Cos'è Leapp

Leggi la checklist "I motivi principali per eseguire l'upgrade a Red Hat Enterprise Linux"

Leapp è uno strumento supportato che permette di eseguire l'upgrade del sistema sul posto da una versione principale di Red Hat® Enterprise Linux® a un'altra e di sfruttare così le ultime funzionalità della piattaforma senza dover reinstallare i sistemi.

Perché è importante eseguire gli upgrade?

Eseguire gli upgrade aiuta a garantire la continuità operativa e permette ai clienti di utilizzare prodotti supportati che dispongono di tutti i miglioramenti, le correzioni, le patch e le funzionalità introdotti con la nuova versione principale di Red Hat Enterprise Linux.

Una piattaforma Red Hat Enterprise Linux più efficiente abbassa il costo totale di proprietà, incrementa la produttività e consente alle organizzazioni di trarre il massimo dal loro investimento tecnologico.

Red Hat Enterprise Linux funziona secondo cicli prevedibili di rilascio delle versioni principali con cadenza triennale e la sottoscrizione resta valida per qualunque versione supportata della piattaforma. In questo modo gli utenti possono accedere sempre alle ultime tecnologie introdotte di volta in volta con le nuove versioni. La durata del supporto per le versioni principali di Red Hat Enterprise Linux è di 10 anni, suddivisi in due fasi distinte.

Per i primi cinque anni successivi alla data di disponibilità generale è previsto il supporto completo (Full Support), che comprende: l'introduzione di nuove funzionalità, il supporto per nuovi componenti hardware e la correzione di problemi e bug. Per i successivi cinque anni è previsto invece il supporto per la manutenzione (Maintenance Support), che comprende: la pubblicazione delle correzioni di sicurezza classificate come critiche e importanti e l'introduzione di un numero selezionato di funzionalità e miglioramenti. Una volta concluso il ciclo di vita decennale standard, è possibile acquistare Red Hat Extended Life Cycle Support Add-On, un'estensione del supporto di ulteriori due anni che include le correzioni di sicurezza critiche e importanti. Per saperne di più, vai alla pagina dedicata al ciclo di vita di Red Hat Enterprise Linux.

L'upgrade di Red Hat Enterprise Linux offre notevoli vantaggi. Ad esempio:

- L'aggiornamento dei software mediante flussi delle applicazioni consente di disporre di runtime dei linguaggi, database e altre applicazioni sempre aggiornati durante tutta la fase di supporto completo delle versioni principali di Red Hat Enterprise Linux.
- Gli strumenti di Red Hat Enterprise Linux come Podman, Buildah e Skopeo supportano la creazione, il deployment e la gestione dei container.
- L'applicazione live delle patch al kernel (kpatch) consente di applicare le patch al kernel per le Common Vulnerabilities and Exposures (CVE) critiche o importanti senza dover riavviare il sistema.

- Gli strumenti basati su tecnologia eBPF permettono di ottenere informazioni dettagliate sulle prestazioni del sistema.
- Il supporto di Flatpak per l'esecuzione di applicazioni che di solito sono utilizzate come applicazioni desktop.
- Cgroup2 che semplifica la regolazione delle risorse utilizzate dai processi.

Sono previsti anche dei miglioramenti relativi alla gestione e all'automazione, come ad esempio l'ottimizzazione dell'interfaccia della web console volta ad agevolare le attività di amministrazione.

Per quanto riguarda l'automazione, i miglioramenti comprendono:

- Nuovi ruoli di sistema per Red Hat Enterprise Linux basati su Red Hat Ansible® Automation Platform concepiti per automatizzare la gestione su larga scala.
- Red Hat Insights, compreso in tutte le sottoscrizioni Red Hat Enterprise Linux, scansiona in maniera proattiva l'ambiente alla ricerca di vulnerabilità, omissioni di ruoli o in base ad altri criteri predefiniti.

Per tutti coloro che desiderano ottenere il massimo dai loro componenti hardware, si ricorda che nel complesso Red Hat Enterprise Linux 9 garantisce prestazioni superiori rispetto alle versioni 7 e 8 della piattaforma. Questo miglioramento è dovuto ad alcuni cambiamenti, tra cui:

- Nuovi elevatori del disco per il kernel.
- Nuovi profili prestazionali ottimizzati.

Per saperne di più, vai alla pagina dedicata all'upgrade da RHEL 6 a RHEL 8.

Cos'è Leapp e perché utilizzarlo?

Eseguire l'upgrade dei server può rivelarsi un compito delicato, ecco perché Red Hat Enterprise Linux comprende Leapp, uno strumento supportato per la gestione degli upgrade che offre un processo unico per l'aggiornamento alla versione principale più recente di Red Hat Enterprise Linux. Con Leapp i clienti riescono a mantenere la sottoscrizione originale (legata al sistema), le configurazioni di sistema, i repository personalizzati e le applicazioni di terze parti.

Leapp è incluso nella versione 7 e nella versione 8 di Red Hat Enterprise Linux. Questo significa che chi esegue l'upgrade da RHEL 7.9 a RHEL 8 oppure da RHEL 8 a RHEL 9, può farlo utilizzando Leapp.

Chi utilizza Red Hat Enterprise Linux 6 invece deve prima aggiornare il sistema alla versione 7 servendosi di altri strumenti e solo allora potrà sfruttare le funzionalità di Leapp per passare alla versione 8 o 9 di RHEL.

Nella tabella di seguito sono riportati i vantaggi derivati dall'upgrade dei server con Leapp.

Upgrade sul posto con Leapp	Reinstallazione
Mantiene la configurazione	Occorre eseguire il backup dei dati della configurazione e riavviarli
Le macchine mantengono i dati della sottoscrizione esistente	Occorre eseguire nuovamente la sottoscrizione delle macchine tramite subscription-manager
Migliora la produttività grazie all'automazione	Richiede più tempo ed è più costoso

Come funziona?

Comprendere il funzionamento di Leapp è essenziale per utilizzare al meglio lo strumento. Il processo di upgrade tramite Leapp si divide in due fasi: un'analisi preliminare sull'attuabilità dell'upgrade e l'upgrade vero e proprio. Al termine del processo inoltre sarà necessario riavviare più volte il sistema e questo è un punto importante da tenere a mente quando si pianifica l'upgrade.

Quando è un singolo host a utilizzare Leapp, le osservazioni sull'upgrade frutto dell'analisi preliminare vengono scaricate come metadati da *cloud.redhat.com*

Quando si hanno più host connessi a Red Hat Satellite, è Satellite a distribuire i metadati tra i server che utilizzano Leapp. Si può poi eseguire l'analisi preliminare su larga scala tramite il plugin Leapp presente in Red Hat Satellite.

L'analisi preliminare genera un report che elenca tutti gli aspetti da sistemare prima di poter procedere all'upgrade.

Per un flusso di lavoro Leapp si serve di numerosi programmi Python. Questi programmi, che prendono il nome di attori, possono apportare modifiche ai sistemi.

Leggi "Esegui l'upgrade di RHEL con Red Hat Satellite e Leapp"

Ad esempio, uno degli attori è **CheckOSRelease** che si occupa di controllare che la versione minore in uso di Red Hat Enterprise Linux sia supportata. Se non è supportata, l'attore blocca il processo di upgrade.

Se gli attori esistenti non coprono tutte le osservazioni sull'upgrade, è possibile crearne di personalizzati che correggano, blocchino l'upgrade o notifichino la mancata conformità del sistema e incorporarli nel flusso di lavoro di Leapp.

Leapp si integra con Red Hat Insights per scansionare l'insieme delle macchine registrate e stabilire quali sono quelle idonee per l'upgrade.

È possibile eseguire l'upgrade con Leapp tramite riga di comando o Red Hat Satellite.

Limitazioni

Prima di procedere all'upgrade, occorre tenere a mente che esistono alcune limitazioni all'utilizzo di Leapp:

- Leapp può essere utilizzato esclusivamente per l'upgrade tra una versione principale di Red Hat Enterprise Linux e la successiva versione principale.
- Leapp non funziona sui sistemi che utilizzano la crittografia del disco per il file system root.
- I dispositivi VDO devono essere convertiti perché siano amministrabili dal gestore logico dei volumi (LVM).
- Il multipath basato su rete o i montaggi di storage di rete come iSCSI o NFS non si possono utilizzare come partizione di sistema.
- Le istanze on demand nel cloud pubblico che utilizzano Red Hat Update Infrastructure (da non confondere con Red Hat Subscription Manager) non sono idonee all'upgrade tramite Leapp.

Eseguire l'upgrade: fase 1

Esaminiamo i passaggi necessari per l'upgrade da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8. Per quanto riguarda l'upgrade dalla versione 8 alla versione 9, il flusso di lavoro è molto simile. Assicurati di aver aggiornato il sistema alla versione Red Hat Enterprise Linux 7.9 utilizzando **yum update**:

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

A questo punto è necessario installare il pacchetto **leapp**. Prima però assicurati che la macchina disponga di una sottoscrizione a Red Hat CDN o al tuo server Satellite e che il canale Red Hat Enterprise Linux 7 Extras sia abilitato. Per verificare tali requisiti utilizza il comando:

```
[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
```

Se il repository rhel-7-server-extras-rpms è disabilitato, abilitalo utilizzando:

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

Procedi quindi all'installazione di Leapp su Red Hat Enterprise Linux 7 utilizzando il comando:

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

Per chi esegue l'upgrade da Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9, riportiamo di seguito la procedura per l'installazione della utility per l'upgrade sul posto di Leapp. Prima di eseguire l'upgrade alla versione 9 potrebbe essere necessario aggiornare i server Red Hat Enterprise Linux 8. Per saperne di più, vai alla pagina Processi di upgrade sul posto supportati per Red Hat Enterprise Linux.

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

Procedi all'installazione dei pacchetti **leapp** e **leapp-upgrade-el8toel9**, disponibili nel repository **rhel-8-for-x86_64-appstream-rpms**, utilizzando il comando:

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

Se hai eseguito in precedenza l'upgrade sul posto da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8, nel sistema potrebbe essere presente la directory **/root/tmp_leapp_py3**. Rimuovila con il comando:

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

Dopo aver installato il pacchetto, o i pacchetti, per l'upgrade sul posto di Leapp adatti alla versione di Red Hat Enterprise Linux, analizza il server con **leapp preupgrade** per individuare eventuali problemi prima di procedere all'upgrade. Il comando non apporta modifiche al sistema ma genera file importanti che delineeranno il processo di upgrade.

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

Il comando preupgrade genera un output simile all'esempio riportato di seguito:

```
…
 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
```

File importanti:

/var/log/leapp/leapp-report.txt	Report chiaro e comprensibile circa l'attuabilità dell'upgrade
/var/log/leapp/leapp-report.json	Lo stesso file in formato JSON
/var/log/leapp/leapp-preupgrade.log	Output del debug eseguito dal comando leapp preupgrade
/var/log/leapp/answerfile	Risposte alle domande poste dal comando leapp upgrade

Il report generato in seguito all'analisi preliminare, disponibile al percorso **/var/log/leapp/leapp-report.txt**, elenca una serie di osservazioni sugli aspetti da sistemare prima di poter eseguire l'upgrade e spiega come procedere per risolvere i problemi.

Comprendere le osservazioni generate dall'analisi preliminare di Leapp

Il report generato dall'analisi preliminare di Leapp, disponibile al percorso /var/log/leapp/leapp-report.txt, contiene diverse indicazioni utili per comprendere e risolvere le non conformità. Definiamo di seguito le voci che compongono ciascuna osservazione. Un ***inhibitor*** (inibitore) è un aspetto che si deve obbligatoriamente correggere prima di poter continuare la procedura di upgrade. In caso contrario, Leapp non permette di eseguire l'upgrade del sistema.

Il ***risk factor*** (fattore di rischio) descrive la gravità e l'impatto dei problemi secondo la seguente scala di valori:

High	È altamente probabile che comprometta il funzionamento del sistema
Medium	Potrebbe compromettere il sistema e le applicazioni
Low	Non dovrebbe compromettere il sistema ma potrebbe influire sulle applicazioni
Info	Segnalazione a scopo informativo. Non dovrebbe compromettere né il sistema né le applicazioni

Il ***title*** (titolo) offre una descrizione sintetica del problema rilevato dall'analisi preliminare.

Il ***summary*** (riassunto) approfondisce il title offendo maggiori informazioni sulla natura del problema rilevato.

La ***remediation*** (correzione) fornisce una soluzione pratica per risolvere il problema rilevato. Di seguito un elenco delle correzioni più frequenti:

- Modificare un file di configurazione.
- Eseguire un comando che modifica il comportamento del sistema.
- Applicare una correzione tramite l'answerfile di Leapp.
- Applicare una correzione che influisce sui software di modularità della Software Collections Library di Red Hat Enterprise Linux 7, come Python, PHP, Node.js, PostgreSQL, ecc.
- Smontare temporaneamente le esportazioni NFS.

Di seguito presenteremo alcuni esempi di problemi rilevati dall'analisi preliminare con fattore di rischio medio o alto. Per ciascun esempio sono indicati:

- Il messaggio presente nel report di Leapp.
- Il sottosistema del software interessato.
- Una spiegazione del problema rilevato.
- L'intervento necessario per risolvere il problema.
- Le conseguenze se si ignora il problema.

Le osservazioni notificate possono variare a seconda della versione di Red Hat Enterprise Linux in uso e della configurazione.

Esempio 1: un inibitore ad alto rischio che richiede di modificare temporaneamente il sistema

In questo caso l'analisi preliminare ha rilevato una non conformità classificata come inibitore ad alto rischio. La mancata correzione del problema genera un errore durante l'esecuzione di Leapp sul sistema e non consente di portare a termine l'upgrade. Di seguito riportiamo non solo il messaggio di Leapp, ma esaminiamo anche in maniera dettagliata come risolvere il problema nel sistema.

```
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
```

Cosa succede se ignoro l'avviso?

Si tratta di un inibitore e non è quindi possibile procedere con l'upgrade se prima non si applicano le correzioni necessarie. Il fattore di rischio è alto perché occorre apportare le modifiche solo al server locale e non alle condivisioni NFS.

Qual è il sottosistema interessato?

I montaggi NFS.

Cosa significa?

I montaggi NFS non si possono utilizzare durante l'upgrade. Occorre smontarli e disabilitarli fino al termine del processo.

Come devo procedere?

Modifica /etc/fstab per impostare temporaneamente le condivisioni NFS come commenti e smonta le condivisioni NFS montate. Interrompi e disabilita temporaneamente autofs.service. Una volta concluso l'upgrade, puoi riabilitare le condivisioni NFS e autofs.service.

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

Esempio 2: un inibitore ad alto rischio che richiede di modificare un file di configurazione esistente

Questo tipo di non conformità si riscontra spesso nell'upgrade da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8.

```
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
```

Cosa succede se ignoro l'avviso?

Si tratta di un inibitore e non è quindi possibile procedere con l'upgrade se prima non si applicano le correzioni necessarie. Considera inoltre che il fattore di rischio è alto e che una gestione inadeguata del problema potrebbe impedire l'accesso remoto al server tramite Secure Shell (SSH).

Qual è il sottosistema interessato?

Il server SSH (sshd.service).

Cosa significa?

L'avviso riportato sopra spiega che esiste una differenza sostanziale nel funzionamento del server SSH tra Red Hat Enterprise Linux 7 e Red Hat Enterprise Linux 8. Per impostazione predefinita, in RHEL 8 l'autenticazione con password è disabilitata per l'utente root. In RHEL 7 il valore predefinito implicito per PermitRootLogin è yes, mentre in RHEL 8 il valore predefinito implicito è prohibit-password.

All'interno di /etc/ssh/sshd_config è presente una direttiva di configurazione implicita sotto forma di commento, ma non è un commento. Serve per far sapere i valori predefiniti della direttiva.

Come devo procedere?

Assicurati di riuscire a effettuare l'accesso, con o senza password, come altro utente.

Definisci in modo esplicito un valore per PermitRootLogin all'interno di /etc/ssh/sshd_config. Imposta yes per consentire all'utente root di accedere tramite SSH oppure no per impedirglielo. L'importante è che la direttiva sia definita in modo esplicito.

Le pagine di manuale di Linux sono un valido alleato. Per saperne di più sulla direttiva di configurazione, esegui il comando **man sshd_config** e cerca la stringa *PermitRootLogin*.

Esempio 3: un inibitore ad alto rischio che richiede l'utilizzo dell'answerfile di Leapp

Questo tipo di non conformità si riscontra spesso nell'upgrade da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8. La peculiarità di questo esempio sta nel fatto che la risoluzione prevede l'utilizzo dell'answerfile di Leapp, un file i cui i dati si possono trasferire automaticamente alla utility di Leapp.

```
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
```

Cosa succede se ignoro l'avviso?

Si tratta di un inibitore e non è quindi possibile procedere con l'upgrade se prima non si autorizza la rimozione del modulo pam_pkcs11. Il fattore di rischio è alto perché è probabile che i valori di controllo *requisite o required* associati al modulo pam_pkcs11 siano nella configurazione PAM, e quindi la rimozione del modulo da Red Hat Enterprise Linux 8 potrebbe impedire l'accesso al sistema.

È possibile risolvere il problema **solo** utilizzando l'answerfile di Leapp.

Qual è il sottosistema interessato?

L'autenticazione (pam).

Cosa significa?

L'avviso riportato sopra spiega che il modulo pam_pkcs11 è stato rimosso da Red Hat Enterprise Linux 8 e ora è SSSD a svolgere le sue funzioni.

Come devo procedere?

Modifica /var/log/leapp/answerfile in questo modo:

```
[remove_pam_pkcs11_module_check]

confirm = True
```

Oppure modifica l'answerfile /var/log/leapp/answerfile con il comando seguente:

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

Assicurati anche di disporre di modalità di autenticazione alternative non vincolate al modulo pam_pkcs11.

Per verificare la presenza di modalità di autenticazione alternative, esegui **grep pam_pkcs11 /etc/pam.d/***

Vai al laboratorio pratico
Managing software from an application stream

Esempio 4: un problema non inibitore ma ad alto rischio che compromette il funzionamento dei programmi Python dopo l'upgrade

Questo tipo di non conformità si riscontra spesso nell'upgrade delle macchine da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8. A differenza degli esempi precedenti, non si tratta di un inibitore. Questo significa che Leapp esegue comunque l'upgrade anche se la criticità non viene risolta. È l'amministratore di sistema, che sa se la macchina utilizza applicazioni basate su Python 2 e se tali applicazioni sono compatibili con Python 3 fornito dalla nuova versione del sistema operativo, a stabilire se il problema costituisce effettivamente un rischio per l'upgrade e se occorre intervenire o meno.

```
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
```

Cosa succede se ignoro l'avviso?

Non si tratta di un inibitore. Questo significa che Leapp esegue comunque l'upgrade anche se la criticità non viene risolta. Il fattore di rischio è alto perché in Red Hat Enterprise Linux 8 il comando python senza versione (/usr/bin/python) non è disponibile per impostazione predefinita. Non è possibile eseguire l'interprete Python né direttamente (ad es. da un terminale) né indirettamente (un altro processo esegue il comando).

Qual è il sottosistema interessato?

Python e tutte le applicazioni che dipendono dal comando senza versione /usr/bin/python.

Cosa significa?

Python 2 è stato deprecato a favore di Python 3, ma è ancora possibile installarlo tramite i flussi delle applicazioni. Il repository dei flussi delle applicazioni offre diversi moduli Python che si possono installare in contemporanea sul server. Quando installi, richiami o interagisci con Python, assicurati sempre di specificare la versione del programma. Per impostazione predefinita il comando python senza versione non è disponibile, ma è possibile configurarlo.

Come devo procedere?

Esegui il comando seguente per assicurarti che la versione predefinita di Python sia /usr/bin/python3:

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

Tutte le applicazioni che richiedono esplicitamente Python 2 devono fare riferimento a /usr/bin/python2. In alternativa, è possibile impostare Python 2 come versione predefinita di Python utilizzando il comando seguente:

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

Esempio 5: un problema non inibitore a rischio medio

Questo tipo di non conformità si riscontra spesso nell'upgrade da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8.

```
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
```

Cosa succede se ignoro l'avviso?

Non si tratta di un inibitore. Questo significa che Leapp esegue comunque l'upgrade anche se la criticità non viene risolta. Il fattore di rischio è medio perché i client Network Time Protocol (NTP), che sono configurati per ottenere l'ora da più server, finiscono per ricevere orari diversi dai diversi server se questi non implementano lo stesso leap smear. Il rischio è che i client smettano di aggiornare gli orologi o passino da un server all'altro in modo casuale.

Qual è il sottosistema interessato?

La sincronizzazione dell'ora con Chrony.

Cosa significa?

Chrony implementa la sincronizzazione dell'ora utilizzando NTP. Per impostazione predefinita, Red Hat Enterprise Linux 8 utilizza la direttiva pool per fare riferimento a un pool di server NTP con le stesse capacità. Utilizzare più direttive server che fanno riferimento a server NTP con capacità diverse può causare problemi con la sincronizzazione dell'ora.

Come devo procedere?

Rimuovi le direttive *leapsectz* e *leapfile* da /etc/chrony.conf e utilizza le direttive pool invece delle direttive server. In questo modo verranno utilizzati solo server NTP con le stesse capacità.

Se desideri sincronizzare l'ora di sistema con server definiti in modo esplicito, assicurati che tutti i server abbiano le stesse capacità.

Leggi la checklist "I motivi principali per eseguire l'upgrade a Red Hat Enterprise Linux"

Eseguire l'upgrade: fase 2

Dopo aver sistemato i problemi rilevati dall'analisi preliminare, esegui nuovamente il comando **leapp preupgrade** e ricontrolla il report per assicurarti di non aver dimenticato nulla che potrebbe compromettere l'upgrade.

A questo punto il sistema e pronto per l'upgrade. Esegui il comando **leapp upgrade** oppure **leapp upgrade --reboot**

Quando pianifichi l'upgrade, tieni a mente che il comando **leapp upgrade** richiederà di riavviare più volte il sistema al termine del processo. È possibile continuare a utilizzare la versione di Red Hat Enterprise Linux esistente fino al primo riavvio.

Il comando **leapp upgrade reboot** riavvia i server in automatico.

Primo riavvio: il bootloader inizializza in automatico un ambiente di upgrade speciale utilizzando la voce del menu **Red Hat Enterprise Linux-Upgrade-Initramfs**. In questo ambiente avverrà l'upgrade dei server. Assicurati di eseguire un backup per poter eventualmente annullare l'upgrade e tornare a utilizzare la versione principale precedente di Red Hat Enterprise Linux.

Secondo riavvio: vengono ripristinate le etichette SELinux e si procede al successivo riavvio.

Terzo riavvio: convalida l'upgrade e scopri le nuove incredibili funzionalità di Red Hat Enterprise Linux.

Convalida la versione di Red Hat Enterprise Linux in uso:

```
[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
```

Chi esegue l'upgrade da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 vedrà un repository chiamato *rhel-8-server-rpms*. Red Hat Enterprise Linux 8 però dispone di due repository: *rhel-8-for-x86_64-baseos-rpms*, che raccoglie le funzionalità principali per il sistema operativo sottostante, e *rhel-8-for-x86_64-appstream-rpms*, che comprende applicazioni per lo spazio utente, linguaggi del runtime e database aggiuntivi ideali per supportare un'ampia gamma di carichi di lavoro e scenari di utilizzo. Per verificare la presenza dei repository:

```
[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
```

Via alla pagina Cos'è BOOM e come si installa?

Scopri di più sulla gestione degli upgrade di sistema con gli snapshot

```
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
```

Dopo aver eseguito l'upgrade e riavviato il sistema, consulta nuovamente **/var/log/leapp/leapp-report.txt**. Qui troverai un report conclusivo che elenca gli interventi necessari per poter ultimare l'upgrade.

Consigli utili

Prima di iniziare l'upgrade, dai un'occhiata ai consigli riportati di seguito.

sosreport

Crea un sosreport. In questo modo potremo offrirti assistenza in caso di necessità.

1. Utilizza **yum install sos** per assicurarti che il pacchetto sos sia installato.
2. Esegui il comando **sosreport** per generare il report.
3. Crea una copia dell'archivio tar da **/var/tmp/** e salvala in una posizione sicura per usufruire di Red Hat Support.

Assicurati di avere un backup

In caso si verificassero circostanze impreviste o malfunzionamenti del sistema o fosse impossibile accedere ai dati, la capacità di ripristinare tempestivamente il sistema e l'operatività è essenziale. I backup dei dati facilitano il processo di ripristino ed è importante eseguirli con regolarità. Per evitare spiacevoli inconvenienti, si consiglia quindi di adottare una strategia di backup dei dati prima di eseguire l'upgrade tramite Leapp.

Sfrutta gli strumenti in uso per adottare una strategia di backup.

- Individua i dati necessari per l'operatività del server.
- Archivia il backup dei dati in una posizione sicura esterna al server che subirà l'upgrade.
- Testa il backup per verificare che sia stato eseguito correttamente.
- Assicurati di riuscire effettivamente a ripristinare i dati dal backup.
- Pianifica il ripristino di emergenza e testane la bontà per assicurarti di riuscire a gestire al meglio eventuali malfunzionamenti del server.

Utilizza Red Hat Insights

Red Hat Insights è un valido strumento per determinare se si hanno i requisiti per l'upgrade.

Usufruisci di Red Hat Satellite Server

Utilizza il plugin Leapp presente in Red Hat Satellite Server per valutare l'idoneità dei sistemi ed eseguire l'upgrade su larga scala.

Prova la web console

La web console semplifica il processo di upgrade perché presenta il report generato dall'analisi preliminare in un formato di facile lettura.

Assicurati di aver installato i pacchetti cockpit e cockpit-leapp utilizzando il comando **yum install cockpit cockpit-leapp**.

Esegui poi il comando **systemctl enable --now cockpit.socket** per attivare il socket di Cockpit.

Aggiungi la porta della web console al firewall utilizzando il comando **firewall-cmd --add-port 9090/tcp** e poi assicurati che la regola sia presente nella configurazione del firewall permanente utilizzando **firewall-cmd --add-port 9090/tcp --permanent**.

Una volta conclusi i passaggi precedenti, accedi alla web console da *https://your_server_name:9090*

I repository di Satellite

Se utilizzi Satellite Server per la gestione dei pacchetti, assicurati di disporre dei seguenti repository:

- 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

Se hai usato il comando yum versionlock per bloccare i pacchetti in una specifica versione, puoi utilizzare **yum versionlock clear** per eliminare il blocco.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software enterprise open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e cloud ibrido caratterizzate da affidabilità e prestazioni elevate. Red Hat consente di sviluppare applicazioni cloud native, integrare applicazioni IT nuove ed esistenti, e automatizzare e gestire ambienti complessi. Considerata un partner affidabile dalle aziende della classifica Fortune 500, Red Hat fornisce pluripremiati servizi di consulenza, formazione e assistenza, che portano i vantaggi dell'innovazione open source in qualsiasi settore. Red Hat è l'elemento catalizzatore in una rete globale di aziende, partner e community, e permette alle organizzazioni di crescere, evolversi e prepararsi a un futuro digitale.

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE,
E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

it.redhat.com
#F31715_0822