Leapp 설명

Leapp은 Red Hat® Enterprise Linux® 메이저 버전의 인플레이스 시스템 업그레이드를 수행하는 데 사용되는 지원 툴입니다. Leapp을 사용하면 시스템을 재설치할 필요 없이 Red Hat Enterprise Linux를 안심하고 업그레이드하고 새로운 기능을 활용할 수 있습니다.

'Red Hat Enterprise Linux로 업그레이드해야 하는 주요 이유' 체크리스트 읽기

업그레이드해야 하는 이유

업그레이드는 고객이 Red Hat Enterprise Linux의 메이저 버전에서 제공되는 새로운 기능과 함께 최신 개선 사항, 수정 사항, 패치가 포함된 지원 제품을 사용함으로써 비즈니스 연속성을 유지하는 데 도움이 됩니다.

Red Hat Enterprise Linux의 향상된 성능을 통해 총소유비용(TCO)을 절감하고 생산성을 높이며 기술 투자 효과를 극대화할 수 있습니다.

Red Hat Enterprise Linux는 예측 가능한 3년의 메이저 릴리스 주기로 운영되며 서브스크립션은 현재 지원되는 모든 Red Hat Enterprise Linux 버전에 유효합니다. 따라서 새로운 버전이 출시되면 최신 이머징 기술에 액세스하여 활용할 수 있습니다. Red Hat Enterprise Linux의 각 메이저 버전은 10년 동안 지원되며 두 가지 지원 단계로 나뉩니다.

첫 번째 단계는 상용화 버전(General Availability, GA) 출시 후 5년이며 전체 지원됩니다. 새 기능이 추가되고 새 하드웨어가 지원되며 문제와 버그가 수정됩니다. 두 번째 5년 동안에는 릴리스가 유지관리 지원으로 전환되어 '매우 중요' 및 '중요' 등급 보안 정오표와 선택된 기타 기능 또는 버그 수정 개선 사항이 계속 게시됩니다. 10년간의 일반적인 라이프사이클이 종료되면 고객은 Red Hat Extended Life Cycle Support Add-On을 구입하여 '매우 중요' 및 '중요' 보안 정오표를 포함하는 2년간의 추가 지원을 받을 수 있습니다. Red Hat Enterprise Linux 라이프사이클 페이지에서 자세한 내용을 확인해 보세요.

Red Hat Enterprise Linux로 업그레이드하면 다음과 같은 여러 가지 새로운 기능을 활용할 수 있습니다.

- 애플리케이션 스트림에서 제공하는 업데이트된 소프트웨어는 Red Hat Enterprise Linux 메이저 릴리스의 전체 지원 단계 전반에 걸쳐 최신 언어 런타임, 데이터베이스, 기타 애플리케이션을 제공합니다.
- Red Hat Enterprise Linux 컨테이너 툴(예: Podman, Buildah, Skopeo)에서 컨테이너의 구축, 배포, 관리를 지원합니다.
- 커널 실시간 패치 적용(kpatch)을 통해 재부팅하지 않고도 일부 '중요' 및 '매우 중요' 등급의 CVE(Common Vulnerabilities and Exposures)에 대한 커널을 패치할 수 있습니다.

- eBPF 기반 툴을 사용하는 성능 관측성 툴로 시스템의 성능 측면을 빠르게 파악할 수 있습니다.
- 일반적으로 데스크탑 애플리케이션에 사용되는 애플리케이션을 실행하기 위해 Flatpak이 지원됩니다.
- Cgroup2에서 프로세스에서 사용하는 리소스를 관리하는 간소화된 기능을 제공합니다.

더욱 원활하게 관리할 수 있도록 개선된 웹 콘솔 인터페이스를 포함하여 다양한 자동화 및 관리 기능이 향상되었습니다.

자동화 개선 사항에는 다음이 포함됩니다.

- Red Hat Ansible® Automation Platform을 기반으로 하는 Red Hat Enterprise Linux의 새로운 시스템 롤을 통해 규모에 맞게 관리를 자동화합니다.
- Red Hat Insights가 모든 Red Hat Enterprise Linux 서브스크립션에 포함되어 취약성, 롤 누락, 기타 사전 정의된 기준을 사전 예방적으로 검사합니다.

하드웨어를 최대한 활용하는 데 중점을 두는 고객은 Red Hat Enterprise Linux 9가 Red Hat Enterprise Linux 7과 Red Hat Enterprise Linux 8보다 일반적으로 성능이 우수하다는 점에 주목해야 합니다. 이를 가능하게 하는 몇 가지 변경 사항은 다음과 같습니다.

- 커널을 위한 새로운 디스크 엘리베이터
- 새롭게 튜닝된 성능 프로필

제품 정보는 Red Hat Enterprise Linux 6에서 Red Hat Enterprise Linux 8로 업그레이드를 참조하세요.

Leapp이란 무엇이며 왜 사용해야 할까요?

서버를 업그레이드하는 일은 까다로운 작업일 수 있지만, Red Hat Enterprise Linux는 지원되는 업그레이드 관리 툴인 Leapp과 함께 제공됩니다. 이 툴은 Red Hat Enterprise Linux의 다음 메이저 버전으로 업그레이드할 수 있는 단일 경로를 제공합니다. Leapp을 사용하면 고객은 시스템에 연결되어 있는 원래의 서브스크립션, 시스템 구성, 사용자 정의 리포지토리, 타사 애플리케이션을 유지할 수 있습니다.

Leapp은 Red Hat Enterprise Linux 7과 Red Hat Enterprise Linux 8에 포함되어 있어 Red Hat Enterprise Linux 7.9에서 Red Hat Enterprise Linux 8로 업그레이드할 수 있습니다. 또한 Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 업그레이드하는 데에도 사용할 수 있습니다.

Red Hat Enterprise Linux 6을 사용 중인 경우에는 먼저 다른 툴을 사용하여 Red Hat Enterprise Linux 7로 업그레이드한 후 Leapp을 사용하여 Red Hat Enterprise Linux 8 또는 Red Hat Enterprise Linux 9로 업그레이드해야 합니다.

아래 표는 Leapp을 사용하여 서버를 업그레이드할 때의 장점을 보여줍니다.

Leapp을 통한 인플레이스 업그레이드	재설치
구성 유지	구성 데이터를 백업하고 재시작해야 함
머신에서 기존 서브스크립션 데이터 유지	subscription-manager를 사용하여 머신에서 서브스크립션에 등록해야 함
자동화를 통해 생산성 향상	추가 시간과 비용 발생

작동 방식

Leapp이 작동하는 방식을 이해하면 업그레이드를 성공적으로 수행하는 능력이 향상됩니다. Leapp 사용은 업그레이드 가능성 분석 단계와 실제 업그레이드 단계로 구성된 2단계 프로세스입니다. 업그레이드 후 재부팅해야 하며 업그레이드를 계획할 때 이를 고려해야 합니다.

Leapp을 사용하는 단일 호스트의 경우 업그레이드 가능성 분석은 *cloud.redhat.com*에서 메타데이터로 다운로드할 수 있는 업그레이드 고려 사항을 기반으로 합니다.

Red Hat Satellite에 연결된 호스트의 경우 메타데이터는 Leapp을 사용하여 Satellite에서 서버에 배포해야 합니다. 그러면 Red Hat Satellite용 Leapp 플러그인을 사용하여 업그레이드 가능성 분석을 대규모로 수행할 수 있습니다.

업그레이드 가능성 분석에서는 업그레이드를 수행하기 전에 해결해야 할 항목을 포함할 수 있는 리포트를 생성합니다.

Leapp은 워크플로우의 일부로 여러 Python 프로그램을 사용합니다. 이러한 Python 프로그램을 행위자(actor)라고 하며 행위자는 시스템을 변경할 수 있습니다.

'Leapp을 통한 업그레이드에 Red Hat Satellite 사용' 읽기

예를 들어, **CheckOSRelease**라는 행위자는 현재 Red Hat Enterprise Linux 마이너 버전이 지원되는지 확인합니다. 지원되지 않으면 업그레이드 프로세스를 차단합니다.

기존 행위자 세트에서 다루지 않는 업그레이드 고려 사항이 있는 경우 해당 고려 사항을 해결, 차단하거나 알리기 위해 고유한 사용자 정의 행위자를 작성할 수 있습니다. 그런 다음 이 행위자를 Leapp 워크플로우에 통합할 수 있습니다.

Leapp은 Red Hat Insights와 통합되어 등록된 시스템을 검사하고 업그레이드에 적합한 머신을 결정합니다.

Leapp을 통한 업그레이드는 커맨드라인 또는 Red Hat Satellite를 통해 실행할 수 있습니다.

제한 사항

서버 업그레이드를 진행하기 전에 Leapp 사용과 관련된 몇 가지 중요한 제한 사항을 이해해야 합니다.

- Leapp은 Red Hat Enterprise Linux의 특정 메이저 버전에서 다음 메이저 버전으로 업그레이드할 때만 사용할 수 있습니다.
- Leapp은 루트 파일 시스템에 디스크 암호화를 사용하는 경우 작동하지 않습니다.
- VDO 기기는 LVM에서 관리하도록 변환해야 합니다.
- 네트워크 기반 다중 경로 또는 네트워크 스토리지 마운트(예: iSCSI, 네트워크 파일 시스템(NFS))는 시스템 파티션에 사용할 수 없습니다.
- Red Hat Update Infrastructure(Red Hat Subscription Manager와는 다름)를 사용하는 퍼블릭 클라우드의 온디맨드 인스턴스는 Leapp을 사용하여 업그레이드할 수 없습니다.

업그레이드할 준비가 되었습니다. 어디서 시작해야 할까요?

Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 업그레이드하는 과정을 살펴보겠습니다. Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 업그레이드하는 워크플로우도 유사합니다. **yum update**를 사용하여 시스템이 Red Hat Enterprise Linux 7.9로 업데이트했는지 확인하세요.

```
[root@leapp7to8 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.9 (Maipo)
```

leapp 패키지를 설치해야 합니다. Red Hat Enterprise Linux 7 Extras 채널이 활성화된 상태에서 머신이 Red Hat CDN 또는 Satellite 서버 서브스크립션에 등록되어 있는지 확인하세요. 다음 명령을 사용하여 확인할 수 있습니다.

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-7-server-extras-rpms
Repo Name: Red Hat Enterprise Linux 7 Server - Extras (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/7Server/$basearch/extras/os
Enabled:   1


Repo ID:   rhel-7-server-rpms
Repo Name: Red Hat Enterprise Linux 7 Server (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel/
server/7/$releasever/$basearch/os
Enabled:   1
```

rhel-7-server-extras-rpms 리포지토리가 활성화되지 않은 경우 다음을 사용하여 활성화할 수 있습니다.

```
[root@leapp7to8 ~]# subscription-manager repos --enable
rhel-7-server-extras-rpm
```

이제 다음을 사용하여 Red Hat Enterprise Linux 7에 Leapp를 설치할 수 있습니다.

```
[root@leapp7to8 ~]# yum install -y leapp
```

Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 업그레이드할 때는 다음 단계를 검토하여 Leapp 인플레이스 업그레이드 유틸리티를 설치합니다. Red Hat Enterprise Linux 9로 업그레이드하기 전에 Red Hat Enterprise Linux 8 서버를 업데이트해야 할 수도 있습니다. 자세한 내용은 Red Hat Enterprise Linux의 지원되는 인플레이스 업그레이드 경로를 참조하세요.

```
[root@leapp8to9 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.6 (Ootpa)
```

leapp 및 **leapp-upgrade-el8toel9** 패키지를 설치해야 합니다. 이 두 패키지는 **rhel-8-for-x86_64-appstream-rpms** 리포지토리에 있습니다. 다음을 사용하여 패키지를 설치합니다.

```
[root@leapp8to9 ~]# yum install -y leapp leapp-upgrade-el8toel9
```

이전에 Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 인플레이스 업그레이드한 경우 시스템에 **/root/tmp_leapp_py3** 디렉터리가 있으면 이 디렉터리를 제거합니다.

```
[root@leapp8to9 ~]# rm -rf /root/tmp_leapp_py3
```

Red Hat Enterprise Linux 릴리스를 위해 Leapp 인플레이스 업그레이드 패키지를 설치한 후에는 업그레이드를 수행하기 전에 **leapp preupgrade**로 서버를 분석하여 잠재적인 문제를 식별해야 합니다. 시스템은 수정되지 않고 유지되며 업그레이드 경로를 구성하는 중요한 파일을 생성합니다.

```
[root@leappXtoY ~]# leapp preupgrade
```

preupgrade 명령을 실행하면 아래와 유사한 출력이 표시될 수 있습니다.

```
…
 output omitted
…

==========================================================
                    UPGRADE INHIBITED
==========================================================
```

```
Upgrade has been inhibited due to the following problems:
    1. Inhibitor: Use of NFS detected. Upgrade can't proceed
Consult the pre-upgrade report for details and possible
remediation.

============================================================
                    UPGRADE INHIBITED
============================================================

Debug output written to /var/log/leapp/leapp-preupgrade.log

============================================================
                           REPORT
============================================================

A report has been generated at /var/log/leapp/leapp-report.json
A report has been generated at /var/log/leapp/leapp-report.txt

============================================================
                       END OF REPORT
============================================================

Answerfile has been generated at /var/log/leapp/answerfile
```

주목할 만한 파일:

/var/log/leapp/leapp-report.txt	Leapp 업그레이드 리포트에 대한 읽기 가능하고 이해하기 쉬운 정보
/var/log/leapp/leapp-report.json	JSON 형식으로 된 리포트
/var/log/leapp/leapp-preupgrade.log	leapp preupgrade 명령의 디버그 출력
/var/log/leapp/answerfile	leapp upgrade 명령에서 묻는 질문에 대한 답변

업그레이드 가능성 분석 리포트는 **/var/log/leapp/leapp-report.txt**에 저장되며 업그레이드를 수행하기 전에 조치를 취해야 하는 중요한 고려 사항이 있을 수 있습니다. 이러한 고려 사항에는 입력이 필요할 수 있으며 리포트 내의 지침에 따라 처리할 수 있습니다.

Leapp 사전 업그레이드 고려 사항 해결

/var/log/leapp/leapp-report.txt의 Leapp 사전 업그레이드 리포트에는 해결해야 할 몇 가지 작업 항목이 있을 수 있습니다. ***inhibitor***(차단자)는 업그레이드를 진행하기 위해 해결해야 하는 차단 항목입니다. 차단자가 해결되지 않으면 시스템에서 Leapp 업그레이드가 수행되지 않습니다.

risk factor(위험 요소)는 다음 키를 사용하여 업그레이드 고려 사항이 미치는 영향을 설명합니다.

높음	상태가 악화될 가능성이 매우 높음
중간	시스템과 애플리케이션 모두에 영향을 미칠 수 있음
낮음	시스템에는 영향을 미치지 않지만 애플리케이션에는 영향을 미칠 수 있음
정보	시스템과 애플리케이션 모두에 영향을 미치지 않는 정보

title(제목)은 Leapp 사전 업그레이드 리포트의 요소를 식별하고, summary(요약)는 자세한 정보를 제공합니다.

summary는 해결이 필요할 수 있는 감지된 문제를 간략히 설명합니다.

remediation(문제 해결)은 보고된 문제에 대한 실행 가능한 해결책입니다. 일반적인 문제 해결의 유형은 다음과 같습니다.

- 구성 파일 편집
- 시스템 작동 방식을 변경하는 명령 실행
- Leapp 응답 파일을 통한 문제 해결
- Python, PHP, Node.js, PostgreSQL 등과 같은 Red Hat Enterprise Linux 7 소프트웨어 컬렉션 라이브러리의 모듈식 소프트웨어에 영향을 미치는 문제 해결
- 일시적으로 NFS 내보내기 마운트 해제

이 섹션에는 높음 및 중간 등급 위험 요소에 대한 업그레이드 고려 사항의 예시가 표시되며 다음을 포함하도록 구성됩니다.

- 예시 스니펫에서 Leapp 리포트에 보고된 메시지
- 영향을 받는 소프트웨어 하위 시스템
- 보고된 항목의 의미 설명
- 취해야 할 조치
- 실행 가능한 보고 항목을 처리하지 않았을 때의 결과

업그레이드할 Red Hat Enterprise Linux 버전과 구성에 따라 시스템 고려 사항이 다를 수 있습니다.

예시 1: 시스템을 일시적으로 변경해야 하는 고위험 차단자

이 예시는 사전 평가 리포트에서 보고한 높은 등급의 차단자 문제를 보여줍니다. 이 문제를 수정하지 않으면 시스템에서 Leapp 업그레이드를 실행할 때 오류가 표시되고 시스템이 업그레이드되지 않습니다. 메시지뿐만 아니라 시스템에서 이 문제를 해결하는 방법도 살펴보겠습니다.

```
Risk Factor: high (inhibitor)
Title: Use of NFS detected. Upgrade can’t proceed
Summary: NFS is currently not supported by the inplace upgrade.
We have found NFS usage at the following locations:
- One or more NFS entries in /etc/fstab
- Currently mounted NFS shares

Remediation: [hint] Disable NFS temporarily for the upgrade if
possible.
Key: 9881b25faceeeaa7a6478bcdac29afd7f6baaaed
```

이 메모를 처리하지 않으면 어떻게 되나요?

이 메모는 차단자에 해당하며 적절한 조치를 취할 때까지 업그레이드를 차단합니다. 위험 요소는 높음이며, 변경 사항이 로컬 서버에만 적용되고 NFS 공유에는 영향을 주지 않을 것으로 예상되기 때문입니다.

영향을 받는 하위 시스템은 무엇인가요?

NFS 마운트

어떤 의미인가요?

업그레이드 프로세스 중에 NFS 마운트를 사용할 수 없으며 업그레이드가 완료될 때까지 마운트를 해제하고 비활성화해야 합니다.

어떤 작업을 수행해야 하나요?

/etc/fstab을 편집하여 NFS 공유를 일시적으로 주석으로 처리하고 현재 마운트된 NFS 공유를 마운트 해제합니다. autofs.service를 일시적으로 중지하고 비활성화합니다. 업그레이드가 완료되면 NFS 항목과 autofs.service를 다시 활성화할 수 있습니다.

```
[root@leapp8to9 ~]# systemctl disable –now autofs.service
```

예시 2: 기존 구성 파일을 변경해야 하는 고위험 차단자

이는 주로 Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 업그레이드할 때 발생합니다.

```
Risk Factor: high (inhibitor)

Title: Possible problems with remote login using root account

Summary: OpenSSH configuration file does not explicitly state
the option PermitRootLogin in sshd_config file, which will
default in Red Hat Enterprise Linux8 to “prohibit-password”.

Remediation: [hint] If you depend on remote root logins using
passwords, consider setting up a different user for remote
administration or adding “PermitRootLogin yes” to sshd_config.

Key: 3d21e8cc9e1c09dc60429de7716165787e99515f
```

이 메모를 처리하지 않으면 어떻게 되나요?

이 메모는 차단자에 해당하며 업그레이드를 차단합니다. 위험 요소는 높음이며, 이 항목을 잘못 처리하면 SSH(Secure Shell)를 사용하여 서버에 원격으로 로그인하지 못할 수 있으므로 주의해야 합니다.

영향을 받는 하위 시스템은 무엇인가요?

ssh 서버(sshd.service)

어떤 의미인가요?

이 스니펫은 SSH 서버가 Red Hat Enterprise Linux 7과 Red Hat Enterprise Linux 8 사이에서 작동하는 방식에 큰 영향을 미치는 변경이 있음을 나타냅니다. Red Hat Enterprise Linux 8의 루트 사용자는 기본적으로 암호 인증을 사용할 수 없습니다. Red Hat Enterprise Linux 7에서는 PermitRootLogin의 묵시적 기본값이 yes지만, Red Hat Enterprise Linux 8에서는 묵시적 기본값이 prevent-password입니다.

묵시적 구성 지시문은 /etc/ssh/sshd_config 내부에 주석처럼 표시되지만 주석이 아닙니다. 지시문의 기본값을 알리기 위해 표시됩니다.

어떤 작업을 수행해야 하나요?

암호를 사용하거나 사용하지 않고 다른 사용자로 로그인할 수 있는지 확인하세요.

/etc/ssh/sshd_config 내에서 PermitRootLogin에 대한 값을 명시적으로 설정해야 합니다. 루트 사용자가 ssh를 통해 로그인하도록 허용하려면 값을 yes로, 이러한 로그인을 차단하려면 no로 설정하면 됩니다. 지시문을 명시적으로 설정하는 것이 중요합니다.

Linux 매뉴얼 페이지는 추가 정보를 얻을 수 있는 유용한 자료입니다. **man sshd_config** 명령을 사용한 후 *PermitRootLogin* 문자열을 검색하면 이 구성 지시문에 대한 자세한 내용을 확인할 수 있습니다.

예시 3: Leapp 응답 파일을 사용해야 하는 고위험 차단자

이 특정 문제는 주로 Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 업그레이드할 때 발생합니다. 이 예시의 고유한 요소는 Leapp 응답 파일을 사용하여 문제를 해결해야 한다는 것입니다. Leapp 응답 파일은 데이터를 자동으로 Leapp 유틸리티에 전달할 수 있는 파일입니다.

```
Risk Factor: high (inhibitor)

Title: Missing required answers in the answer file

Summary: One or more sections in answerfile are missing user
choices: remove_pam_pkcs11_module_check.confirm

For more information consult https://leapp.readthedocs.io/en/
latest/dialogs.html

Remediation: [hint] Please register user choices with leapp
answer cli command or by manually editing the answerfile.

[command] leapp answer --section remove_pam_pkcs11_module_check.
confirm=True

Key: d35f6c6b1b1fa6924ef442e3670d90fa92f0d54b
```

이 메모를 처리하지 않으면 어떻게 되나요?

이 메모는 차단자에 해당하며 pam_pkcs11 모듈 제거를 승인할 때까지 업그레이드를 차단합니다. 위험 요소는 높음입니다. 이는 PAM 구성에 pam_pkcs11 모듈과 관련된 *필수 또는 요구되는* 제어 값이 있을 수 있고 Red Hat Enterprise Linux 8에서 이 모듈을 제거하면 시스템이 잠길 수 있기 때문입니다.

이 업그레이드 항목은 Leapp 응답 파일을 사용하는 **경우에만** 해결할 수 있습니다.

영향을 받는 하위 시스템은 무엇인가요?

인증(pam)

어떤 의미인가요?

이 스니펫은 Red Hat Enterprise Linux8에서 pam_pkcs11 모듈이 제거되었으며 해당 기능이 이제 sssd에서 제공됨을 나타냅니다.

어떤 작업을 수행해야 하나요?

/var/log/leapp/answerfile을 다음과 같이 편집하세요.

```
[remove_pam_pkcs11_module_check]

confirm = True
```

또는 다음 명령을 실행하여 /var/log/leapp/answerfile 응답 파일을 편집합니다.

```
leapp answer --section
remove_pam_pkcs11_module_check.confirm=true
```

또한 pam_pkcs11 모듈을 사용하지 않는 다른 인증 방법이 있는지 확인해야 합니다.

grep pam_pkcs11 /etc/pam.d/*를 실행하여 확인할 수 있습니다.

애플리케이션 스트림에서 소프트웨어 관리에 대한 핸즈온 랩 방문하기

예시 4: 업그레이드 후 Python 프로그램에 영향을 미치는 고위험, 비차단 고려 사항

이 예시는 주로 Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 업그레이드하는 시스템에서 발생합니다. 이전 예시와 달리 차단자가 아니므로 이 감지된 문제가 해결되지 않아도 Leapp 업그레이드 툴에서 업그레이드를 수행합니다. 이 문제를 해결해야 하는지 여부는 시스템 관리자가 결정합니다. 이 머신에서 Python2 기반 애플리케이션을 사용하는지, 그리고 해당 애플리케이션이 업그레이드된 운영 체제에서 제공하는 Python3과 호환되는지도 시스템 관리자가 결정합니다.

```
Risk Factor: high

Title: Difference in Python versions and support in Red Hat
Enterprise Linux 8

Summary: In Red Hat Enterprise Linux 8, there is no ‘python’
command. Python 3 (backward incompatible) is the primary Python
version and Python 2 is available with limited support and
limited set of packages. Read more here: https://access.redhat.
com/documentation/en-us/red_hat_enterprise_linux/8/html-single/
configuring_basic_system_settings/#using-python3

Remediation: [hint] Please run “alternatives --set python /usr/
bin/python3” after upgrade

Key: 0c98585b1d8d252eb540bf61560094f3495351f5
```

이 메모를 처리하지 않으면 어떻게 되나요?

이 메모는 차단자가 아니며 해결 방법을 무시해도 Leapp 업그레이드 명령이 계속 진행됩니다. 위험 요소는 높음입니다. 이는 버전이 지정되지 않은 python 명령(/usr/bin/python)은 기본적으로 Red Hat Enterprise Linux 8에서 사용할 수 없기 때문입니다. Python 인터프리터를 직접(예: 터미널에서) 또는 간접적으로(다른 프로세스에서 명령을 대신 실행) 실행하면 실패합니다.

영향을 받는 하위 시스템은 무엇인가요?

버전이 지정되지 않은 /usr/bin/python 명령을 사용하는 Python과 애플리케이션

어떤 의미인가요?

Python 3이 선호되면서 Python 2는 더 이상 사용되지 않지만, 여전히 애플리케이션 스트림을 사용하여 설치할 수 있습니다. 애플리케이션 스트림 리포지토리에서는 서버에 병렬로 설치할 수 있는 다양한 Python 모듈을 제공합니다. 설치하거나 호출하거나 상호 작용할 Python 버전을 항상 지정해야 합니다. 버전이 지정되지 않은 Python 명령은 기본적으로 사용할 수 없지만, 원하는 경우 구성할 수 있습니다.

어떤 작업을 수행해야 하나요?

다음 명령을 실행하여 기본 Python 버전으로 /usr/bin/python3을 사용하도록 할 수 있습니다.

```
alternatives --set python /usr/bin/python3
```

명시적으로 Python 2가 필요한 애플리케이션은 모두 /usr/bin/python2를 참조해야 합니다. 또는 다음 명령을 사용하여 기본 Python 버전을 Python 2로 설정할 수 있습니다.

```
alternatives --set python /usr/bin/python2
```

예시 5: 중간 위험, 비차단 고려 사항

이 예시는 주로 Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 업그레이드할 때 발생합니다.

```
Risk Factor: medium

Title: chrony using default configuration

Summary: default chrony configuration in Red Hat Enterprise
Linux8 uses leapsectz directive, which cannot be used with leap
smearing NTP servers, and uses a single pool directive instead
of four server directives

Key: c4222ebd18730a76f6bc7b3b66df898b106e6554
```

이 메모를 처리하지 않으면 어떻게 되나요?

이 메모는 차단자가 아니며 Leapp 업그레이드를 차단하지 않습니다. 위험 요소는 중간입니다. 이는 동일한 윤초 스미어(leap smear)를 구현하지 않거나 일부 윤초 스미어를 구현하지 않는 여러 서버에서 시간을 가져오도록 구성된 NTP(Network Time Protocol) 클라이언트는 윤초 스미어링 중 서로 다른 서버에서 다른 시간을 가져오기 때문입니다. 이로 인해 NTP 클라이언트가 시계 업데이트를 중지하거나 다른 서버로 무작위로 이동할 수 있습니다.

영향을 받는 하위 시스템은 무엇인가요?

chrony를 사용한 시간 동기화

어떤 의미인가요?

chrony는 NTP를 사용하여 시간 동기화를 구현합니다. Red Hat Enterprise Linux8에서 pool 지시문은 기본적으로 기능이 동일한 NTP 서버 풀을 참조하는 데 사용됩니다. 다양한 기능의 NTP 서버를 참조하는 여러 개의 server 지시문을 사용하면 시간 동기화 성능이 저하될 수 있습니다.

어떤 작업을 수행해야 하나요?

/etc/chrony.conf에서 *leapsectz* 및 *leapfile* 지시문을 제거하고 /etc/chrony.conf 내에 server 지시문 대신 pool 지시문을 사용합니다. 그러면 기능이 동일한 NTP 서버가 사용됩니다.

명시적으로 정의된 서버에 시스템 시간을 동기화하려면 모든 서버의 기능이 동일한지 확인해야 합니다.

'Red Hat Enterprise Linux로 업그레이드해야 하는 주요 이유' 체크리스트 읽기

업그레이드할 준비가 되었습니다!

사전 업그레이드 리포트에서 식별된 문제를 해결한 후에는 **leapp preupgrade** 명령을 다시 실행하고 리포트 파일을 다시 검토하여 업그레이드 차단의 원인이 되는 누락된 부분이 없는지 확인하는 것이 좋습니다.

시스템을 업그레이드할 준비가 되면 **leapp upgrade** 또는 **leapp upgrade --reboot** 명령 중 하나를 실행합니다.

BOOM 개요 및 설치 방법 알아보기

스냅샷을 사용한 시스템 업그레이드 관리에 대해 자세히 알아보기

leapp upgrade 명령은 업그레이드 프로세스를 대기열에 추가하고, 완료하기까지 여러 번의 재부팅이 필요합니다. 이를 잘 계획하는 것이 중요합니다. 첫 번째 부팅 이전에는 현재 버전의 Red Hat Enterprise Linux를 계속 사용할 수 있습니다.

leapp upgrade reboot 명령은 서버를 자동으로 재부팅합니다.

첫 번째 부팅: 부트로더에서 **Red Hat Enterprise Linux-Upgrade-Initramfs** 메뉴 항목을 사용하여 특수 업그레이드 환경을 자동으로 초기화합니다. 이 업그레이드 환경 내에서 서버가 업그레이드됩니다. 업그레이드를 되돌리고 Red Hat Enterprise Linux의 이전 메이저 버전을 계속 사용하려면 백업이 필요합니다.

두 번째 부팅: SELinux 레이블이 복원되고 서버가 한 번 더 재부팅됩니다.

세 번째 부팅: 업그레이드가 올바른지 확인하고 새로운 Red Hat Enterprise Linux 환경을 이용할 수 있습니다.

현재 사용 중인 Red Hat Enterprise Linux 버전을 확인합니다.

```
[root@leapp7to8 ~]# rpm -q redhat-release
redhat-release-8.6-0.1.el8.x86_64
```

```
[root@leapp8to9 ~]# rpm -q redhat-release
redhat-release-9.0-2.17.el9.x86_64
```

Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 업그레이드하는 경우 *rhel-8-server-rpms*라는 리포지토리가 있을 수 있지만, Red Hat Enterprise Linux8에는 두 개의 리포지토리가 있습니다. *rhel-8-for-x86_64-baseos-rpms*는 핵심적인 기본 OS 기능 세트를 제공하고, *rhel-8-for-x86_64-appstream-rpms*는 다양한 워크로드와 활용 사례를 지원하는 추가 사용자 공간 애플리케이션, 런타임 언어, 데이터베이스를 포함합니다. 이는 다음과 같이 확인할 수 있습니다.

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Available Repositories in /etc/yum.repos.d/redhat.repo
+----------------------------------------------------------+
Repo ID:   rhel-8-for-x86_64-appstream-rpms
```

```
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - AppStream
(RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/
x86_64/appstream/os
Enabled:   1


Repo ID:   rhel-8-for-x86_64-baseos-rpms
Repo Name: Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
Repo URL:  https://cdn.redhat.com/content/dist/rhel8/8.6/
x86_64/baseos/os
Enabled:   1
```

시스템을 업그레이드하고 재부팅한 후에는 업그레이드 후 리포트가 포함된 **/var/log/leapp/leapp-report.txt** 파일에서 완료해야 할 추가 작업 항목이 있는지 다시 확인해야 합니다.

유용한 정보

시작하기 전에 다음 권장 사항을 고려하는 것이 좋습니다.

sosreport

필요한 경우 지원을 제공할 수 있도록 sosreport를 생성하도록 합니다.

1. **yum install sos**를 사용하여 sos 패키지가 설치되었는지 확인합니다.
2. **sosreport** 명령을 사용하여 리포트를 생성합니다.
3. Red Hat 지원이 필요한 경우 **/var/tmp/**에 있는 생성된 tar 아카이브를 안전한 위치에 복사합니다.

백업 생성

시스템이 작동하지 않거나 데이터에 액세스할 수 없는 예기치 않은 상황이 발생할 경우, 적시에 복구하고 작업을 재개할 수 있는 기능이 가장 중요합니다. 데이터를 백업하면 복구 프로세스를 용이하게 수행할 수 있으며, 이미 수행하고 있어야 합니다. 특히 Leapp을 사용하여 서버를 업그레이드하기 전에 데이터를 백업하는 것을 잊지 않아야 합니다.

사용 중인 툴을 사용하여 백업 전략을 구현하세요.

- 작동 중인 서버와 관련된 데이터를 확인합니다.
- 업그레이드할 서버 외부의 안전한 위치에 데이터를 백업합니다.
- 백업을 테스트하여 데이터가 백업되었는지 확인합니다.
- 백업에서 데이터를 복원할 수 있는지 확인합니다.
- 재해 복구 계획을 검증하여 잠재적인 서버 손실에 충분히 대비할 수 있도록 합니다.

Red Hat Insights 사용

Red Hat Insights를 사용하여 업그레이드 적격성을 확인할 수 있습니다.

Red Hat Satellite 서버 활용

Red Hat Satellite 서버는 Leapp 플러그인을 활용하여 적격 시스템을 대규모로 검사하고 업그레이드할 수 있습니다.

웹 콘솔 사용

업그레이드 프로세스를 용이하게 진행하려면 웹 콘솔을 사용하는 것이 좋습니다. 사전 업그레이드 리포트를 읽기 쉬운 형식으로 제공하기 때문입니다.

yum install cockpit cockpit-leapp을 사용하여 cockpit 및 cockpit-leapp 패키지가 설치되어 있는지 확인해야 합니다.

그런 다음 **systemctl enable --now cockpit.socket**을 사용하여 cockpit 소켓을 활성화합니다.

firewall-cmd --add-port 9090/tcp를 사용하여 방화벽에 웹 콘솔 포트를 추가한 다음 **firewall-cmd --add-port 9090/tcp --permanent**를 사용하여 영구 방화벽 구성에 규칙이 추가되었는지 확인합니다.

*https://your_server_name:9090*에서 웹 콘솔에 로그인합니다.

Satellite 리포지토리 요구 사항

Satellite 서버를 사용하여 패키지를 관리하는 경우 다음 리포지토리를 사용할 수 있는지 확인합니다.

- rhel-7-server-rpms
- rhel-7-server-extras-rpms
- rhel-8-for-x86_64-baseos-rpms
- rhel-8-for-x86_64-appstream-rpms

yum versionlock

yum versionlock 명령을 사용하여 패키지를 특정 버전으로 잠근 경우, **yum versionlock clear**를 사용하여 이러한 잠금을 해제합니다.

www.facebook.com/redhatkorea
구매문의 080 708 0880
buy-kr@redhat.com