Modèle linux_by_ssh_advanced

Contexte

Le modèle linux_by_ssh_advanced comporte 9 checks (en plus de celui du modèle linux_by_ssh), permettant ainsi de superviser sa machine linux de manière plus avancée.

La plupart des checks ajoutés ici sont destinés à vous fournir des informations approfondies souvent uniquement disponibles via des métriques, vous permettant de les utiliser comme vous le souhaitez.

Pré-requis pour certains checks

Certains checks requièrent un accès spécifique à des fichiers. Pour se faire une commande est à votre disposition. Cette commande permettra au groupe de l'utilisateur choisi pour votre supervision Shinken d'avoir un accès (en lecture seule) au fichier /var/log/btmp (pour le check Connections Failed SSH) et au fichier /etc/ssh/sshd_config (pour le check Security SSH), fichiers comportant vos logs de connexions échouées et votre configuration SSH. Sans cet accès les sondes ne fonctionneront pas et vous renverront le statut "Unknown".

Remarque

Cette commande ne peut être effectuée qu'en ayant les droits root. Donc en étant connecté au compte root ou en ayant fait la commande "su" au préalable.

Fonctionnement

La commande modifie le fichier /usr/lib/tmpfiles.d/var.conf qui est chargé de rétablir les droits au redémarrage de la machine (ce fichier n'est pas disponible sur toutes les distributions Linux, vous pourrez alors avoir une erreur, "no such file or directory", cela n'affecte en rien l'application de la commande).

Ensuite le fichier /etc/logrotate.conf sera modifié de la même façon pour qu'à la rotation des logs (tous les mois par défaut) les droits ne soient pas rétablis.

Pour finir nous changeons donc les droits des fichiers /var/log/btmp et /etc/ssh/sshd_config pour permettre au groupe utilisé pour la supervision (et donc son utilisateur) de les lire.

Exécution de la commande

Pour donner un accès en lecture seule au fichier /var/log/btmp et au fichier /etc/ssh/sshd_config au groupe **shinken**, en root depuis le serveur à superviser, exécutez :

Utilisation

```
sed -i -e "s/btmp 0600 root utmp/btmp 0640 root shinken/g" /usr/lib/tmpfiles.d/var.conf ; sed -i -e "s/create 0600 root utmp/create 0640 root shinken/g" /etc/logrotate.conf ; chmod 640 /var/log/btmp /etc/ssh/sshd_config ; chown root:shinken /var/log/btmp /etc/ssh/sshd_config
```