 단계를 진행하기 전에 업그레이드에 사용할 [Satellite 등록 시스템 준비](#) 단계를 완료해야 합니다.

4. 선택 사항: 시스템 자체와 관련이 없는 데이터 파일만 포함하는 파일 시스템과 같이 업그레이드에 필요하지 않은 시스템 이외의 OS 파일 시스템을 마운트 해제하고 **/etc/fstab** 파일에서 주석 처리합니다. 이로 인해 업그레이드 프로세스에 필요한 시간을 줄이고 사용자 지정 또는 타사 행위자가 업그레이드하는 동안 제대로 마이그레이션되지 않는 타사 애플리케이션과 관련된 잠재적인 문제를 방지할 수 있습니다.
5. subscription-manager를 사용하여 시스템이 서브스크립션되었는지 확인합니다.
  - a. SCA([Simple Content Access](#))가 활성화된 계정을 사용하여 시스템을 등록한 경우 **Content Access Mode가 Simple Content Access** 메시지로 설정되어 있는지 확인합니다.

```
# subscription-manager status
```

```
+-----+
System Status Details
+-----+
Overall Status: Disabled
Content Access Mode is set to Simple Content Access. This host has access to content,
regardless of subscription status.
System Purpose Status: Disabled
```

- b. SCA가 비활성화된 계정을 사용하여 시스템을 등록한 경우 Red Hat Linux Server 서브스크립션이 연결되고 제품 이름이 **Server** 이고 상태가 **Subscribed** 인지 확인합니다.

```
# subscription-manager list --installed
+-----+
Installed Product Status
+-----+
Product Name: Red Hat Enterprise Linux Server
Product ID: 69
Version: 7.9
Arch: x86_64
Status: Subscribed
```

6. 적절한 리포지토리가 활성화되어 있는지 확인합니다. 다음 명령은 64비트 Intel 아키텍처용 리포지토리를 나열합니다. 다른 아키텍처의 경우 [RHEL 7 리포지토리](#)를 참조하십시오.

- a. 기본 리포지토리를 활성화합니다.

```
# subscription-manager repos --enable rhel-7-server-rpms
```

- b. **Leapp** 및 해당 종속 항목을 사용할 수 있는 추가 리포지토리를 활성화합니다.

```
# subscription-manager repos --enable rhel-7-server-extras-rpms
```



### 참고

선택적으로 선택적(CodeReady Linux Builder라고도 함) 또는 추가 리포지토리를 활성화할 수 있습니다. 리포지토리 ID에 대한 자세한 내용은 [RHEL 7 리포지토리의 선택적 및 추가 리포지토리 목록](#)을 참조하십시오. 이러한 리포지토리의 콘텐츠에 대한 자세한 내용은 [CodeReady Linux Builder 리포지토리 및 추가 리포지토리](#)를 참조하십시오.

7. 최신 RHEL 7 콘텐츠를 사용하도록 Red Hat Subscription Manager를 설정합니다.

```
# subscription-manager release --unset
```

8. 선택 사항: 사용자 지정 리포지토리를 사용하려면 사용자 [지정 리포지토리 지식베이스 구성](#) 문서를 참조하십시오.
9. **yum-plugin-versionlock** 플러그인을 사용하여 패키지를 특정 버전으로 잠그면 다음을 실행하여 잠금을 지웁니다.

```
# yum versionlock clear
```

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

10. 퍼블릭 클라우드에서 RHUI(Red Hat Update Infrastructure)를 사용하여 업그레이드하는 경우 필요한 RHUI 리포지토리를 활성화하고 필요한 RHUI 패키지를 설치하여 시스템을 업그레이드할 준비가 되었는지 확인합니다.

a. AWS의 경우:

```
# yum-config-manager --enable rhui-client-config-server-7
# yum-config-manager --enable rhel-7-server-rhui-extras-rpms
# yum -y install rh-amazon-rhui-client leapp-rhui-aws
```

b. Microsoft Azure의 경우:

```
# yum-config-manager --enable rhui-microsoft-azure-rhel7
# yum -y install rhui-azure-rhel7
# yum-config-manager --enable rhui-rhel-7-server-rhui-extras-rpms
# yum -y install leapp-rhui-azure
```



### 참고

Azure VM(가상 머신)을 마이너 릴리스에 고정된 경우 버전 잠금을 제거합니다. 자세한 내용은 [RHEL 7.x VM 비 EUS로 다시 전환](#)을 참조하십시오.

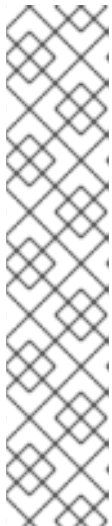
c. Google Cloud Platform의 경우 [GCP\(Google Cloud Platform\) 지식베이스용 Leapp RHUI 패키지](#)를 따르십시오.

11. Docker에서 컨테이너를 관리하는 경우 Podman을 사용하여 적절한 컨테이너 이미지로 컨테이너를 재생성한 다음 사용 중인 볼륨을 첨부합니다. 자세한 내용은 [How do I migrate my Docker containers to Podman prior to moving from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8?](#)에서 참조하십시오.

12. **Leapp** 유틸리티를 설치합니다.

```
# yum install leapp-upgrade
```

현재 **leapp-upgrade-el7toel8** RPM 패키지가 포함된 **leapp-repository** 패키지 버전 0.17.0 이상 및 버전 0.20.0 이상이 필요합니다.



### 참고

시스템이 인터넷에 액세스할 수 없는 경우 [Red Hat 고객 포털](#)에서 다음 패키지를 다운로드하십시오.

- **leapp**
- **leapp-deps**
- **python2-leapp**
- **leapp-upgrade-el7toel8**
- **Leapp-upgrade-el7toel8-deps** RHEL 7.9의 오프라인 시스템에 **leapp** 패키지를 설치하는 방법을 참조하십시오. 자세한 내용은 지식베이스 문서입니다.



13. 모든 패키지를 최신 RHEL 7 버전으로 업데이트하고 재부팅합니다.

```
# yum update
# reboot
```

14. **leapp-upgrade-el7toel8** 패키지의 최신 릴리스에는 필요한 모든 데이터 파일이 포함되어 있습니다. 이러한 데이터 파일을 이전 버전으로 교체한 경우 **/etc/leapp/files** 디렉터리의 모든 JSON 파일을 제거하고 **leapp-upgrade-el7toel8** 패키지를 다시 설치하여 데이터 파일이 최신 상태인지 확인합니다.
15. 안티바이러스 소프트웨어를 일시적으로 비활성화하여 업그레이드가 실패하지 않도록 합니다.
16. 구성 관리 시스템이 인플레이스 업그레이드 프로세스를 방해하지 않도록 합니다.
- **Puppet, Salt** 또는 **Chef**와 같은 클라이언트-서버 아키텍처와 함께 구성 관리 시스템을 사용하는 경우 **leapp preupgrade** 명령을 실행하기 전에 시스템을 비활성화합니다. 업그레이드 중 문제가 발생하지 않도록 업그레이드가 완료될 때까지 구성 관리 시스템을 활성화하지 마십시오.
  - **Ansible**과 같은 에이전트가 없는 아키텍처와 함께 구성 관리 시스템을 사용하는 경우, **RHEL 7에서 RHEL 8로의 업그레이드를 수행**하는데 설명된 대로 인플레이스 업그레이드 중에 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.
17. 시스템이 커널(**eth**)에서 사용하는 접두사를 기반으로 이름에 두 개 이상의 NIC(네트워크 인터페이스 카드)를 사용하지 않는지 확인합니다. RHEL 8으로 업그레이드하기 전에 다른 이름 지정 체계로 마이그레이션하는 방법에 대한 자세한 내용은 **RHEL 7에서 커널 NIC 이름을 사용하는 경우 RHEL 8으로 인플레이스 업그레이드를 수행하는 방법**을 참조하십시오.
18. ISO 이미지를 사용하여 업그레이드하는 경우 ISO 이미지에 대상 OS 버전(예: RHEL 8.8)이 포함되어 있는지 확인하고, **Leapp** 유틸리티가 업그레이드 프로세스 전체에서 이미지에 액세스할 수 있도록 영구 로컬 마운트 지점에 저장됩니다.
19. 전체 시스템 백업 또는 가상 머신 스냅샷이 있는지 확인합니다. 환경 내에서 표준 재해 복구 절차를 따르는 경우 시스템을 업그레이드 전 상태로 만들 수 있습니다. 다음 백업 옵션을 사용할 수 있습니다.
- **Relax-and-Recover(ReaR)** 유틸리티를 사용하여 시스템의 전체 백업을 생성합니다. 자세한 내용은 [ReaR 문서](#) 및 [What is Relax and Recover \(ReaR\) and how can I use it for disaster recovery?](#)에서 참조하십시오.
  - **LVM 스냅샷** 또는 **RAID 분할**을 사용하여 시스템의 스냅샷을 생성합니다. 가상 머신을 업그레이드하는 경우 전체 VM의 스냅샷을 생성할 수 있습니다. **Boom** 유틸리티를 사용하여 스냅샷 및 롤백 부팅 항목을 관리할 수도 있습니다. 자세한 내용은 **BOOM이란 무엇이며 설치하는 방법 및 스냅샷을 사용하여 시스템 업그레이드 관리를 참조**하십시오.

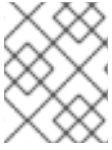


### 참고

LVM 스냅샷은 시스템의 전체 백업을 생성하지 않으므로 특정 업그레이드 실패 후 시스템을 복구하지 못할 수 있습니다. 따라서 ReaR 유틸리티를 사용하여 전체 백업을 생성하는 것이 더 안전합니다.

## 4.2. 업그레이드를 위한 **SATELLITE** 등록 시스템 준비

다음 절차에서는 RHEL 8으로의 업그레이드를 위해 Satellite에 등록된 시스템을 준비하는 데 필요한 단계를 설명합니다.



### 참고

Satellite 시스템 자체를 업그레이드하려는 경우 [Leapp](#) 을 사용하여 [Satellite](#) 또는 [Capsule](#) 에 설명된 절차를 [Red Hat Enterprise Linux 8 In-Place](#) 로 따르십시오.



### 중요

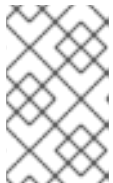
Satellite 시스템의 사용자는 이 절차와 [업그레이드를 위해 RHEL 7 시스템 준비](#) 에 설명된 준비 단계를 완료해야 합니다.

### 사전 요구 사항

- Satellite Server에 대한 관리 권한이 있습니다.

### 절차

1. Satellite가 완전 지원 버전 또는 유지 관리 지원 버전인지 확인합니다. 자세한 내용은 [Red Hat Satellite 제품 라이프 사이클](#)을 참조하십시오.
2. RHEL 8 리포지토리가 포함된 서브스크립션 매니페스트를 Satellite Server로 가져옵니다. 자세한 내용은 [Red Hat Satellite](#) 특정 버전에 대한 콘텐츠 관리 가이드의 Red Hat 서브스크립션 관리 장을 참조하십시오(예: [버전 6.12](#)).
3. Satellite Server의 필요한 모든 RHEL 7 및 RHEL 8 리포지토리를 RHEL 7.9의 최신 업데이트 및 대상 OS 버전(예: RHEL 8.10)과 동기화합니다. 필요한 리포지토리는 콘텐츠 보기에서 사용할 수 있어야 하며 관련 활성화 키로 활성화되어야 합니다.



### 참고

RHEL 8 리포지토리의 경우 각 리포지토리의 대상 OS 버전을 활성화합니다(예: 8.10). RHEL 8 버전의 리포지토리만 활성화하면 인플레이스 업그레이드가 금지됩니다.

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

- Red Hat Enterprise Linux 7 Server(RPM)  
rhel-7-server-rpms  
  
x86\_64 7Server
- Red Hat Enterprise Linux 7 Server - Extras(RPM)  
rhel-7-server-extras-rpms  
  
x86\_64
- Red Hat Enterprise Linux 8 for x86\_64 - AppStream(RPM)  
rhel-8-for-x86\_64-appstream-rpms

x86\_64 <target\_os\_version>

- Red Hat Enterprise Linux 8 for x86\_64 - BaseOS(RPM)  
rhel-8-for-x86\_64-baseos-rpms

x86\_64 <target\_os\_version>

target\_os\_version 을 대상 OS 버전(예: 8.10)으로 바꿉니다.

다른 아키텍처의 경우 [RHEL 7 리포지토리](#) 및 [RHEL 8 리포지토리](#)를 참조하십시오.

자세한 내용은 [Red Hat Satellite](#) 특정 버전에 대한 [콘텐츠 관리 가이드](#)의 콘텐츠 가져오기 장을 참조하십시오(예: [버전 6.12](#)).

4. 필수 RHEL 7 및 RHEL 8 리포지토리가 포함된 콘텐츠 뷰에 콘텐츠 호스트를 연결합니다.  
자세한 내용은 [Red Hat Satellite](#) 특정 버전에 대한 [콘텐츠 관리 가이드](#)의 콘텐츠 뷰 관리 장을 참조하십시오(예: [버전 6.12](#)).

## 검증

1. 올바른 RHEL 7 및 RHEL 8 리포지토리가 Satellite Server의 올바른 Content View에 추가되었는지 확인합니다.
  - a. Satellite 웹 UI에서 [콘텐츠 > 라이프사이클 > 콘텐츠 뷰](#)로 이동하여 콘텐츠 뷰의 이름을 클릭합니다.
  - b. **Repositories** (리포지토리) 탭을 클릭하고 리포지토리가 올바르게 표시되는지 확인합니다.



### 참고

다음 명령을 사용하여 리포지토리가 콘텐츠 뷰에 추가되었는지 확인할 수도 있습니다.

```
# hammer repository list --search 'content_label ~ rhel-7' --content-view
<content_view_name> --organization <organization> --lifecycle-
environment <lifecycle_environment>
# hammer repository list --search 'content_label ~ rhel-8' --content-view
<content_view_name> --organization <organization> --lifecycle-
environment <lifecycle_environment>
```

< content\_view\_name >을 콘텐츠 뷰의 이름으로, < organization >을 조직으로, < lifecycle\_environment >를 라이프사이클 환경의 이름으로 바꿉니다.

2. 콘텐츠 뷰와 연결된 활성화 키에서 올바른 RHEL 8 리포지토리가 활성화되어 있는지 확인합니다.
  - a. Satellite 웹 UI에서 [콘텐츠 > 라이프사이클 > 활성화키](#)로 이동하여 활성화 키 이름을 클릭합니다.
  - b. **Repository Sets** 탭을 클릭하고 필요한 리포지토리의 상태가 **Enabled** 인지 확인합니다.
3. 예상되는 모든 RHEL 7 리포지토리가 호스트에서 활성화되었는지 확인합니다. 예를 들면 다음과 같습니다.

```
# subscription-manager repos --list-enabled | grep "^Repo ID"  
Repo ID: rhel-7-server-extras-rpms  
Repo ID: rhel-7-server-rpm
```

## 5장. 업그레이드 전 보고서 검토

시스템의 upgradability를 평가하려면 **leapp preupgrade** 명령을 사용하여 사전 업그레이드 프로세스를 시작합니다. 이 단계에서 **Leapp** 유틸리티는 시스템에 대한 데이터를 수집하고 업그레이드 가능성을 평가하고 업그레이드 전 보고서를 생성합니다. 사전 업그레이드 보고서는 잠재적인 문제를 요약하고 권장 솔루션을 제안합니다. 이 보고서는 또한 업그레이드를 진행할 수 있는지 여부를 결정하는 데 도움이 됩니다.



### 참고

업그레이드 전 평가는 시스템 구성을 수정하지 않지만 **/var/lib/leapp** 디렉터리에서 필요하지 않은 공간을 사용합니다. 대부분의 경우 업그레이드 전 평가에는 최대 4GB의 공간이 필요하지만 실제 크기는 시스템 구성에 따라 다릅니다. 호스팅 파일 시스템에 공간이 충분하지 않으면 업그레이드 전 보고서에 분석의 전체 결과가 표시되지 않을 수 있습니다. 문제를 방지하려면 시스템에 **/var/lib/leapp** 디렉터리에 충분한 공간이 있는지 확인하거나 공간 소비가 시스템의 다른 부분에 영향을 미치지 않도록 디렉터를 전용 파티션으로 이동하십시오.



### 중요

보고서가 업그레이드에 억제 없는 경우에도 항상 전체 업그레이드 전 보고서를 검토합니다. 사전 업그레이드 보고서에는 업그레이드 전에 완료해야 하는 권장 작업이 포함되어 업그레이드된 시스템이 제대로 작동하는지 확인할 수 있습니다.

내부 업그레이드 프로세스 대신 RHEL 8 시스템을 새로 설치하려는 경우 사전 업그레이드 보고서 검토도 유용할 수 있습니다.

다음 방법 중 하나를 사용하여 사전 업그레이드 단계에서 업그레이드 가능성을 평가할 수 있습니다.

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



### 참고

예를 들어 사용자 지정 스크립트를 사용하여 사전 업그레이드 보고서를 처리하여 다양한 환경에서 여러 보고서의 결과를 비교할 수 있습니다. 자세한 내용은 [Red Hat Enterprise Linux 사전 업그레이드 보고서 워크플로 자동화](#)를 참조하십시오.



### 중요

사전 업그레이드 보고서는 전체 인플레이스 업그레이드 프로세스를 시뮬레이션할 수 없으므로 시스템과 관련된 모든 억제 문제를 식별할 수 없습니다. 결과적으로 보고서의 모든 문제를 검토하고 수정한 후에도 인플레이스 업그레이드가 계속 종료될 수 있습니다. 예를 들어 사전 업그레이드 보고서는 손상된 패키지 다운로드와 관련된 문제를 감지할 수 없습니다.

### 5.1. 명령줄에서 업그레이드 가능성 평가

명령줄 인터페이스를 사용하여 사전 업그레이드 단계에서 잠재적인 업그레이드 문제를 식별합니다.

#### 사전 요구 사항

- 업그레이드 준비에 나열된 단계가 완료되었습니다.

## 절차

1. RHEL 7 시스템에서 사전 업그레이드 단계를 수행합니다.

```
# leapp preupgrade --target <target_os_version>
```

<target\_os\_version>을 대상 OS 버전(예: 8.10)으로 바꿉니다. 대상 OS 버전이 정의되지 않은 경우 **Leapp**은 지원되는 업그레이드 경로 의 테이블 1.1에 지정된 기본 대상 OS 버전을 사용합니다.

- 업그레이드에 `/etc/yum.repos.d/` 디렉터리에서 사용자 지정 리포지토리를 사용하는 경우 다음과 같이 선택한 리포지토리를 활성화합니다.

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

- RHSM없이 업그레이드 하거나 RHUI를 사용하는 경우 `--no-rhsm` 옵션을 추가합니다.
  - EUS (Extended Upgrade Support), Advanced Update Support (AUS) 또는 Update Services for SAP Solutions (E4S) 서브스크립션이 있는 경우 `--channel <channel>` 옵션을 추가합니다.
    - RHEL 8.8로 업그레이드하는 경우 채널을 채널 이름(예: **eus,aus** 또는 **e4s**)으로 바꿉니다. SAP HANA 고객은 [How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 가이드](#)를 사용하여 인플레이스 업그레이드를 수행해야 합니다.
    - RHEL 8.10으로 업그레이드하는 경우 채널을 **ga**로 바꿉니다.
2. `/var/log/leapp/leapp-report.txt` 파일에서 보고서를 검사하고 보고된 모든 문제를 수동으로 해결합니다. 보고된 일부 문제에는 수정 제안 사항이 포함되어 있습니다. **억제** 문제로 인해 해결될 때까지 업그레이드할 수 없습니다. 보고서에 나타나는 다양한 문제에 대한 자세한 내용은 [How do I upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8](#)에서 참조하십시오. 보고서에는 다음과 같은 위험 요소 수준이 포함되어 있습니다.

### 높음

시스템 상태가 저하될 가능성이 매우 높습니다.

### 중간

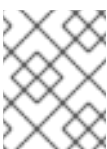
시스템과 애플리케이션 모두에 영향을 미칠 수 있습니다.

### 낮음 (LOW)

시스템에 영향을 주지 않지만 애플리케이션에 영향을 줄 수 있어야 합니다.

### 정보

시스템 또는 애플리케이션에 대한 예상 영향 없이 정보를 제공합니다.



### 참고

발견된 문제의 심각도 및 영향에 따라 인플레이스 업그레이드를 수행하는 대신 RHEL 8의 새로 설치를 수행하는 것이 좋습니다.

3. 특정 시스템 구성에서 **Leapp** 유틸리티는 수동으로 응답해야 하는 true 또는 false 질문을 생성합니다. 사전 업그레이드 보고서에 응답 파일 메시지에 **Missing 필수 응답이 포함된 경우** 다음 단계를 완료합니다.
  - a. `/var/log/leapp/answerfile` 파일을 열고 true 또는 false 질문을 검토합니다.
  - b. `/var/log/leapp/answerfile` 파일을 수동으로 편집하고, # 기호를 삭제하여 파일의 confirm 줄의 주석을 제거하고, 응답을 **True** 또는 **False** 로 확인합니다. 자세한 내용은 [Leapp answerfile](#) 을 참조하십시오.



#### 참고

또는 다음 명령을 실행하여 true 또는 false 질문에 응답할 수 있습니다.

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

예를 들어 PAM 구성에서 `pam_pkcs11` 모듈을 비활성화하시겠습니까?라는 질문에 대한 **False** 응답을 확인하려면 다음 명령을 실행합니다.

```
# leapp answer --section
remove_pam_pkcs11_module_check.confirm=False
```

4. 이전 단계를 반복하여 pre-upgrade 보고서를 다시 실행하여 모든 중요한 문제를 해결했는지 확인합니다.

## 5.2. 웹 콘솔을 통해 업그레이드 가능성 평가 및 자동 복구 적용

사전 업그레이드 단계에서 잠재적인 문제를 식별하고 웹 콘솔을 사용하여 자동화된 수정을 적용합니다.

### 사전 요구 사항

- 업그레이드 준비 단계에 나열된 단계를 완료했습니다.

### 절차

1. **cockpit-leapp** 플러그인을 설치합니다.

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

웹 콘솔에 **root** 로 로그인하거나 **sudo** 로 관리 명령을 입력할 수 있는 권한이 있는 사용자로 로그인합니다. 웹 콘솔에 대한 자세한 내용은 [RHEL 웹 콘솔을 사용하여 시스템 관리](#) 를 참조하십시오.

2. RHEL 7 시스템에서 명령줄 인터페이스 또는 웹 콘솔 터미널에서 사전 업그레이드 단계를 수행합니다.

```
# leapp preupgrade --target <target_os_version>
```

<target\_os\_version >을 대상 OS 버전(예: 8.10)으로 바꿉니다. 대상 OS 버전이 정의되지 않은 경우 **Leapp** 은 지원되는 업그레이드 경로 의 테이블.1에 지정된 기본 대상 OS 버전을 사용합니다.

- 업그레이드에 `/etc/yum.repos.d/` 디렉터리에서 사용자 지정 리포지토리를 사용하는 경우 다음과 같이 선택한 리포지토리를 활성화합니다.



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

- **RHSM 없이 업그레이드** 하거나 RHUI를 사용하는 경우 **--no-rhsm** 옵션을 추가합니다.
  - **EUS (Extended Upgrade Support), Advanced Update Support (AUS)** 또는 **Update Services for SAP Solutions (E4S)** 서브스크립션이 있는 경우 **--channel <channel>** 옵션을 추가합니다.
    - RHEL 8.8로 업그레이드하는 경우 채널을 채널 이름(예: **eus, aus** 또는 **e4s**)으로 바꿉니다. SAP HANA 고객은 [How to in-place upgrade SAP environments from RHEL 7 to RHEL 8 가이드](#)를 사용하여 인플레이스 업그레이드를 수행해야 합니다.
    - RHEL 8.10으로 업그레이드하는 경우 채널을 **ga** 로 바꿉니다.
3. 웹 콘솔의 탐색 메뉴에서 **Upgrade Report** 를 선택하여 보고된 모든 문제를 검토합니다. **역제** 문제로 인해 해결될 때까지 업그레이드할 수 없습니다. 보고서에 나타나는 다양한 문제에 대한 자세한 내용은 [How do I upgrade from Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8](#) 에서 참조하십시오.
- 문제를 자세히 보려면 세부 정보 창을 열 행을 선택합니다.

그림 5.1. 웹 콘솔의 인플레이스 업그레이드 보고서

Upgrade Report for: leapp-20230320120729

Title	Risk Factor	Description	Tags	Time
Packages available in excluded repositories will not be installed	High		repository	20.03.2023 12:53:16
Difference in Python versions and support in RHEL 8	High	Remediation hint Links	python	20.03.2023 12:53:16
Upgrade is unsupported	High		upgrade process, sanity	20.03.2023 12:53:17
Packages not signed by Red Hat found on the system	High		sanity	20.03.2023 12:53:18
GRUB core will be updated during upgrade	High		boot	20.03.2023 12:53:19
Missing required answers in the answer file	High	Inhibitor Remediation hint Remediation command		20.03.2023 12:54:45
chrony using default configuration	Medium		services, time management	20.03.2023 12:53:17
Grep has incompatible changes in the next major version	Low	Remediation hint	tools	20.03.2023 12:53:16
SELinux will be set to permissive mode	Low	Remediation hint	selinux, security	20.03.2023 12:53:16
Dosfstools incompatible changes in the next major version	Low	Remediation hint	filesystem, tools	20.03.2023 12:53:18
Postfix has incompatible changes in the next major version	Low		services, email	20.03.2023 12:53:20
The subscription-manager release is going to be kept as it is during the upgrade	Low	Remediation hint	upgrade process	20.03.2023 12:54:45
Excluded target system repositories		Remediation hint	repository	20.03.2023 12:53:14
SELinux relabeling will be scheduled			selinux, security	20.03.2023 12:53:16
Current PAM and nsswitch.conf configuration will be kept.			authentication, security, tools	20.03.2023 12:53:19

30 per page 1-15 of 15 1 of 1

보고서에는 다음과 같은 위험 요소 수준이 포함되어 있습니다.

**높음**

시스템 상태가 저하될 가능성이 매우 높습니다.

**중간**

시스템과 애플리케이션 모두에 영향을 미칠 수 있습니다.

**낮음 (LOW)**

시스템에 영향을 주지 않지만 애플리케이션에 영향을 줄 수 있어야 합니다.

**정보**

시스템 또는 애플리케이션에 대한 예상 영향 없이 정보를 제공합니다.





### 참고

발견된 문제의 심각도 및 영향에 따라 인플레이스 업그레이드를 수행하는 대신 RHEL 8의 새로 설치를 수행하는 것이 좋습니다.

4. 특정 구성에서 **Leapp** 유틸리티는 수동으로 응답해야 하는 **true** 또는 **false** 질문을 생성합니다. 업그레이드 보고서에 응답 **파일 행에 Missing 필수 응답이 포함된** 경우 다음 단계를 완료하십시오.
  - a. 응답 **파일 행에서 Missing 필수 답변을** 선택하여 세부 정보 창 을 엽니다. 기본 답변은 수정 명령 끝에 표시됩니다.
  - b. 기본 응답을 확인하려면 **Add to Remediation Plan** (해결 계획에 추가) 을 선택하여 나중에 수정을 실행하거나 **Remediation을 실행하여** 즉시 수정을 실행합니다.
  - c. 대신 기본이 아닌 답변을 선택하려면 터미널에서 **leapp answer** 명령을 실행하여 응답하려는 질문을 지정하고 확인된 답변을 지정합니다.

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

예를 들어, **PAM** 구성에서 **Disableovn\_pkcs11** 모듈에 대한 **False** 응답을 확인하려면 다음 명령을 실행합니다.

```
# leapp answer --section remove_pam_pkcs11_module_check.confirm=False
```

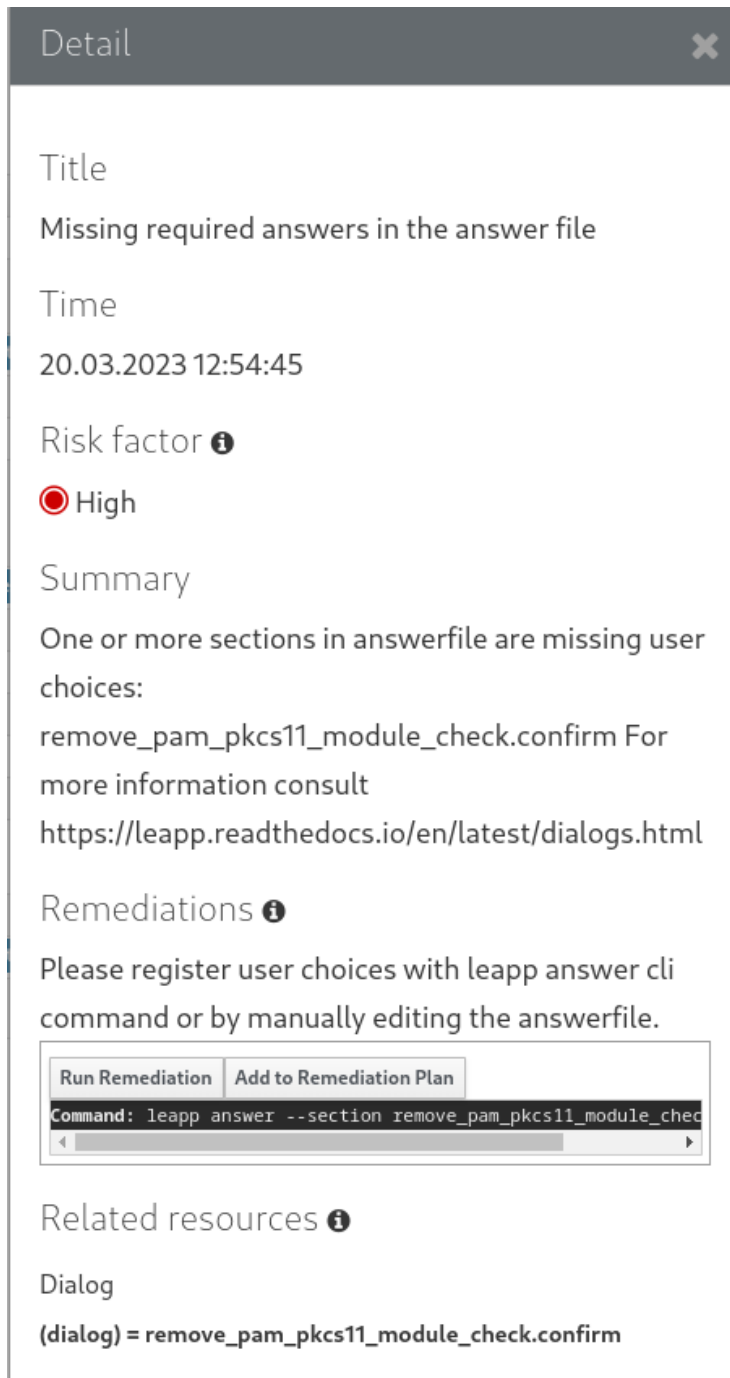


### 참고

**/var/log/leapp/answerfile** 파일을 수동으로 편집하고, **#** 기호를 삭제하여 파일의 확인 줄의 주석을 제거하고, 답변을 **True** 또는 **False** 로 확인할 수도 있습니다. 자세한 내용은 [Leapp answerfile 예제](#) 를 참조하십시오.

5. 일부 문제에는 문제를 자동으로 해결하기 위해 실행할 수 있는 해결 명령이 있습니다. 수정 명령에서 개별적으로 또는 모두 수정 명령을 실행할 수 있습니다.
  - a. 단일 수정 명령을 실행하려면 문제에 대한 **세부 정보** 창을 열고 **Run Remediation** 을 클릭합니다.
  - b. 수정 계획에 수정 명령을 추가하려면 문제에 대한 세부 정보 창 을 열고 **Add to Remediation Plan** 을 클릭합니다.

그림 5.2. 세부 정보 창



- c. 추가된 모든 수정 명령이 포함된 수정 계획을 실행하려면 보고서 오른쪽 상단에 있는 **Remediation plan** 링크를 클릭합니다. 나열된 모든 명령을 실행하려면 검사 계획 실행을 클릭합니다.
6. 보고서를 검토하고 보고된 모든 문제를 해결한 후 3-7 단계를 반복하여 보고서를 다시 실행하여 모든 중요한 문제를 해결했는지 확인합니다.

## 6 장. RHEL 7에서 RHEL 8로의 업그레이드 수행

**Leapp** 유틸리티를 사용하여 RHEL 8로 업그레이드합니다.

### 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 7 시스템에서 업그레이드 프로세스를 시작합니다.

```
# leapp upgrade --target <target_os_version>
```

<target\_os\_version>을 대상 운영 체제(OS) 버전으로 바꿉니다(예: 8.10). 대상 OS 버전이 정의되지 않은 경우 **Leapp**은 지원되는 업그레이드 경로 의 테이블.1에 지정된 기본 대상 OS 버전을 사용합니다.

### 참고

업그레이드에 **/etc/yum.repos.d/** 디렉터리에서 사용자 지정 리포지토리를 사용하는 경우 다음과 같이 선택한 리포지토리를 활성화합니다.

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

**RHSM 없이 업그레이드** 하거나 RHUI를 사용하는 경우 **--no-rhsm** 옵션을 추가합니다.

ISO 이미지를 사용하여 업그레이드하는 경우 **--no-rhsm** 및 **--iso <file\_path>** 옵션을 추가합니다. <file\_path>를 저장된 ISO 이미지의 파일 경로(예: **/home/rhel8.iso**)로 바꿉니다.

**EUS (Extended Upgrade Support), Advanced Update Support (AUS)** 또는 **Update Services for SAP Solutions (E4S)** 서브스크립션이 있는 경우 **--channel <channel>** 옵션을 추가합니다.

- RHEL 8.8로 업그레이드하는 경우 channel 을 **leapp preupgrade** 명령과 함께 사용한 값으로 교체합니다(예: **eus,aus, e4s**). **leapp preupgrade** 및 **leapp upgrade** 명령 모두에서 **--channel** 옵션과 함께 동일한 값을 사용해야 합니다.
- RHEL 8.10으로 업그레이드하는 경우 채널을 **ga** 로 바꿉니다.

업그레이드 프로세스 시작 시 **Leapp**은 사전 업그레이드 보고서 검토에 설명된 사전 업그레이드 단계를 수행합니다.

시스템을 업그레이드할 수 있는 경우 **Leapp**은 필요한 데이터를 다운로드하고 업그레이드를 위해 RPM 트랜잭션을 준비합니다.

시스템이 안정적인 업그레이드의 매개변수를 충족하지 않는 경우 **Leapp**은 업그레이드 프로세스를 종료하고 문제를 설명하는 기록과 권장 솔루션을 **/var/log/leapp/leapp-report.txt** 파일로 제공합니다. 자세한 내용은 **문제 해결**을 참조하십시오.

2. 시스템을 수동으로 다시 시작하십시오.

```
# reboot
```

이 단계에서는 시스템은 RHEL 8 기반 초기 RAM 디스크 이미지 `initramfs`로 부팅됩니다. **LeApp**은 모든 패키지를 업그레이드하고 RHEL 8 시스템으로 자동으로 재부팅합니다.

또는 **--reboot** 옵션을 사용하여 **kubevirt upgrade** 명령을 입력하고 이 수동 단계를 건너뛸 수 있습니다.

오류가 발생하면 [문제 해결](#)에 설명된 대로 로그를 조사합니다.

3. RHEL 8 시스템에 로그인하고 [RHEL 8 시스템 업그레이드 후 상태 확인](#)에 설명된 대로 상태를 확인합니다.
4. 업그레이드 보고서 및 업그레이드 후 작업 수행에 설명된 모든 [업그레이드 후 작업을 수행합니다](#). 특히 보안 정책을 다시 평가 및 다시 적용합니다.
5. **FIPS 모드에서** 실행되고 있는 시스템을 업그레이드하는 경우 RHEL 7 커널을 제거합니다. 그런 다음, 다시 생성 및 그렇지 않으면 모든 암호화 키의 FIPS 컴플라이언스를 확인합니다. 자세한 내용은 [RHEL 8의 암호화 키 위치](#)를 참조하십시오.

## 7장. RHEL 8 시스템의 업그레이드 후 상태 확인

다음 절차에서는 RHEL 8으로 업그레이드한 후 수행하는 데 권장되는 확인 확인 목록입니다.

### 사전 요구 사항

- RHEL 7에서 RHEL 8로의 업그레이드 수행에 설명된 단계에 따라 시스템이 업그레이드되었으며 RHEL 8로 로그인할 수 있습니다.

### 절차

업그레이드가 완료되면 시스템에 필요한 상태를 확인합니다. 적어도 다음을 확인합니다.

- 현재 OS 버전이 Red Hat Enterprise Linux 8인지 확인합니다.

```
# cat /etc/redhat-release
Red Hat Enterprise Linux release <target_os_version> (Ootpa)
```

target\_os\_version 을 대상 OS 버전(예: 8.10)으로 바꿉니다.

- OS 커널 버전을 확인합니다.

```
# uname -r
4.18.0-305.el<target_os>.x86_64
```

target\_os 는 **8** 또는 대상 OS 버전이어야 합니다(예: **8\_10**). **.el8** 이 중요하며 버전이 4.18.0-305 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: <target_os_version>
Arch: x86_64
Status: Subscribed
```

target\_os\_version 을 대상 OS 버전(예: 8.10)으로 바꿉니다.

- 업그레이드 직후 릴리스 버전이 대상 OS 버전으로 설정되어 있는지 확인합니다.

```
# subscription-manager release
Release: <target_os_version>
```

target\_os\_version 을 대상 OS 버전(예: 8.10)으로 바꿉니다.

- 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 데이터베이스를 마이그레이션하려면 [RHEL 8 데이터베이스 서버 설명서](#)의 지침을 따르십시오.

## 8장. 업그레이드 후 작업 수행

RHEL 8로 인플레이스 업그레이드 후 다음 주요 작업이 권장됩니다.

### 사전 요구 사항

- RHEL 7에서 RHEL 8로의 업그레이드 수행에 설명된 단계에 따라 시스템을 업그레이드했으며 RHEL 8에 로그인할 수 있습니다.
- RHEL 8 시스템의 업그레이드 후 상태 확인에 설명된 단계에 따라 인플레이스 업그레이드의 상태를 확인했습니다.

### 절차

업그레이드를 수행한 후 다음 작업을 완료합니다.

1. **snactor** 패키지를 포함하여 **/etc/dnf/dnf.conf** 구성 파일의 **exclude** 목록에서 나머지 **Leapp** 패키지를 제거합니다. 인플레이스 업그레이드 중에 **Leapp** 유틸리티를 사용하여 설치된 **Leapp** 패키지가 자동으로 제외 목록에 추가되어 중요한 파일이 제거되거나 업데이트되지 않도록 합니다. 인플레이스 업그레이드 후 시스템에서 제거하기 전에 이 **Leapp** 패키지를 제외 목록에서 제거해야 합니다.
  - 제외 목록에서 패키지를 수동으로 제거하려면 **/etc/dnf/dnf.conf** 구성 파일을 편집하고 **exclude** 목록에서 원하는 **Leapp** 패키지를 제거합니다.
  - **exclude** 목록에서 모든 패키지를 제거하려면 다음을 수행합니다.

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

2. 나머지 **Leapp** 패키지가 포함된 나머지 RHEL 7 패키지를 제거합니다.

- a. 이전 커널 버전을 확인합니다.

```
# cd /lib/modules && ls -d *.el7*
```

- b. 이전 커널에서 약한 모듈을 제거합니다. 이전 커널이 여러 개 있는 경우 각 커널에 대해 다음 단계를 반복합니다.

```
# [ -x /usr/sbin/weak-modules ] && /usr/sbin/weak-modules --remove-kernel <version>
```

&lt;version>을 이전 단계에서 결정된 커널 버전으로 바꿉니다. 예를 들면 다음과 같습니다.

```
# [ -x /usr/sbin/weak-modules ] && /usr/sbin/weak-modules --remove-kernel 3.10.0-1160.25.1.el7.x86_64
```



### 참고

커널 패키지가 이전에 제거된 경우 생성되는 다음과 같은 오류 메시지를 무시합니다.

```
/usr/sbin/weak-modules: line 1081: cd: /lib/modules/<version>/weak-updates: No such file or directory
```

- c. 부트 로더 항목에서 이전 커널을 제거합니다. 오래된 커널이 여러 개 있는 경우 각 커널에 대해 이 단계를 반복합니다.

```
# /bin/kernel-install remove <version> /lib/modules/<version>/vmlinuz
```

version을 이전 단계에서 확인한 커널 버전으로 교체합니다. 예를 들면 다음과 같습니다.

```
# /bin/kernel-install remove 3.10.0-1160.25.1.el7.x86_64 /lib/modules/3.10.0-1160.25.1.el7.x86_64/vmlinuz
```

- d. 나머지 RHEL 7 패키지를 찾습니다.

```
# rpm -qa | grep -e '\.el[67]' | grep -vE '(gpg-pubkey|libmodulemd|katello-ca-consumer)' | sort
```

- e. RHEL 8 시스템에서 이전 커널 패키지를 포함한 나머지 RHEL 7 패키지 및 **kernel-workaround** 패키지를 제거합니다. RPM 종속 항목이 유지 관리되도록 하려면 이러한 작업을 수행할 때 **YUM** 또는 **DNF** 를 사용합니다. 수락하기 전에 트랜잭션을 검토하여 패키지가 의도하지 않게 제거되지 않았는지 확인합니다. 예를 들면 다음과 같습니다.

```
# yum remove kernel-workaround $(rpm -qa | grep \.el7 | grep -vE 'gpg-pubkey|libmodulemd|katello-ca-consumer')
```

- f. 나머지 **Leapp** 종속성 패키지를 제거합니다.

```
# yum remove leapp-deps-el8 leapp-repository-deps-el8
```

- g. 나머지 빈 디렉토리를 제거하십시오.

```
# rm -r /lib/modules/*el7*
```

3. 선택 사항: 시스템에서 나머지 업그레이드 관련 데이터를 모두 제거합니다.

```
# rm -rf /var/log/leapp /root/tmp_leapp_py3 /var/lib/leapp
```



### 중요

이 데이터를 제거하면 업그레이드 후 문제를 조사하고 해결하는 Red Hat 지원 기능이 제한될 수 있습니다.

4. RHEL 8에 패키지를 설치하거나 사용할 수 없는 YUM 리포지토리를 비활성화합니다. RHSM에서 관리하는 리포지토리는 자동으로 처리됩니다. 이러한 리포지토리를 비활성화하려면 다음을 수행합니다.

```
# yum config-manager --set-disabled <repository_id>
```

<repository\_id>를 리포지토리 ID로 바꿉니다.

5. 이전 복구 커널 및 초기 RAM 디스크를 현재 커널 및 디스크로 교체하십시오.

- a. 기존 복구 커널 및 초기 RAM 디스크를 제거합니다.



```
# rm /boot/vmlinuz-*rescue* /boot/initramfs-*rescue*
```

- b. rescue 커널 및 관련 초기 RAM 디스크를 다시 설치합니다.

```
# /usr/lib/kernel/install.d/51-dracut-rescue.install add "$(uname -r)" /boot "/boot/vmlinuz-$(uname -r)"
```



### 참고

시스템의 커널 패키지에 실시간 시스템과 같은 이름이 다른 경우 **kernel-core**를 올바른 패키지 이름으로 교체합니다.

- c. 시스템이 IBM Z 아키텍처에 있는 경우 `zipl` 부트로더를 업데이트합니다.

```
# zipl
```

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

### 검증

1. 이전 커널이 부트로더 항목에서 제거되었는지 확인합니다.

```
# grubby --info=ALL | grep "\.el7" || echo "Old kernels are not present in the bootloader."
```

2. 이전에 제거된 복구 커널 및 복구 초기 RAM 디스크 파일이 현재 커널에 대해 생성되었는지 확인합니다.

```
# ls /boot/vmlinuz-*rescue* /boot/initramfs-*rescue*
# lsinitrd /boot/initramfs-*rescue*.img | grep -qm1 "$(uname -r)/kernel/" && echo "OK" || echo "FAIL"
```

3. 복구 부팅 항목이 기존 복구 파일을 참조하는지 확인합니다. `grubby` 출력을 참조하십시오.

```
# grubby --info $(ls /boot/vmlinuz-*rescue*)
```

## 9장. 보안 정책 적용

인플레이스 업그레이드 프로세스 중에 특정 보안 정책을 비활성화 상태로 유지해야 합니다. 또한 RHEL 8에서는 시스템 전체 암호화 정책의 새로운 개념을 도입하고 보안 프로필에 주요 릴리스 간의 변경 사항이 포함될 수 있습니다. 시스템을 보다 안전하게 보호하려면 SELinux를 강제 모드로 전환하고 시스템 전체 암호화 정책을 설정합니다. 특정 보안 프로필을 준수하도록 시스템을 수정하고자 할 수도 있습니다.

### 9.1. 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 8 시스템의 후 업그레이드 상태 확인에 설명된 확인을 수행했습니다.

#### 절차

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

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

이전 단계에서는 가장 일반적인 시나리오만 처리됩니다. 가능한 모든 SELinux 거부를 확인하려면 전체 절차를 제공하는 SELinux 사용의 [SELinux 거부 확인](#) 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

## 9.2. 시스템 전체 암호화 정책 설정

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

설치 또는 인플레이스 업그레이드 프로세스가 완료되면 시스템 전체 암호화 정책이 자동으로 **DEFAULT** 로 설정됩니다. **DEFAULT** 시스템 전체 암호화 정책 수준은 현재 위협 모델에 대한 보안 설정을 제공합니다.

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
```

시스템 전체 암호화 정책을 사용자 지정할 수도 있습니다. 자세한 내용은 [하위 정책을 사용하여 시스템 전체 암호화 정책 사용자 지정 및 사용자 지정 시스템 전체 암호화 정책 생성 및 설정을 참조하십시오.](#)

## 추가 리소스

- 시스템 전체 암호화 정책 사용
- 시스템의 `update-crypto-policies(8)` 도움말 페이지.

## 9.3. 시스템 업그레이드에 보안 기준 개선

RHEL 8으로 업그레이드한 후 완전히 강화된 시스템을 얻으려면 OpenSCAP 제품군에서 제공하는 자동화된 수정을 사용할 수 있습니다. OpenSCAP 수정을 통해 PCI-DSS, OSPP 또는 ACSC Eight와 같은 보안 기준선에 맞게 시스템을 조정합니다. 구성 규정 준수 권장 사항은 보안 제품의 진화로 인해 Red Hat Enterprise Linux의 주요 버전마다 다릅니다.

강화된 RHEL 7 시스템을 업그레이드할 때 **Leapp** 툴은 완전한 강화를 유지할 수 있는 직접 방법을 제공하지 않습니다. 구성 요소 구성의 변경 사항에 따라 업그레이드 중 RHEL 8의 권장 사항과 다를 수 있습니다.



### 참고

RHEL 7 및 RHEL 8을 스캔하는 데 동일한 SCAP 콘텐츠를 사용할 수 없습니다. 시스템 규정 준수가 Red Hat Satellite 또는 Red Hat Insights와 같은 툴에 의해 관리되는 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 대한 시스템 검사](#)를 참조하십시오.

절차에 따라 PCI-DSS 프로파일로 시스템을 자동으로 강화합니다.



### 중요

자동 수정은 기본 구성에서 RHEL 시스템을 지원합니다. 설치 후 시스템 업그레이드가 변경 되었으므로 실행 중인 수정을 통해 필요한 보안 프로필을 완전히 준수하지 못할 수 있습니다. 일부 요구 사항을 수동으로 수정해야 할 수도 있습니다.

### 사전 요구 사항

- **scap-security-guide** 패키지는 RHEL 8 시스템에 설치됩니다.

### 절차

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

```
$ ls /usr/share/xml/scap/ssg/content/
ssg-firefox-cpe-dictionary.xml  ssg-rhel6-ocil.xml
ssg-firefox-cpe-oval.xml      ssg-rhel6-oval.xml
...
ssg-rhel6-ds-1.2.xml          ssg-rhel8-oval.xml
ssg-rhel8-ds.xml             ssg-rhel8-xccdf.xml
...
```

자세한 내용은 [규정 준수 프로필 보기](#) 를 참조하십시오.

2. 적절한 데이터 스트림에서 선택한 프로필에 따라 시스템을 교정합니다.

```
# oscap xccdf eval --profile pci-dss --remediate /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

**--profile** 인수의 **pci-dss** 값을 시스템 강화하려는 프로필 ID로 교체할 수 있습니다. RHEL 8에서 지원되는 전체 프로필 목록은 [RHEL에서 지원되는 SCAP 보안 프로필](#) 을 참조하십시오.



### 주의

Remediate 옵션을 사용하여 시스템 평가를 수행한 경우 신중하게 수행하지 않으면 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-rhel8-ds.xml
```

### 추가 리소스

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

## 10장. 문제 해결

다음 팁을 참조하여 RHEL 7에서 RHEL 8로의 업그레이드 문제를 해결할 수 있습니다.

### 10.1. 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 **leapp upgrade** 명령과 함께 **--verbose** 또는 **--debug** 옵션을 사용합니다.

- verbose 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 **leapp 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.

### 10.2. 문제 해결 팁

다음 문제 해결 팁을 참조할 수 있습니다.

#### 업그레이드 전 단계

- 시스템이 [업그레이드 계획](#)에 나열된 모든 조건을 충족하는지 확인하십시오.
- [업그레이드 준비](#)에 설명된 모든 단계, 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. 예제 질문:
  - PAM 구성에서 pam\_pkcs11 모듈을 비활성화합니다.
  - PAM 구성에서 pam\_krb5 모듈을 비활성화합니다.

- 다음 `authselect` 호출을 사용하여 PAM 및 `nsswitch.conf`를 구성합니다.
- `/var/log/leapp/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 10.1. Leapp 응답 파일

다음은 편집되지 않은 `/var/log/leapp/answerfile` 파일의 예입니다.

```
[remove_pam_pkcs11_module_check]
# Title:      None
# Reason:     Confirmation
# ===== remove_pam_pkcs11_module_check.confirm =====
# Label:      Disable pam_pkcs11 module in PAM configuration? If no, the upgrade process will
              be interrupted.
# Description: PAM module pam_pkcs11 is no longer available in RHEL-8 since it was replaced
              by SSSD.
# Type:       bool
# Default:    None
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
# confirm =
```

**Label** 필드는 대답이 필요한 질문을 지정합니다. 이 예에서 질문은 **PAM 구성에서 pam\_pkcs11 모듈을 비활성화합니까?**입니다.

질문에 답변하려면 **confirm** 행의 주석을 제거하고 **True** 또는 **False**에 대한 답변을 입력합니다. 이 예제에서 선택한 응답은 **True**입니다.

```
[remove_pam_pkcs11_module_check]
...
# Available choices: True/False
# Unanswered question. Uncomment the following line with your answer
confirm = 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/` 디렉터리는 비어 있거나 트랜잭션 디버그 데이터가 생성되지 않은 경우 존재하지 않습니다. 이는 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.

### 업그레이드 후 단계

- 시스템이 성공적으로 업그레이드되었지만 이전 RHEL 7 커널로 부팅된 것처럼 보이는 경우 시스템을 다시 시작하고 GRUB에서 기본 항목의 커널 버전을 확인합니다.
- **RHEL 8 시스템의 후 업그레이드 상태 확인** 에서 권장 단계를 수행했는지 확인하십시오.
- SELinux를 강제 모드로 전환한 후 애플리케이션 또는 서비스가 작동하지 않거나 잘못 작동하는 경우 **ausearch**, **journalctl** 또는 **dmesg** 유틸리티를 사용하여 서비스 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.

## 10.3. 확인된 문제

다음은 RHEL 7에서 RHEL 8로 업그레이드할 때 발생할 수 있는 알려진 문제입니다.

- NIC 터밍은 현재 Network Manager가 비활성화되거나 설치되지 않은 동안 인플레이스 업그레이드가 수행될 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 7 시스템에서 Red Hat에서 제공되지만 RHEL 8에서는 사용할 수 없는 장치 드라이버를 사용하는 경우 **Leapp** 은 업그레이드를 금지합니다. 그러나 RHEL 7 시스템에서 **Leapp** 이 `/etc/leapp/files/device_driver_deprecation_data.json` 파일에 대한 데이터가 없는 타사 장치 드라이버를 사용하는 경우 **Leapp** 은 이러한 드라이버를 감지하고 업그레이드를 진행하지 않습니다. 따라서 업그레이드 후 시스템을 부팅하지 못할 수 있습니다.
- **winbind** 및 **wins** Samba 모듈이 `/etc/nsswitch.conf` 파일에서 사용되는 경우 인플레이스 업그레이드를 수행할 수 없습니다. 업그레이드 트랜잭션은 다음 오류 메시지와 함께 실패하고 **Leapp** inhibits는 업그레이드에 실패합니다.

```
upgrade[469]: STDERR:
upgrade[469]: Error in PREIN scriptlet in rpm package unbound-libs
upgrade[469]: Error: Transaction failed
upgrade[469]: Container el8userspace failed with error code 1.
unbound-libs has a PREIN failure
```

이 문제를 해결하려면 업데이트 중에 **user**, **groups**, **hosts** 데이터베이스에 대해 로컬 공급자만 사용하도록 시스템을 구성합니다.

1. 시스템 `/etc/nsswitch.conf` 구성 파일을 열고 **winbind** 또는 **wins** 문자열이 포함된 항목을 검색합니다.



2. 이러한 항목을 찾으면 `/etc/nsswitch.conf`의 백업을 만듭니다.
  3. `/etc/nsswitch.conf`를 편집하고 `winbind` 또는 `wins`가 포함된 항목에서 `winbind`를 제거합니다.
  4. 인플레이스 업그레이드를 수행합니다.
  5. 업그레이드 후 `winbind`를 추가하고 시스템 구성 요구 사항에 따라 `/etc/nsswitch.conf`의 항목에 문자열을 이깁니다.  
(BZ#1410154)
- **Leapp** 유틸리티는 업그레이드 프로세스 중에 사용자 지정 인증 구성을 변경하지 않습니다. 더 이상 사용되지 않는 `authconfig` 유틸리티를 사용하여 RHEL 7 시스템에서 인증을 구성한 경우 RHEL 8에서 인증이 제대로 작동하지 않을 수 있습니다. RHEL 8 시스템에서 사용자 지정 구성이 제대로 작동하는지 확인하려면 `authselect` 유틸리티를 사용하여 RHEL 8 시스템을 다시 구성합니다.



### 중요

인플레이스 업그레이드 중에 더 이상 사용되지 않는 `pam_krb5` 또는 `pam_pkcs11` 플러그인 인증 모듈(PAM)이 제거됩니다. 결과적으로 RHEL 7 시스템의 PAM 구성에 `ECDHE_gradle b5` 또는 `ECDHE_pkcs11` 모듈이 포함되어 있고 이러한 모듈에 필수 또는 필수 제어 값이 있는 경우 인플레이스 업그레이드를 수행하면 시스템에서 잠길 수 있습니다. 이 문제를 해결하려면 업그레이드 프로세스를 시작하기 전에 `pam_krb5` 또는 `pam_pkcs11`을 사용하지 않도록 RHEL 7 시스템을 재구성하십시오.

- 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.
  - a. 타사 패키지 제거
  - b. 타사 패키지를 Red Hat에서 제공하는 패키지로 교체
- 보안상의 이유로 DES(Single DES) 및 트리플 DES (3DES) 암호화 유형에 대한 지원이 RHEL 8에서 제거되었습니다. RHEL 7 IdM(Identity Management)은 여전히 3DES 암호화를 지원합니다. RHEL 버전 모두 기본적으로 더 강력한 AES 암호화 유형을 선호하기 때문에 IdM 클라이언트를 업그레이드하거나 전체 IdM 환경을 RHEL 7에서 RHEL 8로 마이그레이션할 수 있습니다.

IdM 버전	기본 암호화 유형	지원되는 추가 암호화 유형
RHEL 7	<code>aes256-cts</code> <code>aes128-cts</code>	<code>camellia256-cts</code> <code>camellia128-cts</code> <code>des3-hmac</code> <code>arcfour-hmac</code>
RHEL 8	<code>aes256-cts</code> <code>aes128-cts</code>	<code>aes256-sha2</code> <code>aes128-sha2</code> <code>camellia256-cts</code> <code>camellia128-cts</code> <code>arcfour-hmac</code> <sup>[a]</sup>

IdM 버전	기본 암호화 유형	지원되는 추가 암호화 유형
<p>[a] RC4 암호화는 최신 AES-128 및 AES-256 암호화 유형보다 안전하지 않기 때문에 RHEL 8에서 기본적으로 사용되지 않으며 비활성화되어 있습니다. 기존 Active Directory 환경과의 호환성을 위해 RC4 지원을 활성화하는 방법에 대한 자세한 내용은 <a href="#">AD 및 RHEL의 공통 암호화 유형에 대한 지원</a>을 참조하십시오.</p>		

DES 또는 3DES 암호화 만 사용하도록 KDC(non-IdM Kerberos Distribution Center)를 수동으로 구성한 경우 다음과 같은 RHEL 8의 최신 Kerberos 패키지로 업데이트한 후 서비스 중단이 발생할 수 있습니다.

- Kerberos 인증 오류
- **unknown enctype** 암호화 오류
- DES로 암호화된 Database Master Keys(**K/M**)가 있는 KDC를 시작할 수 없습니다.

사용자 환경에서 DES 또는 3DES 암호화를 사용하지 않는 것이 좋습니다. 더 강력한 암호화 유형을 사용하도록 Kerberos 주체를 다시 입력하는 방법에 대한 자세한 내용은 MIT Kerberos 문서의 [Retiring DES](#)를 참조하십시오.

- 소프트웨어 RAID(Redundant Array of Independent Disks)가 있는 시스템에서 인플레이스 업그레이드가 실패할 수 있습니다. ([RHEL-3279](#))
- Puppet을 사용하는 시스템과 같은 GRUB 부트 로더 사양이 비활성화된 시스템은 최신 커널에 대해 새 initramfs를 생성할 수 없습니다. 이 문제를 해결하려면 [Chapter 6에 설명된 대로 부팅 로더 항목에서 패키지 및 이전 커널을 수동으로 제거합니다. 업그레이드 후 작업 실행.](#) ([BZ#1955099](#))
- Relax-and-Recover (ReaR) 유틸리티는 IBM Z 아키텍처에서 사용할 수 없습니다. 결과적으로 IBM Z 시스템은 OpenSCAP 제품군에 의해 완전히 수정될 수 없으며 보안 기준선을 완전히 준수하지 않을 수 있습니다. ([BZ#1958939](#))
- 인플레이스 업그레이드 중에 **Leapp** 유틸리티는 일반적으로 RHEL 7과 RHEL 8 간의 네트워크 인터페이스 컨트롤러(NIC) 이름을 유지합니다. 그러나 네트워크 본딩이 있는 시스템과 같은 일부 시스템에서는 NIC 이름을 RHEL 7과 RHEL 8 사이에서 업데이트해야 합니다. 해당 시스템에서 다음 단계를 수행합니다.
  - a. **Leapp** 유틸리티가 원래 RHEL 7 NIC 이름을 잘못 유지하지 않도록 **LEAPP\_NO\_NETWORK\_RENAMING=1** 환경 변수를 설정합니다.
  - b. 인플레이스 업그레이드를 수행합니다.
  - c. 네트워크가 올바르게 작동하는지 확인합니다. 필요한 경우 네트워크 구성을 수동으로 업데이트합니다. ([BZ#1919382](#))
- 인플레이스 업그레이드 후 시스템이 다음 조건을 충족하는 경우 SSH 키가 더 이상 자동으로 생성되지 않습니다.
  - 시스템이 클라우드에 있습니다.
  - cloud-init 패키지가 설치되어 있습니다.
  - ssh\_genkeytypes 구성은 기본값인 /etc/cloud/cloud.cfg 파일에서 ~로 설정됩니다.

이 문제로 인해 원래 키가 제거된 경우 시스템에서 SSH를 사용하여 연결할 수 없습니다. 이 문제를 방지하려면 템플릿을 RHEL 8.7 또는 9 지식 베이스 솔루션으로 업그레이드한 후 새 가상 머신에 SSH를 사용할 수 없습니다. (BZ#2210012)

- 하드웨어 수준 13에서 생성되어 UEFI로 부팅하는 VMware 가상 머신은 NVRAM 파일이 너무 작기 때문에 업그레이드 중에 문제가 발생할 수 있습니다. 이 문제 및 해결 방법에 대한 자세한 내용은 VMWare를 참조하십시오. efibootmgr 또는 mokutil 명령을 실행하여 항목을 추가할 때 "장치에 남은 공간 없음"을 가져옵니다. (RHEL-3362)
- ISO 이미지와 함께 RHUI를 사용하여 업그레이드하는 경우 업그레이드가 실패할 수 있습니다. 업그레이드와 함께 `--iso` 옵션을 사용하지 않거나 ISO를 사용하여 오프라인 Leapp 업그레이드 지침에 따라 'rhul-microsoft-azure-rhel8' 리포지토리 'rhul-microsoft-azure-rhel8'에 대한 캐시를 동기화하지 않고 이 리포지토리를 무시하고 이 문제를 해결할 수 있습니다. (RHEL-3296)

- 업그레이드 전 프로세스는 다음 오류 메시지와 함께 실패할 수 있습니다.

**mountError: failed to create mount target directory...**

이 문제가 발생하면 `LEAPP_OVL_IMG_FS_EXT4=1` 환경 변수를 내보냅니다. 자세한 내용은 MountError (OverlayFS + XFS ftype=1)를 사용하여 Leapp이 실패할 수 있습니다. (RHEL-3330)

- 파일 시스템이 너무 많은 경우 다음 오류 메시지와 함께 사전 업그레이드 프로세스가 실패할 수 있습니다.

**OperationalError: unable to open database file  
Cannot create XFS filesystem in ...**

이 문제가 발생하면 다음 단계를 완료합니다.

1. 시스템 파티션과 관련이 없고 업그레이드 프로세스 중에 필요하지 않은 파일 시스템을 마운트 해제합니다.
  2. 업그레이드 프로세스 중에 마운트되지 않도록 `/etc/fstab` 파일에서 마운트 해제된 파일 시스템의 항목을 주석 처리합니다.
  3. 업그레이드 후 원래 파일 시스템 구성을 복원합니다. (RHEL-3320)
- `/etc/sysconfig/kernel` 시스템 구성 파일이 시스템에 없는 경우 업그레이드가 실패하여 시스템이 손상됩니다. 이 문제를 방지하려면 예상 구성을 사용하여 파일을 수동으로 생성합니다. 자세한 내용은 부트 로더 확인을 참조하십시오. (RHEL-22306)
  - `/etc/fstab` 파일에 정의된 마운트된 파일 시스템에 공유 전파 플래그가 설정되지 않은 경우 업그레이드가 실패할 수 있습니다. 이 문제를 방지하려면 이러한 파일 시스템을 다시 마운트하여 공유로 설정합니다.

**# mount -o remount --make-shared <mountpoint>**

마운트 지점을 각 파일 시스템의 마운트 지점으로 바꿉니다.

자세한 내용은 DNF 트랜잭션 확인 중에 Leapp "RPM 파일을 로드할 수 없음"을 참조하십시오. (RHEL-23449)

- 업그레이드 프로세스에 제한된 리소스가 설정된 경우 업그레이드가 실패할 수 있습니다. 예를 들어, 열려 있는 파일의 최대 수와 프로세스에서 작성한 최대 파일 크기 및 해당 하위 속성이 설정된 경우 업그레이드 프로세스에서 도달할 수 있습니다. 이러한 문제를 방지하려면 업그레이드 프로세스 전에 이러한 제한을 늘리거나 제거하십시오. 자세한 내용은 `sqlite3.OperationalError: unable`

to open database file traceback 오류를 열 수 없는 이유와 [/var/lib/leapp/scratch/diskimages/root\\_boot가 필요한 이유](#)를 참조하십시오. (RHEL-16881, RHEL-26459)

- **jbcs-httpd24-brotli** RPM이 시스템에 설치된 경우(예: 시스템에서 JBoss Core Services Web Server를 사용하는 경우) 업그레이드가 실패할 수 있습니다. 이 문제를 방지하려면 업그레이드하기 전에 패키지를 제거하십시오. 또는 업그레이드 전에 패키지를 제거할 수 없는 경우 다음 명령을 실행하여 업그레이드 중에 **brotli** 패키지가 설치되었는지 확인합니다.

```
# echo brotli >> /etc/leapp/transaction/to_install
```

(RHEL-22542)

- IBM Z 머신의 RoCE와 같이 PCI 버스에 없는 네트워크 카드가 있는 시스템은 변경된 NIC 이름으로 인해 업그레이드 후 연결 손실이 발생할 수 있습니다. 이 문제를 방지하려면 업그레이드하기 전에 다음 단계를 완료합니다.

1. 커널 부팅 매개변수에 **net.ifnames=0** 을 추가합니다.

```
# grubby --update-kernel=ALL --args 'net.ifnames=0'
```

2. IBM Z 시스템에서 다음 명령을 입력하여 변경 사항을 적용합니다.

```
# zipl
```

3. 시스템을 재부팅합니다.

(RHEL-22371)

- RHEL 7 시스템에서 Red Hat에서 제공하지만 RHEL 8에서는 사용할 수 없는 장치 드라이버를 사용하는 경우 인플레이스 업그레이드 전에 드라이버를 언로드해야 합니다. 그러나 일부 장치 드라이버(예: **mptcl** 드라이버)가 다른 서비스에서 사용하는 경우 드라이버가 자동으로 다시 로드될 수 있습니다. 이 문제를 해결하려면 언로드할 수 없는 **mptctl** 모듈로 **IPU**가 억제됩니다. (RHEL-15894)
- RHUI를 사용하여 업그레이드하는 경우 **/usr/share/leapp-repository/repositories/system\_upgrade/common/files/rhui/** 디렉터리에 있는 파일이 업그레이드 전 보고서의 사용자 지정 파일로 잘못 보고됩니다. 이러한 파일을 수동으로 수정하지 않으면 보고서에서 이러한 파일에 대한 경고를 무시할 수 있으며 인플레이스 업그레이드에는 영향을 미치지 않습니다. (RHEL-40115)

## 10.4. 지원 받기

지원 케이스를 열려면 RHEL 7 을 제품으로 선택하고 시스템에서 **sosreport** 를 제공합니다.

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

```
# sosreport
```

케이스 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.

## 11장. 관련 정보

다음과 같은 자료를 참조할 수 있습니다.

- [Red Hat Enterprise Linux Infrastructure 업그레이드](#)
- [Red Hat Enterprise Linux 기술 기능 및 제한사항](#)
- [Red Hat Enterprise Linux에서 지원되는 인플레이스 업그레이드 경로](#)
- [인플레이스 업그레이드 지원 정책](#)
- [RHEL 8 도입의 고려 사항](#)
- [Red Hat Enterprise Linux 인플레이스 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 프로세스 자동화](#)
- [RHEL 6에서 RHEL 7으로 업그레이드](#)
- [RHEL 6에서 RHEL 8로 업그레이드](#)
- [Convert2RHEL 유틸리티를 사용하여 Linux 배포에서 RHEL로 변환](#)
- [Red Hat Satellite의 RHEL 7에서 RHEL 8로 호스트 업그레이드](#)
- [SAP 환경을 RHEL 7에서 RHEL 8로 인플레이스 업그레이드하는 방법](#)
- [Red Hat Insights 문서](#)
- [업그레이드 관련 지식 베이스 문서 및 솔루션](#)
- [Leapp을 사용하여 RHEL 업그레이드 수행을 위한 모범 사례 및 권장 사항](#)
- [Leapp 업그레이드 FAQ \(Frequently Asked Questions\)](#)
- [Red Hat Enterprise Linux Upgrade Helper](#)

## 부록 A. RHEL 7 리포지토리

업그레이드하기 전에 적절한 리포지토리가 업그레이드에 대해 [RHEL 7 시스템 준비 절차](#)의 4 단계에 설명된 대로 활성화되어 있는지 확인하십시오.

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

아키텍처	리포지토리	리포지토리 ID
64비트 Intel	Base	<b>rhel-7-server-rpms</b>
	Extras	<b>rhel-7-server-extras-rpms</b>
IBM POWER8 (little endian)	Base	<b>rhel-7-for-power-le-rpms</b>
	Extras	<b>rhel-7-for-power-le-extras-rpms</b>
IBM Z	Base	<b>rhel-7-for-system-z-rpms</b>
	Extras	<b>rhel-7-for-system-z-extras-rpms</b>

**subscription-manager repos --enable repository\_id** 명령을 사용하여 업그레이드하기 전에 다음 리포지토리를 활성화할 수 있습니다.

아키텍처	리포지토리	리포지토리 ID
64비트 Intel	선택 사항	<b>rhel-7-server-optional-rpms</b>
	Supplementary	<b>rhel-7-server-supplementary-rpms</b>
IBM POWER8 (little endian)	선택 사항	<b>rhel-7-for-power-le-optional-rpms</b>
	Supplementary	<b>rhel-7-for-power-le-supplementary-rpms</b>
IBM Z	선택 사항	<b>rhel-7-for-system-z-optional-rpms</b>
	Supplementary	<b>rhel-7-for-system-z-supplementary-rpms</b>



### 참고

인플레이스 업그레이드 전에 RHEL 7 Optional 또는 RHEL 7 Supplementary 리포지토리를 활성화한 경우 **Leapp** 은 [RHEL 8 CodeReady Linux Builder](#) 또는 [RHEL 8 Supplementary 리포지토리](#)를 각각 활성화합니다.

사용자 정의 리포지토리를 사용하려면 사용자 정의 리포지토리 구성의 지침에 따라 활성화합니다.

## 부록 B. RHEL 8 리포지토리

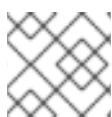
RHSM(Red Hat Subscription Manager)을 사용하여 시스템이 Red Hat CDN(Content Delivery Network)에 등록된 경우 인플레이스 업그레이드 중에 RHEL 8 리포지토리가 자동으로 활성화됩니다. 그러나 RHSM을 사용하여 Red Hat Satellite에 등록된 시스템에서는 업그레이드 전 보고서를 실행하기 전에 RHEL 7 및 RHEL 8 리포지토리를 모두 수동으로 활성화하고 동기화해야 합니다.



### 참고

각 리포지토리의 대상 운영 체제(OS) 버전을 활성화해야 합니다(예: RHEL 8.10). RHEL 8 버전의 리포지토리만 활성화한 경우 인플레이스 업그레이드가 억제됩니다.

업그레이드 중에 Red Hat Satellite를 사용하려는 경우 Satellite 웹 UI 또는 **hammer repository-set enable** 및 **hammer product synchronize** 명령을 사용하여 업그레이드하기 전에 다음 RHEL 8 리포지토리를 활성화하고 동기화해야 합니다.



### 참고

<target\_os\_version>을 대상 운영 체제(OS) 버전으로 바꿉니다(예: 8.10).

표 B.1. RHEL 8 리포지토리

아키텍처	리포지토리	리포지토리 ID	리포지토리 이름	릴리스 버전
64비트 Intel	BaseOS	<b>rhel-8-for-x86_64-baseos-rpms</b>	Red Hat Enterprise Linux 8 for x86_64 - BaseOS(RPM)	x86_64 <target_os_version>
	AppStream	<b>rhel-8-for-x86_64-appstream-rpms</b>	Red Hat Enterprise Linux 8 for x86_64 - AppStream(RPM)	x86_64 <target_os_version>
IBM Power8 (little endian)	BaseOS	<b>rhel-8-for-ppc64le-baseos-rpms</b>	Red Hat Enterprise Linux 8 for Power, little endian - BaseOS(RPM)	ppc64le <target_os_version>
	AppStream	<b>rhel-8-for-ppc64le-appstream-rpms</b>	Red Hat Enterprise Linux 8 for Power, little endian - AppStream(RPM)	ppc64le <target_os_version>
IBM Z	BaseOS	<b>rhel-8-for-s390x-baseos-rpms</b>	Red Hat Enterprise Linux 8 for IBM z Systems - BaseOS(RPM)	s390x <target_os_version>

아키텍처	리포지터리	리포지터리 ID	리포지터리 이름	릴리스 버전
	AppStream	<b>rhel-8-for-s390x-appstream-rpms</b>	Red Hat Enterprise Linux 8 for IBM z Systems - AppStream(RPM)	s390x < <i>target_os_version</i> >



## 부록 C. RHEL 8의 암호화 키 위치

FIPS(Federal Information Processing Standard) 모드에서 실행되는 시스템을 업그레이드한 후 다시 생성하고 그렇지 않으면 모든 암호화 키의 FIPS 준수 여부를 확인해야 합니다. 이러한 키의 잘 알려진 위치는 다음 표에 있습니다. 목록이 완료되지 않았으며 다른 위치도 확인할 수 있습니다.

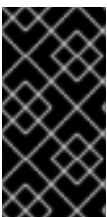
표 C.1. RHEL 8의 암호화 키 위치

애플리케이션	키 위치	참고
Apache mod_ssl	<b>/etc/pki/tls/private/localhost.key</b>	<b>/etc/pki/tls/private/localhost.key</b> 가 없는 경우 <b>/usr/lib/systemd/httpd-init.service</b> 서비스는 <b>/usr/libexec/httpd-ssl-gencerts</b> 파일을 실행합니다.
Bind9 RNDc	<b>/etc/rndc.key</b>	<b>named-setup-rndc.service</b> 서비스는 <b>/etc/rndc.key</b> 파일을 생성하는 <b>/usr/libexec/generate-rndc-key.sh</b> 스크립트를 실행합니다.
Cyrus IMAPd	<b>/etc/pki/cyrus-imapd/cyrus-imapd-key.pem</b>	<b>cyrus-imapd-init.service</b> 서비스는 시작 시 <b>/etc/pki/cyrus-imapd/cyrus-imapd-key.pem</b> 파일을 생성합니다.
DNSSEC-Trigger	<b>/etc/dnssec-trigger/dnssec_trigger_control.key</b>	<b>dnssec-triggerd-keygen.service</b> 서비스는 <b>/etc/dnssec-trigger/dnssec_trigger_control.key</b> 파일을 생성합니다.
Dovecot	<b>/etc/pki/dovecot/private/dovecot.pem</b>	<b>dovecot-init.service</b> 서비스는 시작 시 <b>/etc/pki/dovecot/private/dovecot.pem</b> 파일을 생성합니다.
OpenPegasus	<b>/etc/pki/Pegasus/file.pem</b>	<b>tog-pegasus.service</b> 서비스는 <b>/etc/pki/Pegasus/file.pem</b> 개인 키 파일을 생성합니다.

애플리케이션	키 위치	참고
OpenSSH	<code>/etc/ssh/ssh_host*_key</code>	Ed25519 및 DSA 키는 FIPS와 호환되지 않습니다.  CRD(Custom Diffie-Hellman) 매개변수는 FIPS 모드에서 지원되지 않습니다. <b>sshd_config</b> 파일의 <b>ModuliFile</b> 옵션을 주석 처리하여 FIPS 모드와의 호환성을 확인합니다. <b>moduli</b> 파일 (기본적으로 <code>/etc/ssh/moduli</code> )을 그대로 유지할 수 있습니다.
Postfix	<code>/etc/pki/tls/private/postfix.key</code>	<b>postfix</b> 패키지에 포함된 설치 후 스크립트는 <code>/etc/pki/tls/private/ECDHE.key</code> 파일을 생성합니다.
RHEL 웹 콘솔	<code>/etc/cockpit/ws-certs.d/</code>	웹 콘솔은 <code>/etc/cockpit/ws-certs.d/</code> 디렉터리에 키를 생성하는 <code>/usr/libexec/cockpit-ensure-for-cockpit-tls</code> 파일을 실행합니다.
sendmail	<code>/etc/pki/tls/private/sendmail.key</code>	<b>sendmail</b> 패키지에 포함된 설치 후 스크립트는 <code>/etc/pki/tls/private/sendmail.key</code> 파일을 생성합니다.

타사 애플리케이션의 암호화 키의 FIPS 준수 여부를 확인하려면 해당 애플리케이션의 해당 문서를 참조하십시오. 또한 다음을 수행합니다.

- 포트를 여는 모든 서비스는 TLS 인증서를 사용할 수 있습니다.
  - 모든 서비스에서 암호화 키를 자동으로 생성하는 것은 아니지만 기본적으로 자동으로 시작하는 많은 서비스가 자주 수행됩니다.
- NSS, GnuTLS, OpenSSL 및 libcrypt와 같은 암호화 라이브러리를 사용하는 서비스에도 중점을 둡니다.
- 백업, 디스크 암호화, 파일 암호화 및 유사한 애플리케이션도 확인합니다.



**중요**

RHEL 8의 FIPS 모드는 DSA 키, DH 매개변수, RSA 키는 1024비트보다 짧기 때문에 이전 암호화 키는 RHEL 7에서 업그레이드한 후 작동을 중지합니다. 자세한 내용은 RHEL 8 보안 강화 문서의 시스템 전체 암호화 정책 사용 장에 있는 RHEL 8 문서 채택 시 핵심 암호화 구성 요소의 변경 사항 섹션을 참조하십시오.

## 추가 리소스

- [RHEL 8 보안 강화 문서에서 시스템을 FIPS 모드로 전환](#)
- [update-crypto-policies\(8\) 및 fips-mode-setup\(8\) 도움말 페이지](#)