Leapp – Überblick

Leapp ist das unterstützte Tool, mit dem In-Place-System-Upgrades von einer Hauptversion von Red Hat® Enterprise Linux® zu einer anderen durchgeführt werden. Mit Leapp können Sie Ihr Upgrade sorgenfrei durchführen und von den neuen Funktionen von Red Hat Enterprise Linux profitieren, ohne dass Sie Ihr System neu installieren müssen.

Warum sollte ich ein Upgrade durchführen?

Lesen Sie die Checkliste „Die wichtigsten Gründe für ein Upgrade auf Red Hat Enterprise Linux“

Die Durchführung eines Upgrades sorgt dafür, dass Business Continuity gewährleistet wird und Kunden und Kundinnen von unterstützten Produkten profitieren, die die neuesten Verbesserungen, Fixes, Patches und Funktionen enthalten, die Teil einer neuen Hauptversion von Red Hat Enterprise Linux sind.

Performance-Verbesserungen in Red Hat Enterprise Linux senken Ihre Gesamtbetriebskosten (TCO), beeinflussen die Produktivität und stellen sicher, dass Sie Ihre Investitionen in Technologie maximieren.

Red Hat Enterprise Linux folgt einem prognostizierbaren Dreijahres-Release-Zyklus, und Ihre Subskription ist gültig für alle aktuell unterstützten Versionen von Red Hat Enterprise Linux. Dadurch erhalten Sie Zugriff auf die neuesten Technologien, von denen Sie profitieren können, sobald neue Versionen verfügbar sind. Der Support für eine Hauptversion von Red Hat Enterprise Linux besteht zehn Jahre lang und wird in zwei Support-Phasen unterteilt.

Die erste Phase, die ab der allgemeinen Verfügbarkeit (General Availability, GA) fünf Jahre lang dauert, wird als „Vollständiger Support“ bezeichnet. Neue Funktionen werden hinzugefügt, neue Hardware wird unterstützt, Probleme und Bugs werden behoben. Danach geht das Release für die nächsten fünf Jahre in den Wartungssupport über. In dieser Phase werden weiterhin kritische und wichtige Sicherheits-Errata und weitere ausgewählte Funktionen oder Bugfix-Erweiterungen veröffentlicht. Wenn der normale Lifecycle von zehn Jahren abgeschlossen ist, können Kunden und Kundinnen ein Red Hat Extended Life Cycle Support Add-On erwerben, mit dem sie zwei zusätzliche Jahre Support erhalten, in denen kritische und wichtige Sicherheits-Errata enthalten sind. Besuchen Sie die Seite mit dem Red Hat Enterprise Linux Lifecycle für weitere Details.

Kunden und Kundinnen profitieren von vielen neuen Funktionen, wenn Sie ein Upgrade auf Red Hat Enterprise Linux durchführen, darunter:

- Aktualisierte Software, die von Anwendungsstreams bereitgestellt wird, bietet während der gesamten Phase mit vollständigem Support einer Red Hat Enterprise Linux Hauptversion neuere Sprach-Runtimes, Datenbanken und andere Anwendungen.
- Red Hat Enterprise Linux Container-Tools, wie beispielsweise Podman, Buildah und Skopeo, die Erstellung, Deployment, und Management von Containern unterstützen.
- Kernel-Live-Patching (kpatch), das Ihnen das Patching des Kernels für ausgewählte wichtige und kritische CVEs (Common Vulnerabilities and Exposures) ermöglicht, ohne dass Sie einen Neustart durchführen müssen.

- Performance-Observability-Tools, die eBPF-basierte Tools verwenden, um schnell Insights in Aspekte der Systemperformance zu erhalten.
- Flatpack-Support, um Anwendungen auszuführen, die normalerweise für Desktop-Anwendungen genutzt werden.
- 2Cgroup2, das optimierte Funktionen zur Regulierung von Ressourcen bietet, die von Prozessen verbraucht werden.

Es gibt zahlreiche Automatisierungs- und Managementverbesserungen, darunter eine verbesserte Webkonsolenoberfläche für einfachere Administration.

Enthaltene Automatisierungsverbesserungen:

- Neue Systemrollen für Red Hat Enterprise Linux, basierend auf Red Hat Ansible® Automation Platform, um Management in großem Umfang zu automatisieren.
- Red Hat Insights, das Teil der Red Hat Enterprise Linux Subskription ist und proaktiv nach Schwachstellen, Rollenversäumnissen und anderen vordefinierten Kriterien sucht.

Unternehmen, die das Potenzial ihrer Hardware voll ausschöpfen möchten, sollten wissen, dass Red Hat Enterprise Linux 9 im Allgemeinen eine bessere Performance bietet als Red Hat Enterprise Linux 7 und Red Hat Enterprise Linux 8. Dies ist unter anderem durch diese Änderungen möglich:

- Neue Disk Elevators für den Kernel
- Optimierte Performance-Profile

Produktinformationen finden Sie unter Upgrade von Red Hat Enterprise Linux 6 auf Red Hat Enterprise Linux 8.

Was ist Leapp und warum sollte ich es verwenden?

Ein Upgrade Ihrer Server kann eine Herausforderung sein. Aber Red Hat Enterprise Linux enthält das unterstützte Upgrade-Managementtool Leapp, mit dem Sie über einen zentralen Prozess ein Upgrade auf die nächste Hauptversion von Red Hat Enterprise Linux durchführen können. Mit Leapp können Kunden die ursprüngliche Subskription, die mit dem System verknüpft ist, sowie Systemkonfigurationen, benutzerdefinierte Repositories und Drittanbieteranwendungen beibehalten.

Leapp ist in Red Hat Enterprise Linux 7 und Red Hat Enterprise Linux 8 enthalten und ermöglicht Ihnen ein Upgrade von Red Hat Enterprise Linux 7.9 auf Red Hat Enterprise Linux 8. Es kann außerdem dazu verwendet werden, ein Upgrade von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9 durchzuführen.

Falls Sie Red Hat Enterprise Linux 6 verwenden, müssen Sie mit anderen Tools ein Upgrade auf Red Hat Enterprise Linux 7 durchführen, bevor Sie mit Leapp ein Upgrade auf Red Hat Enterprise Linux 8 oder Red Hat Enterprise Linux 9 durchführen können.

Die folgende Tabelle zeigt die Vorteile eines Server-Upgrades mit Leapp.

In-Place-Upgrade mit Leapp	Neuinstallation
Konfiguration wird beibehalten	Konfigurationsdaten müssen gesichert und neu gestartet werden
Bestehende Subskriptionsdaten werden auf Maschinen beibehalten	Maschinen müssen mit subscription-manager abonniert werden
Produktivität wird durch Automatisierung positiv beeinflusst	Zusätzlicher Zeit- und Kostenaufwand

Funktionsweise

Wenn Sie die Funktionsweise von Leapp verstehen, ist es einfacher, ein erfolgreiches Upgrade durchzuführen. Die Verwendung von Leapp ist ein zweistufiger Prozess, der aus einer Analyse der Upgrade-Fähigkeit und dem eigentlichen Upgrade besteht. Nach dem Upgrade sind Neustarts erforderlich, das sollten Sie bei der Planung Ihres Upgrades unbedingt bedenken.

Bei einem einzelnen Host, der Leapp verwendet, basiert die Analyse der Upgrade-Fähigkeit auf Upgrade-Überlegungen, die als Metadaten von *cloud.redhat.com* heruntergeladen werden.

Bei Hosts, die mit Red Hat Satellite verbunden sind, müssen die Metadaten per Satellite an die Server verteilt werden, die Leapp verwenden. Die Analyse der Upgrade-Fähigkeit kann dann in großem Umfang mit dem Leapp-Plugin für Red Hat Satellite durchgeführt werden.

Bei der Analyse der Upgrade-Fähigkeit wird ein Bericht generiert, der möglicherweise Punkte enthält, die Sie vor dem Upgrade beheben müssen.

Leapp verwendet mehrere Python-Programme als Teil eines Workflows. Diese Python-Programme werden „Actors" genannt und können Änderungen an Ihrem System durchführen.

Lesen Sie „Red Hat Satellite für ein Upgrade mit Leapp verwenden"

Ein Beispiel für einen Actor ist **CheckOSRelease**, der überprüft, ob das aktuelle Red Hat Enterprise Linux Neben-Release unterstützt wird. Falls nicht, verhindert er den Upgrade-Prozess.

Wenn Sie eine Upgrade-Überlegung haben, die nicht von einem bestehenden Set von Actors in Betracht gezogen wird, können Sie Ihren eigenen, benutzerdefinierten Actor schreiben, um diese Überlegungen zu lösen, zu verhindern oder Sie über diese zu informieren. Ihr Actor kann dann in den Leapp-Workflow integriert werden.

Leapp ist in Red Hat Insights integriert, um Ihre registrierte Population zu scannen und festzustellen, welche Maschinen für ein Upgrade in Frage kommen.

Ein Upgrade mit Leapp kann über die Befehlszeile oder über Red Hat Satellite durchgeführt werden.

Einschränkungen

Bevor Sie mit dem Upgrade Ihres Servers fortfahren, müssen Sie ein paar wichtige Einschränkungen bei der Verwendung von Leapp berücksichtigen:

- Das Tool kann nur dazu verwendet werden, ein Upgrade von einer Hauptversion von Red Hat Enterprise Linux auf die nächste Hauptversion durchzuführen.
- Leapp funktioniert nicht, wenn Ihr System Festplattenverschlüsselung für das Root-Dateisystem verwendet.
- VDO-Geräte müssen für eine Verwaltung durch LVM konvertiert werden.
- Netzwerkbasierte Multipath- oder Netzwerk-Storage-Mounts wie z. B. iSCSI oder NFS (Network File System) können nicht für eine Systempartition verwendet werden.
- Für On-Demand-Instanzen in der Public Cloud, die Red Hat Update Infrastructure verwenden (die sich von Red Hat Subscription Manager unterscheidet), kann kein Upgrade mit Leapp durchgeführt werden.

Ich bin bereit für das Upgrade. Wo fange ich an?

Schauen wir uns an, wie ein Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 abläuft. Ein Upgrade von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9 hat einen ähnlichen Workflow. Stellen Sie sicher, dass Sie Ihr System mit **yum update** auf Red Hat Enterprise Linux 7.9 aktualisiert haben:

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

Das **leapp**-Paket muss installiert sein. Stellen Sie sicher, dass Ihre Maschine das Red Hat CDN oder Ihren Satellite-Server abonniert hat und der Red Hat Enterprise Linux 7 Extras Channel aktiviert ist. Das können Sie mit diesem Befehl verifizieren:

```
[root@leapp7to8 ~]# subscription-manager repos --list-enabled
+----------------------------------------------------------+
    Verfügbare 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
```

Wenn das Repository „rhel-7-server-extras-rpms“ nicht aktiviert ist, können Sie es wie folgt aktivieren:

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

Leapp kann nun auf Red Hat Enterprise Linux 7 folgendermaßen installiert werden:

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

Wenn Sie ein Upgrade von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9 durchführen, führen Sie die folgenden Schritte aus, um das In-Place-Upgrade-Tool Leapp zu installieren. Red Hat Enterprise Linux 8 Server müssen möglicherweise aktualisiert werden, bevor Sie ein Upgrade auf Red Hat Enterprise Linux 9 durchführen können. Weitere Informationen finden Sie unter Supported in-place upgrade paths for Red Hat Enterprise Linux.

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

Die Pakete **leapp** und **leapp-upgrade-el8toel9** müssen installiert werden. Beide Pakete befinden sich im Repository **rhel-8-for-x86_64-appstream-rpms**. Installieren Sie diese folgendermaßen:

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

Wenn Sie zuvor ein In-Place-Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 durchgeführt haben, entfernen Sie das Verzeichnis **/root/tmp_leapp_py3**, falls es sich auf Ihrem System befindet:

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

Sobald Sie das bzw. die Leapp-In-Place-Upgrade-Paket(e) für Ihr Red Hat Enterprise Linux Release installiert haben, muss Ihr Server vor dem Upgrade mit **leapp preupgrade** analysiert werden, um potenzielle Probleme zu identifizieren. Ihr System bleibt unverändert und erstellt wichtige Dateien, die Ihren Upgrade-Pfad vorgeben.

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

Nachdem Sie den Pre-Upgrade-Befehl ausgeführt haben, wird eine Ausgabe angezeigt, die ungefähr so aussieht:

```
…
 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
```

Beachtenswerte Dateien:

/var/log/leapp/leapp-report.txt	Lesbare und verständliche Informationen über den Leapp-Upgrade-Bericht
/var/log/leapp/leapp-report.json	Das JSON-formatierte Äquivalent
/var/log/leapp/leapp-preupgrade.log	Die Debug-Ausgabe des Befehls „leapp preupgrade“
/var/log/leapp/answerfile	Antworten auf die Fragen, die der Befehl „leapp preupgrade“ stellt

Der Bericht zur Analyse der Upgrade-Fähigkeit wird unter **/var/log/leapp/leapp-report.txt** gespeichert und enthält möglicherweise wichtige Überlegungen, die Sie berücksichtigen sollten, bevor Sie das Upgrade durchführen. Diese Überlegungen erfordern unter Umständen Eingaben von Ihnen, die Sie ausführen können, indem Sie die Anweisungen im Bericht befolgen.

Handhabung der Leapp-Pre-Upgrade-Überlegungen

Möglicherweise enthält der Leapp-Pre-Upgrade-Bericht unter /var/log/leapp/leapp-report.txt verschiedene Aktionspunkte, die Sie angehen müssen. Ein Inhibitor (***inhibitor***) ist ein Faktor, der das Upgrade verhindert und den Sie beheben müssen, um mit dem Upgrade fortzufahren. Wenn Inhibitoren nicht beseitigt werden, wird kein Leapp-Upgrade auf dem System durchgeführt.

Der Risikofaktor (***risk factor***) beschreibt die Auswirkung einer Upgrade-Überlegung mit den folgenden Abstufungen:

High	Sehr hohe Wahrscheinlichkeit für einen verschlechterten Zustand
Medium	Kann Auswirkungen auf das System und auf Anwendungen haben
Low	Sollte keine Auswirkungen auf das System haben, könnte aber Anwendungen betreffen
Info	Information, die keine erwarteten Auswirkungen auf System oder Anwendungen hat.

Der Titel (***title***) identifiziert ein Element des Leapp-Pre-Upgrade-Berichts, und die Zusammenfassung bietet Ihnen weitere Informationen.

Die Zusammenfassung (***summary***) bietet eine kurze Beschreibung des gefundenen Problems, das gelöst werden muss.

Eine Problembehebung (***remediation***) ist eine konkrete Lösung für ein gemeldetes Problem. Häufige Problembehebungs-Typen sind:

- das Bearbeiten einer Konfigurationsdatei
- das Ausführen eines Befehls, der das Verhalten Ihres Systems ändert
- Problembehebung mithilfe der Leapp-Antwortdatei
- Modularitätssoftware zur Problembehebung aus der Red Hat Enterprise Linux 7 Software Collections Library, wie z. B. Python, PHP, Node.js, PostgreSQL, usw.
- das temporäre Unmounten von NFS-Exporten

Beispiele für Upgrade-Überlegungen für hohe und mittlere Risikofaktoren werden in diesem Abschnitt gezeigt und sind folgendermaßen strukturiert:

- Die Meldung, die im Beispielausschnitt des Leapp-Berichts angezeigt wird
- Das betroffene Software-Subsystem
- Eine Erklärung, was das gefundene Element bedeutet
- Maßnahmen, die Sie ergreifen sollten
- Die Konsequenzen, falls Sie das gefundene Element ignorieren

Ihre Systeme zeigen möglicherweise unterschiedliche Überlegungen an, abhängig von Ihrer Konfiguration und der Version von Red Hat Enterprise Linux, auf die Sie ein Upgrade durchführen.

Beispiel 1: Ein Inhibitor mit hohem Risiko, der temporäre Änderungen an Ihrem System erfordert

Dies ist ein Beispiel für ein Inhibitor-Problem, das im Pre-Upgrade-Bericht mit einem hohen Risikofaktor eingestuft wurde. Wenn dieser Fehler nicht behoben wird, endet ein Leapp-Upgrade, das auf diesem System ausgeführt wird, in einer Fehlermeldung, und es wird kein Upgrade auf dem System durchgeführt. Abgesehen von der Meldung sehen wir uns an, wie wir dieses Problem im System lösen.

```
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
```

Was passiert, wenn ich diesen Hinweis ignoriere?

Es handelt sich um einen Inhibitor, der das Upgrade verhindert, bis die notwendigen Maßnahmen durchgeführt wurden. Der Risikofaktor ist hoch, da erwartet wird, dass Änderungen nur am lokalen Server und nicht an NFS-Shares durchgeführt werden.

Welches Subsystem ist betroffen?

NFS-Mounts.

Was bedeutet das?

NFS-Mounts können während des Upgrade-Prozesses nicht verwendet werden. Sie müssen unmounted und deaktiviert werden, bis das Upgrade abgeschlossen wurde.

Was muss ich tun?

Bearbeiten Sie /etc/fstab so, dass NFS-Shares auskommentiert werden, und unmounten Sie aktuell gemountete NFS-Shares. Stoppen und deaktivieren Sie autofs.service temporär. Die NFS-Einträge und autofs.service können wieder aktiviert werden, sobald das Upgrade beendet wurde.

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

Beispiel 2: Ein Inhibitor mit hohem Risiko, der Änderungen an einer bestehenden Konfigurationsdatei erfordert

Dies trifft meistens bei einem Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 zu.

```
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
```

Was passiert, wenn ich diesen Hinweis ignoriere?

Es handelt sich um einen Inhibitor, der das Fortsetzen des Upgrades verhindert. Der Risikofaktor ist allerdings hoch, und wenn Sie dieses Problem nicht korrekt lösen, können Sie sich möglicherweise nicht mehr über Secure Shell (SSH) remote bei Ihrem Server anmelden.

Welches Subsystem ist betroffen?

Der SSH-Server (sshd.service).

Was bedeutet das?

Dieser Ausschnitt gibt an, dass es bei der Funktionsweise des SSH-Servers zwischen Red Hat Enterprise Linux 7 und Red Hat Enterprise Linux 8 eine Veränderung mit großer Auswirkung gibt. Passwort-Authentifizierung ist in Red Hat Enterprise Linux 8 für den Root-Nutzenden standardmäßig nicht zulässig. In Red Hat Enterprise Linux 7 ist der implizierte Standardwert für PermitRootLogin „yes“, aber in Red Hat Enterprise Linux 8 ist der implizierte Standardwert „prohibit-password“.

Eine implizierte Konfigurationsrichtlinie erscheint als Kommentar in /etc/ssh/sshd_config, aber sie ist kein Kommentar. Es scheint eine Information über die Standardwerte der Richtlinie zu sein.

Was muss ich tun?

Stellen Sie sicher, dass sie sich als ein anderer Nutzender einloggen können, entweder mit einem Passwort oder ohne.

Sie müssen einen expliziten Wert für PermitRootLogin in /etc/ssh/sshd_config festlegen. Dieser Wert kann „yes“ sein, um dem Root-Nutzenden eine Anmeldung über SSH zu erlauben, oder „no“, um dies zu verhindern. Das wichtigste ist, dass die Richtlinie explizit festgelegt wird.

Linux-Manpages sind hilfreiche Quellen für zusätzliche Informationen. Verwenden Sie den Befehl **man sshd_config**, und suchen Sie nach der Zeichenfolge *PermitRootLogin*, um mehr über diese Konfigurationsrichtlinie zu erfahren.

Beispiel 3: Ein Inhibitor mit hohem Risiko, der die Verwendung der Leapp-Antwortdatei erfordert

Dieses konkrete Problem entsteht hauptsächlich beim Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8. Das spezielle an diesem Beispiel ist, dass zur Problembehebung die Leapp-Antwortdatei erforderlich ist. Hierbei handelt es sich um eine Datei, in der Daten automatisch an das Leapp-Tool weitergegeben werden können.

```
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
```

Was passiert, wenn ich diesen Hinweis ignoriere?

Es handelt sich um einen Inhibitor, der das Fortsetzen des Upgrades verhindert, bis Sie das Entfernen des Moduls „pam_pkcs11“ autorisieren. Der Risikofaktor ist hoch, da Sie die *benötigten* Kontrollwerte möglicherweise mit dem Modul „pam_pkcs11“ in Ihrer PAM-Konfiguration in Verbindung gebracht haben und das Entfernen dieses Moduls in Red Hat Enterprise Linux 8 Sie eventuell aus Ihrem System ausschließen könnte.

Dieses Upgrade-Problem kann **nur** durch die Verwendung der Leapp-Antwortdatei behoben werden.

Welches Subsystem ist betroffen?

Authentifizierung (pam).

Was bedeutet das?

Dieser Ausschnitt gibt an, dass das Modul „pam_pkcs11“ aus Red Hat Enterprise Linux 8 entfernt wurde und seine Funktionalität nun durch sssd bereitgestellt wird.

Was muss ich tun?

Bearbeiten Sie /var/log/leapp/answerfile folgendermaßen:

```
[remove_pam_pkcs11_module_check]

confirm = True
```

Oder führen Sie den folgenden Befehl aus, um die Antwortdatei /var/log/leapp/answerfile zu bearbeiten:

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

Sie müssen außerdem sicherstellen, dass Ihnen andere Authentifizierungsmöglichkeiten zur Verfügung stehen, die nicht auf dem Modul „pam_pkcs11“ basieren.

Dies können Sie überprüfen, indem Sie **grep pam_pkcs11 /etc/pam.d/*** ausführen.

Unter Managing software from an application stream finden Sie ein praxisorientiertes Lab

Beispiel 4: Ein Faktor mit hohem Risiko, der kein Inhibitor ist, aber nach dem Upgrade Auswirkungen auf Python-Programme hat

Dieses Beispiel betrifft meistens Maschinen, für die ein Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 durchgeführt wird. Im Gegensatz zu den vorherigen Beispielen handelt es sich nicht um einen Inhibitor. Das heißt, dass das Leapp-Upgrade-Tool auch dann ein Upgrade durchführt, wenn dieses festgestellte Problem nicht gelöst wird. Ob dieses Problem gelöst werden muss, wird vom Systemadministrator festgestellt. Ob diese Maschine Python2-basierte Anwendungen verwendet und ob diese Anwendungen mit Python3 kompatibel sind, welches nach dem Upgrade vom Betriebssystem bereitgestellt wird, wird ebenfalls vom Systemadministrator festgestellt.

```
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
```

Was passiert, wenn ich diesen Hinweis ignoriere?

Es handelt sich nicht um einen Inhibitor, und ein Ignorieren der Problembehebung verhindert die Ausführung des Leapp-Upgrade-Befehls nicht. Der Risikofaktor ist hoch, da der unversionierte Python-Befehl (/usr/bin/python) standardmäßig nicht in Red Hat Enterprise Linux 8 zur Verfügung steht. Die direkte (z. B. von einem Terminal) oder indirekte Ausführung des Python-Übersetzers (ein anderer Prozess führt den Befehl für Sie aus) wird nicht erfolgreich ausgeführt.

Welches Subsystem ist betroffen?

Python und Anwendungen, die auf dem unversionierten /usr/bin/python-Befehl aufbauen.

Was bedeutet das?

Python 2 ist im Vergleich zu Python 3 veraltet, kann aber trotzdem mit Anwendungsstreams installiert werden. Das Anwendungsstreams-Repository bietet mehrere Python-Module an, die Sie parallel auf Ihrem Server installieren können. Sie sollten die Version von Python immer angeben, entweder beim Installieren, beim Aufrufen oder bei Interaktionen. Der unversionierte Python-Befehl ist standardmäßig nicht verfügbar, kann aber bei Bedarf trotzdem konfiguriert werden.

Was muss ich tun?

Sie können den folgenden Befehl ausführen, um sicherzustellen, dass /usr/bin/python3 als standardmäßige Version von Python ausgeführt wird:

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

Anwendungen, die explizit Python 2 benötigen, müssen /usr/bin/python2 referenzieren, oder Sie müssen die Standardversion von Python auf Python 2 setzen, indem sie den folgenden Befehl ausführen:

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

Beispiel 5: Ein Faktor mit mittlerem Risiko, der kein Inhibitor ist

Dieses Beispiel trifft meistens bei einem Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 zu.

```
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
```

Was passiert, wenn ich diesen Hinweis ignoriere?

Es handelt sich nicht um einen Inhibitor, der das Fortsetzen des Leapp-Upgrades verhindert. Der Risikofaktor ist mittel, da NTP-Clients (Network Time Protocol), die so konfiguriert sind, dass ihre Zeit von mehreren Servern abgerufen werden, die nicht denselben oder überhaupt keinen Leap-Smear implementieren, während dem Leap-Smear verschiedene Zeiten von verschiedenen Servern erhalten. Dies kann dazu führen, dass NTP-Clients ihre Uhrzeiten nicht mehr aktualisieren oder zufällig zwischen Servern hin- und herspringen.

Welches Subsystem ist betroffen?

Zeitsynchronisierung mit chrony.

Was bedeutet das?

Chrony implementiert die Zeitsynchronisierung mit NTP. In Red Hat Enterprise Linux 8 wird die Pool-Richtlinie standardmäßig dazu verwendet, einen Pool von NTP-Servern mit denselben Funktionen zu referenzieren. Die Verwendung mehrerer Server-Richtlinien, die NTP-Server mit verschiedenen Funktionen referenzieren, könnte zu einer beeinträchtigten Zeitsynchronisierung führen.

Lesen Sie die Checkliste „Die wichtigsten Gründe für ein Upgrade auf Red Hat Enterprise Linux“

Was muss ich tun?

Entfernen Sie alle *leapsectz*- und *leapfile* -Richtlinien aus /etc/chrony.conf, und verwenden Sie die Pool-Richtlinie anstatt der Server-Richtlinie in /etc/chrony.conf. Dadurch stellen Sie sicher, dass NTP-Server mit den gleichen Funktionen verwendet werden.

Wenn Sie Ihre Systemzeit mit explizit definierten Servern synchronisieren möchten, stellen Sie sicher, dass alle Server dieselben Funktionen aufweisen.

Ich bin bereit für ein Upgrade!

Nachdem Sie die Probleme gelöst haben, die im Pre-Upgrade-Bericht aufgelistet wurden, wird eine erneute Ausführung des Befehls **leapp preupgrade** empfohlen. Öffnen Sie außerdem noch einmal die Berichtdatei, um sicherzustellen, dass Sie keine Punkte vergessen haben, die ein erfolgreiches Upgrade verhindern würden.

Sobald Ihr System bereit für das Upgrade ist, führen Sie einen der folgenden Befehle aus: **leapp upgrade** oder **leapp upgrade --reboot**

Rufen Sie What is BOOM and how to install it? auf

Der Befehl **leapp upgrade** leitet den Upgrade-Prozess ein und sein Abschluss erfordert mehrere Neustarts. Es ist wichtig, dass diese mit eingeplant sind. Vor dem ersten Startvorgang können Sie Ihre aktuelle Version von Red Hat Enterprise Linux weiterverwenden.

Weitere Informationen finden Sie unter System-Upgrades mit Snapshots verwalten

Der Befehl **leapp upgrade reboot** führt automatischen einen Neustart des Servers durch.

Erster Start: Der Bootloader initialisiert mit dem Menüeintrag **Red Hat Enterprise Linux-Upgrade-Initramfs** automatisch eine spezielle Upgrade-Umgebung. Innerhalb dieser Upgrade-Umgebung wird das Upgrade auf Ihrem Server durchgeführt. Es wird ein Backup benötigt, falls Sie das Upgrade rückgängig machen und die vorherige Hauptversion von Red Hat Enterprise Linux nutzen möchten.

Zweiter Start: SELinux-Label werden wiederhergestellt, und Ihr Server wird noch einmal neugestartet.

Dritter Start: Sie können Ihr Upgrade überprüfen und Ihr neues Red Hat Enterprise Linux Erlebnis genießen.

Überprüfen Sie, welche Version von Red Hat Enterprise Linux momentan verwendet wird:

```
[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
```

Wenn Sie ein Upgrade von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 durchführen, erwarten Sie vielleicht, ein Repository namens *rhel-8-server-rpms* zu sehen. Allerdings enthält Red Hat Enterprise Linux 8 zwei Repositories: *rhel-8-for-x86_64-baseos-rpms*, welches das Kernset der zugrunde liegenden OS-Funktionalität enthält, und *rhel-8-for-x86_64-appstream-rpms* , welches zusätzliche Userspace-Anwendungen, Runtime-Sprachen und Datenbanken enthält, die verschiedene Workloads und Use Cases unterstützen. Dies kann folgendermaßen verifiziert werden:

```
[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
```

Sobald das Upgrade und ein Neustart Ihres Systems durchgeführt wurden, sollten Sie **/var/log/leapp/leapp-report.txt** erneut öffnen und den Post-Upgrade-Bericht lesen, der möglicherweise zusätzliche Aktionspunkte enthält, die Sie ausführen müssen.

Haben Sie Tipps für mich?

Bevor Sie beginnen, sollten Sie die folgenden Empfehlungen berücksichtigen.

sosreport

Ziehen Sie das Generieren eines sosreport in Betracht, damit wir Ihnen bei Bedarf Support anbieten können.

1. Verwenden Sie **yum install sos**, um sicherzustellen, dass das sos-Paket installiert wird.
2. Generieren Sie den Bericht, indem Sie den Befehl **sosreport** verwenden.
3. Kopieren Sie das generierte TAR-Archiv aus **/var/tmp/** an einen sicheren Speicherort, damit es zur Verfügung steht, falls Sie den Red Hat Support benötigen.

Denken Sie daran, ein Backup zu erstellen

Für den Fall, dass unvorhergesehene Ereignisse eintreten, bei denen Ihr System nicht funktionsfähig oder Ihre Daten nicht zugänglich sind, ist die Möglichkeit für eine zeitnahe Wiederherstellung und eine Wiederaufnahme des Betriebs äußerst wichtig. Datenbackups erleichtern den Wiederherstellungsprozess und sollten bereits von Ihnen durchgeführt worden sein. Aber es ist wichtig zu verstehen, dass Sie Ihre Daten sichern müssen, bevor Sie Leapp dazu verwenden, ein Upgrade Ihrer Server durchzuführen.

Verwenden Sie Ihre aktuellen Tools, um eine Backupstrategie zu implementieren.

- Identifizieren Sie die Daten, die für den Betrieb Ihres Servers relevant sind.
- Erstellen Sie ein Backup Ihrer Daten an einem sicheren Speicherort, der sich außerhalb des Servers befindet, für den ein Upgrade durchgeführt werden soll.
- Testen Sie Ihr Backup, um sicherzustellen, dass Ihre Daten erfolgreich gesichert wurden.
- Stellen Sie sicher, dass Sie aus Ihrem Backup Daten wiederherstellen können.
- Überprüfen Sie Ihren Disaster-Recovery-Plan, um sicherzustellen, dass Sie ausreichend auf einen möglichen Ausfall Ihres Servers vorbereitet sind.

Verwenden Sie Red Hat Insights

Sie können Red Hat Insights dazu verwenden, Ihre Berechtigung für ein Upgrade festzustellen.

Nutzen Sie die Vorteile von Red Hat Satellite Server

Red Hat Satellite Server kann das Leapp-Plugin dazu nutzen, berechtigte Systeme in großem Umfang zu scannen und bei diesen Upgrades durchzuführen.

Verwenden Sie die Webkonsole

Ziehen Sie es in Betracht, die Webkonsole für die Durchführung des Upgradeprozesses zu nutzen, da diese den Pre-Upgrade-Bericht in einem leicht lesbaren Format generiert.

Stellen Sie sicher, dass Sie die Pakete „cockpit" und „cockpit-leapp" mit **yum install cockpit cockpit-leapp** installiert haben.

Verwenden Sie dann **systemctl enable --now cockpit.socket**, um das Cockpit-Socket zu aktivieren.

Fügen Sie den Webkonsolen-Port mit **firewall-cmd --add-port 9090/tcp** zu Ihrer Firewall hinzu, und stellen Sie dann sicher, dass die Regel mit **firewall-cmd --add-port 9090/tcp --permanent** zu Ihrer permanenten Firewall-Konfiguration hinzugefügt wird.

Melden Sie sich jetzt unter *https://your_server_name:9090* bei der Webkonsole an.

Satellite-Repository-Anforderungen

Wenn Sie den Satellite-Server für die Verwaltung von Paketen verwenden, stellen Sie sicher, dass Ihnen die folgenden Repositories zur Verfügung stehen:

- 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

Wenn Sie den Befehl „yum versionlock" verwendet haben, um Pakete auf eine spezifische Version zu beschränken, dann heben Sie diese Beschränkung mit **yum versionlock clear** auf.

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

de.redhat.com
#F31715_0822