Mise à jour Patch Sécurité OS Redhat et CentOS

07/2019
AMT/PTD/NMA/0062/5/1/FR

Avertissement

Bien que les informations contenues dans ce document soient considérées comme pertinentes, Mitel Networks Corporation (MITEL ®) ne peut en garantir l'exactitude.

Les informations sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées de quelque façon que ce soit comme un engagement de Mitel, de ses entreprises affiliées ou de ses filiales.

Mitel, ses entreprises affiliées et ses filiales ne sauraient être tenus responsables des erreurs ou omissions que pourrait comporter ce document. Celui-ci peut être revu ou réédité à tout moment afin d'y apporter des modifications.

SOMMAIRE

1.1 INTRODUCTION

Ce document décrit la mise à jour des patchs de sécurité pour les OS Redhat Enterprise ou CentOS 7.x relativement aux environnements MiVoice 5000 Server et MiVoice 5000 Manager respectivement en R6.3 / 3.3 minimum

Cas des systèmes redondés

Dans le cas d'un système redondé, la mise à jour est à effectuer sur les machines Maitre et Esclave (MiVoice 5000 Server ou MiVoice 5000 Manager) avec les préconisations indiquées au paragraphe 1.4 :

- Dans le cas du MiVoice 5000 Manager, il est impératif de commencer la mise à jour des patchs sur la machine **maitre** (active).
- Dans le cas d'un système MiVoice 5000 Server redondé, il est recommandé de commencer la mise à jour sur la machine esclave (inactive) afin de minimiser les interruptions de service.

1.2 PROCÉDURE POUR OS REDHAT ENTERPRISE

1.2.1 PRÉ-REQUIS

- Disposer d'une machine en R6.3 / 3.3 minimum (sous RedHat 7.x avec 2 ≤ x).
- Disposer d'au moins 2 Go disponibles sur la partition « / ».

Dans le cas de RedHat, le serveur doit être enregistré sous Red Hat Subscription Manager (RHSM). Si ce n'est pas le cas il faut inscrire la machine AVANT d'utiliser le package 'Security Patches'. Dans le cas de RedHat, si la machine n'est pas déjà inscrite sous RHSM, inscrire la machine à RHSM via la commande « **subscription-manager** ».

Cette commande permet l'inscription au canal de base de mise à jour. Il faut aussi inscrire la machine au canal « optionnel » de mise à jour, via la commande « **subscription-manager** »

Pour pouvoir profiter des mises à jour de tous les paquetages dans un environnement redondé, l'abonnement auprès de RedHat doit inclure le add-on « **HighAvailability »**.

La machine doit disposer d'un accès Internet.

1.2.2 PROCÉDURE

ATTENTION : Effectuer préalablement une sauvegarde de la configuration.

En fonction du nombre de patchs et de la connexion internet, la durée de la procédure variera. A titre indicatif, il faut compter au moins 30 mn.

- Se connecter sous le login « **root** ».
- Monter l'image ISO fournie pour les machines avec accès Internet :

securityPatch7.x.yy.iso

(où **7.x** signifie OS en version 7.x et **yy** est à remplacer par l'édition du DVD de patchs).

- Dans une fenêtre « **Terminal** », se déplacer à la racine du montage de l'image ISO, puis exécuter la commande « **./installClientWeb.sh** ».
- Démonter l'image ISO.
- Effectuer un reboot de la machine.

1.3 PROCÉDURE POUR CENTOS

1.3.1 PRÉ-REQUIS

- Disposer d'une machine en R6.3 / 3.3 minimum (sous CentOS 7.x avec 2 ≤ x).
- Disposer d'au moins 2 Go disponibles sur la partition « / ».

1.3.2 MACHINE AVEC ACCÈS INTERNET

ATTENTION : Effectuer préalablement une sauvegarde de la configuration.

En fonction du nombre de patchs et de la connexion internet, la durée de la procédure variera. A titre indicatif, il faut compter au moins 30 mn.

- Se connecter sous le login « **root** ».
- Monter l'image ISO fournie pour les machines avec accès Internet :

  securityPatch6.x.yy.iso

  (où **6.x** signifie OS en version 6.x et **yy** est à remplacer par l'édition du DVD de patchs).
- Dans une fenêtre « **Terminal** », se déplacer à la racine du montage de l'image ISO, puis exécuter la commande « **./installClientWeb.sh** ».
- Démonter l'image ISO.
- Effectuer un reboot de la machine.

1.3.3 MACHINE SANS ACCÈS INTERNET

Rappel : Ce paragraphe ne concerne que CentOS.

ATTENTION : Effectuer préalablement une sauvegarde de la configuration.

- Se connecter sous le login « **root** ».
- Monter l'image ISO fournie pour les machines sans accès Internet :

  securityPatch7.x.yy_Private.iso

  (où **6.x** signifie OS en version 6.x et **yy** est à remplacer par l'édition du DVD de patchs).
- Dans une fenêtre « **Terminal** », se déplacer à la racine du montage de l'image ISO ou du DVD, puis exécuter la commande « **./installClientPrivate.sh** ».
- Démonter l'image ISO.
- Effectuer un reboot de la machine.

1.4 CAS DES SYSTÈMES REDONDÉS

ATTENTION : La procédure est différente selon le type d'application MiVoice 5000 Manager et MiVoice 5000 Server.

1.4.1 CAS D'UN SYSTÈME MIVOICE 5000 MANAGER REDONDÉ

Dans le cas du MiVoice 5000 Manager, il est impératif de commencer la mise à jour des patchs sur la machine **maitre** (active).

Procédure détaillée :

Sur la machine Active > Maitre :

- Machine active (**maitre**) vérifier état de la duplication (**cat /proc/drbd**).
- Vérification : **cat /proc/drbd** (Primary/Secondary) sur la machine active (**maitre**).
- Installer les patchs sur la machine active (**maitre**) en se référant aux paragraphes 1.2 et 1.3.
- Vérifier les log installations des patch (sous **/tmp**) sur la machine active (**maitre**). Se référer au paragraphe 1.5.
- Reboot de la machine (**maitre**).
- Dans le cas d'une machine virtuelle, contrôler que les VMWARE TOOLS sont actifs, sinon réinstaller les VMWARE TOOLS et effectuer un reboot (machine **maitre** virtuelle uniquement).
- Basculer sur la machine **Maitre si nécessaire.**
- Vérifier le fonctionnement.
- Basculer sur la machine **esclave** qui devient active.

Sur la machine Active > Esclave :

- Installer les patchs sur la machine active (**esclave**) en se référant aux paragraphes 1.2 et 1.3.
- Verifier les log installations des patch (sous **/tmp**) sur la machine active (**esclave**). Se référer au paragraphe 1.5.
- Reboot de la machine (**esclave**).
- Dans le cas d'une machine virtuelle, contrôler que les VMWARE TOOLS sont actifs, sinon réinstaller les VMWARE TOOLS et effectuer un reboot (machine **esclave** virtuelle uniquement).
- Re-basculer sur la machine **esclave** qui devient active.
- Vérifier le fonctionnement.
- Rebasculer sur la machine Maitre.

1.4.2 CAS D'UN SYSTÈME MIVOICE 5000 SERVER REDONDÉ

Dans le cas d'un système MiVoice 5000 Server redondé, il est recommandé de commencer la mise à jour sur la machine esclave (inactive) afin de minimiser les interruptions de service.

Procédure détaillée :

- Machine active (**maitre**) vérifier état de la duplication (**cat /proc/drbd**).

Sur la machine Inactive > Esclave :

- Installer les patchs sur la machine inactive (**esclave**) en se référant aux paragraphes 1.2 et 1.3.
- Vérification : **cat /proc/drbd** (secondary/primary) sur la machine inactive (**esclave**).
- Vérifier les log installations des patch (sous **/tmp**) sur la machine inactive (**esclave**). Se référer au paragraphe 1.5.
- Reboot de la machine inactive (**esclave**).
- Dans le cas d'une machine virtuelle, contrôler que les VMWARE TOOLS sont actifs, sinon réinstaller les VMWARE TOOLS et effectuer un reboot (machine **esclave** virtuelle uniquement).
- Vérifier état de la duplication (**cat /proc/drbd**) (primary/secondary) sur la machine active (maitre).
- Basculer sur la machine **esclave** qui devient active, vérifier le fonctionnement.

Sur la machine Inactive > Maitre :

- Installer les patch sur la machine inactive (**maitre**) en se référant aux paragraphes 1.2 et 1.3.
- Vérifier les log installations des patch (sous **/tmp**) sur la machine inactive (**maitre**). Se référer au paragraphe 1.5.
- Reboot la machine inactive (**maitre**).
- Dans le cas d'une machine virtuelle, contrôler que les VMWARE TOOLS sont actifs, sinon réinstaller les VMWARE TOOLS et effectuer un reboot (machine **maitre** virtuelle uniquement).
- Re-basculer sur la machine **maitre** qui devient active.
- Vérifier le fonctionnement.

1.5 CONSULTATION DES FICHIERS DE TRACE

Deux types de fichiers trace sont générés suite à la mise à jour des patchs :

- Un fichier résumé consultable sous /root/, indiquant la date, le résultat des l'installation et de la mise à jour de DRBD dans le cas systèmes redondés.
- Un fichier complet des traces consultable sous /tmp/, Ce fichier ne doit être examiné (ou envoyé à Mitel) que lorsque le fichier résumé contient le mot « Failure ».

1.5.1 FICHIER RÉSUMÉ

Le fichier résumé, nommé **Mitel_OS.log**, est généré dans le répertoire /**root**/.

Il est complété à chaque installation pour préciser :

- La date et le résultat de l'installation des patchs ("Success"/"Failure") en précisant l'édition de ces patchs.
- Dans le cas d'un système redondé, la date et le résultat de la mise à jour de DRBD-KM ("Success"/"Failure").

Exemples de contenu de ce fichier :

Pour une mise à jour sous RedHat/CentOS par le Web sur système redondé :

2012-11-19-19:46 SecurityPatch7.x.05 Success.

2012-11-19-19:46 drbd-km-3.10.0.el6-8.4.7-1.x86_64.rpm Success.

Pour une mise à jour sous CentOS sans accès au Web sur système redondé :

2012-11-19-19:37 SecurityPatch7.x.05_Private Success.

2012-11-19-19:37 drbd-km-3.10.0.el6-8.4.7-1.x86_64.rpm Success.

1.5.2 FICHIER COMPLET

Dans tous les cas, un fichier de trace (affichage des écrans successifs) est généré sous **/tmp/ :**

Si la machine dispose d'un accès Internet (avec DNS) :

- **installClientWeb_AAAA-MM-JJ.log.**

Si la machine ne dispose pas d'accès Internet :

- **installClientPrivate_AAAA-MM-JJ.log.**

Avec AAAA-MM-JJ qui correspond à la date d'exécution de la commande – année, mois, jour).

Pour information, voici la liste des messages ajoutés dans le LOG en cas de succès ou d'échec de la mise à jour :

Succès :

- *Installation depuis internet seulement :* "General package patch download successfully completed".
- "General package patch update successfully completed".
- *Machine redondée seulement (DRBD présent) :* "drbd-km package update successfully completed".

Echec :

- Installation depuis internet seulement : "General package download failed".
- "General package update failed".
- Machine redondée seulement (DRBD présent) : "drbd-km package update failed".

Note : Les messages de succès et/ou d'échec peuvent être recherchés à partir des mots clés successfully et/ou failed.

1.6 CAS PARTICULIER DES MACHINES VIRTUELLES AVEC VMWARE TOOLS

Dans le cas d'une machine virtuelle dans laquelle les VMWARE TOOLS ont été installés, un traitement supplémentaire est exécuté lors du redémarrage (reboot) qui suit l'installation des patchs de sécurité. Les VMWARE TOOLS sont automatiquement reconfigurés pendant le reboot pour s'adapter au nouveau kernel. Cette opération peut allonger le temps de ce reboot d'une à deux minutes.

1.7 PROBLEMES DE DEMARRAGE (BOOT) SUR CERTAINES MACHINES

Sur certaines machines, par exemple les serveurs DELL R210, le nouveau « kernel » apporté par les patchs de sécurité peut échouer dans son démarrage.

Pour palier à ce problème, il faut éditer le fichier /boot/grub/menu.lst et ajouter à la fin la ligne correspondant au nouveau kernel le paramètre « reboot=pci ».

Voici un exemple ci-dessous dans le cas de Red Hat.

```
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-358.18.1.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-358.18.1.el6.x86_64 ro root=UUID=d3b6e1ca-b488-4ac8-a354-17640561c278
rd_NO_LUKS rd_NO_MD quiet LANG=fr_FR.UTF-8 SYSFONT=latarcyrheb-sun16 rhgb KEYBOARDTYPE=pc
KEYTABLE=fr-latin9 rd_NO_LVM crashkernel=auto rhgb quiet rd_NO_DM reboot=pci
        initrd /initramfs-2.6.32-358.18.1.el6.x86_64.img
```