Modèle windows

Sommaire

Contexte

Cette page a pour but de vous décrire la mise en place du pack **linux_by_ssh**.

Elle vous accompagnera dans :

- le déploiement du pack sur votre plateforme,
- dans la configuration de vos connexions SSH,
- dans la mise à jour du package d'OpenSSH
- et dans la mise en place de pré-requis pour certains checks.

Procédure de mise en place du pack

En préambule,

1. récupérer la dernière version du pack,
2. transfèrer le pack sur votre Synchronizer et votre/vos Pollers.

En utilisant l'installeur "install.sh"

Que ce soit sur un Synchronizer où sur un Pollers :

1. Désarchiver le pack :

```
tar --no-same-owner -xf NOM_DU_PACK.tar.xz
```

2. Entrée dans le répertoire extrait de l'archive et lancer le "install.sh"

```
cd NOM_DU_PACK/
./install.sh
```

3. L'installeur dépose les éléments suivants :

    - Le fichier de configuration de la source "**shinken-additional-packs-import**" qui servira à importer la définition du pack dans le **Synchronizer**.
    - Les fichiers de définitions des éléments du pack, à importer dans le **Synchronizer**.
    - Les sondes du pack.

```
==========================================
INSTALL PACK [ shinken-linux_by_ssh ]
==========================================

    ----------------------------
    |   COLLECTOR [ shinken-additional-packs-import ]

        => ADDING Collector cfg file
              - Path : /etc/shinken/sources/shinken-additional-packs-import.cfg
        => CREATING Collector DATA space
              - Path : /etc/shinken-user/source-data/source-data-shinken-additional-packs-
import
              => ADDING Definition File [ definition_shinken-additional-packs-import.cfg ]
                     - Path : /etc/shinken-user/source-data/source-data-shinken-additional-
packs-import/definition_shinken-additional-packs-import.cfg
              - Changing owner ( to "shinken" user )
              - Setting rights

    ----------------------------
    |   MONITORING DEFINITION:

        => Installing definition files in source-data folder ( Collector => shinken-additional-
packs-import )
              - Path : /etc/shinken-user/source-data/source-data-shinken-additional-packs-
import
              - Changing owner ( to "shinken" user )
              - Setting rights

    ----------------------------
    |   PROBES:

        => Deleting previous probes
        => Installing probes
              - Path : /var/lib/shinken-user/libexec/shinken-additional-packs/shinken-
linux_by_ssh
              - Setting owner ( to "shinken" user )
              - Setting rights
```

4. Si c'est la première fois que vous utilisez le collecteur "**shinken-additional-packs-import**",

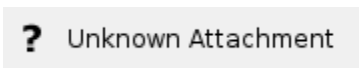
   Ajouter le nom de la nouvelle source au **Synchronizer** en modifiant le paramètre **sources** du fichier **/etc/shinken/synchronizers/synchronizer-master.cfg.**

```
define synchronizer {
    [...]
    sources                   Source 1, Source 2, Source 3, shinken-additional-packs-import
    [...]
}
```

   et en suivant, redémarrez le Synchronizer pour que le collecteur soit pris en compte :

```
service shinken-synchronizer restart
```

5. Lancer l'import du collecteur "**shinken-additional-packs-import**",



- En suivant, vous devrez peut-être accepter ou des nouveautés ou des différences qui seraient liés à ce pack (*en fonction de l'évolution du pack*).

Desinstaller le pack avec "uninstall.sh"

Entrée dans le répertoire extrait de l'archive et lancer le "uninstall.sh"

```
cd PACK__shinken__linux-by-ssh__VX.X.X-RCXXX__Linux
./uninstall.sh
```

Ce mécanisme va seulement enlever les fichiers mis en place lors de l'installation (*Fichier du collecteur d'import, définition des éléments de supervision, et les sondes proposées*), mais ne touchent pas aux éléments que vous avez absorbés dans le **Synchronizer**.

```
============================================
DELELE PACK [ shinken-linux_by_ssh ]
============================================

    ----------------------------
    |   COLLECTOR [ shinken-additional-packs-import ]

        => Deleting collector configuration file
              - Path : /etc/shinken/sources/shinken-additional-packs-import.cfg
        => Deleting collector data folder
              - Path : /etc/shinken-user/source-data/source-data-shinken-additional-packs-import

    ----------------------------
    |   MONITORING DEFINITION:

        => Deleting pack globaldata folder
              - Path : /etc/shinken/resource.d/shinken-additional-packs-import/

    ----------------------------
    |   PROBES:

        => Deleting probes
              - Path : /var/lib/shinken-user/libexec/shinken-additional-packs/shinken-linux_by_ssh
```

À noter : Vous devrez retirer manuellement les éléments importés dans le **Synchronizer** (modèles d'hôtes, checks, ...) via les actions de masses .

Manuellement

Sur le Synchronizer

Si vous avez déjà installé une version précédente de ce pack, il vous faudra supprimer les anciens dossiers dans lesquels le pack était présent (*afin d'éviter de garder d'ancien fichier en cas d'évolution de la structure du pack*).

Pour supprimer ces dossiers, utilisez la commande suivante :

```
rm /etc/shinken/sources/shinken-additional-packs-import.cfg
rm -rf /etc/shinken-user/source-data/source-data-shinken-additional-packs-import/
rm -rf /var/lib/shinken-user/libexec/shinken-linux_by_ssh
```

Ensuite, plaçons maintenant les différents éléments du pack au bon endroit :

- Les fichiers de configuration :
  - Nous vous conseillons de créer un Collecteur de type (***cfg-file-import***) qui permet d'importer des définitions d'éléments Shinken depuis les fichiers de définitions présents dans ce pack.
    - Vous trouverez la procédure de mise en place dans la page de documentation suivante (Collecteur de type (cfg-file-import) - Import depuis des fichiers au format .cfg)
    - Pour la suite des explications, nous considérerons que ce collecteur s'appele "**shinken-additional-packs-import**"
  - Une fois le collecteur mis en place, nous allons déployer le pack au bon endroit :

- En premier, le fichier de configuration :

```
cp -r ./linux_by_ssh/configuration/* /etc/shinken-user/source-data/source-data-cfg-Shinken-additionalPacks/elements/linux_by_ssh/
chown -R shinken:shinken /etc/shinken-user/source-data/source-data-cfg-Shinken-additionalPacks/packs/linux_by_ssh/
```

- Ensuite les sondes :

```
mkdir /var/lib/shinken-user/libexec/linux_by_ssh
cp -r ./linux_by_ssh/libexec/* /var/lib/shinken-user/libexec/linux_by_ssh/
```

Une fois ces commandes exécutées, vous n'avez plus qu'à importer les nouveaux éléments via le collecteur " **cfg-file-Shinken-additionalPacks** " ou celui que vous avez défini depuis votre interface de configuration.

Vous pouvez également supprimer le dossier qui a été créer suite à la décompression du pack en utilisant la commande suivante :

```
rm -rf ./linux_by_ssh
```

Attention à ne pas supprimer le tar.gz, connaître la version exacte du pack qui vous a été livré vous sera utile en cas de problème avec votre pack.

Sur les Pollers

Si vous avez déjà installé une version précédente de ce pack, il vous faudra supprimer les anciens dossiers dans lesquels le pack était présent. Pour supprimer ces dossiers, utilisez la commande suivante :

```
rm -rf /var/lib/shinken-user/libexec/linux_by_ssh
```

Ensuite, transférer sur votre machine et décompressez le fichier en utilisant commande et en remplaçant **"PACK__shinken__nom-du-pack__version__arch.tar.gz"** par le nom du pack qui vous est livré,

Pour windows :

```
tar -xvzf PACK__shinken__nom-du-pack__version__windows.tar.gz -C ./
```

Pour Linux :

```
tar -xjfv --no-same-owner PACK__shinken__nom-du-pack__version__linux.tar.xz -C ./
```

Le paramètre --no-same-owner permet de ne pas conserver les attributs d'utilisateurs/roles utilisés lors de la compression.

Puis, on place les sondes, pour que le Poller puisse les utiliser, tel que défini dans la UI de Configuration :

```
mkdir /var/lib/shinken-user/libexec/linux_by_ssh
cp -r ./linux_by_ssh/libexec/* /var/lib/shinken-user/libexec/linux_by_ssh/
```

Comment configurer la connexion SSH ?

Pour l'exécution correcte des commandes du pack linux_by_ssh, vous aurez besoin d'une connexion SSH.

Quelques informations au préalable sont nécessaires pour la bonne compréhension de cette partie.

- D'une part, du côté **de l'architecture Shinken**, l'exécution des checks (*plus exactement les sondes*) sont réalisées par les Pollers, en tant qu'utilisateur "**shinken**".

    - Donc l'utilisateur "**shinken** " devra avoir accès aux clefs SSH que vous utiliserez pour la connexion SSH sur les serveurs distants monitorés.
- D'autre part, du côté des **machines Linux supervisées**,
    - un **nom d'utilisateur**, et une **clé SSH** ou **mot de passe** sont requis.
    - Dans le modèle linux_by_ssh, des données sont prévues à cet effet.

Nous conseillons l'utilisation d'un utilisateur spécifique (*pour le service de supervision*) ainsi que l'utilisation d'une connexion via clé SSH, afin d'éviter l'utilisation du super utilisateur root qui n'est pas requis par les checks.

Côté client (machine ou serveur Linux supervisé)

Si votre utilisateur de supervision n'est pas déjà créé sur votre linux à superviser, depuis un terminal de la machine supervisée "**linux-1**" (en root), il faut créer un nouvel utilisateur local avec mot de passe.

- dans cet exemple, nous utilisons "**user-service-shinken**" mais vous pouvez créer un autre utilisateur.

```
              [root@linux-1 ~]# adduser -m -r user-service-shinken
[FACULTATIF] : [root@linux-1 ~]# passwd user-service-shinken
```

Notez que la mise en place d'un mot de passe pour cet utilisateur n'est pas obligatoire, mais il vous faudra copier la clé SSH via la **méthode manuelle** expliquée plus bas, car la commande automatique ssh-copy-id requiert un mot de passe pour l'utilisateur du système de destination.

Côté serveur Poller

Copie de la clé SSH de votre utilisateur de supervision "**user-service-shinken**" depuis le serveur Poller "**shinken-poller**" (pour cet exemple), vers le serveur supervisé "**linux-1**" (dans cet exemple, IP : 192.168.1.19)

Copie clé SSH via commande ssh-copy-id

Soit via la méthode "automatique" via la commande ssh-copy-id en se connectant au préalable via l'utilisateur **shinken** sur le ou les serveurs pollers :

```
[root@shinken-poller ~]# su - shinken
[shinken@shinken-poller ~]#  ssh-copy-id -i ~/.ssh/user-service-shinken_id_rsa.pub user-service-
shinken@linux-1
The authenticity of host '192.168.1.19 (192.168.1.19)' can't be established.
RSA key fingerprint is 00:ff:ee:dd:cc:bb:aa:d6:d3:79:1d:f6:93:47:80:27.
Are you sure you want to continue connecting (yes/no)? yes
user-service-shinken@linux-1's password: XXXXXXXXXX
Now try logging into the machine, with "ssh 'user-service-shinken@linux-1'", and check in:
  .ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

Copie clé SSH via commande ssh

Soit via une commande SSH depuis le serveur Poller, il s'agit d'ajouter la clé publique au fichier "authorized_keys" du serveur supervisé (ici vm2) :

```
cat /var/lib/shinken/.ssh/user-service-shinken_id_rsa.pub | ssh root@vm2 "cat >> /var/lib/shinken/.ssh
/authorized_keys"
```

Ici la connexion se fait via l'utilisateur root du serveur vm2 (mais vous pouvez utiliser votre propre utilisateur), le but étant de rajouter, en une commande SSH, la clé de l'utilisateur shinken du Poller **/var/lib/shinken/.ssh/user-service-shinken_id_rsa.pub** à la fin du fichier **/var/lib/shinken/.ssh/authorized_keys** du serveur supervisé.

Copie clé SSH manuellement

Soit via méthode "manuelle" via rajout de la clé dans le fichier authorized_keys

- Récupérez la clé publique de l'utilisateur qui va établir la connexion SSH, et la copier

```
[root@shinken-poller ~]# su - shinken
[-bash-4.1]$ less .ssh/id_rsa.pub

-> copiez la clé
```

- Connectez-vous sur le serveur linux supervisé avec votre utilisateur de supervision et collez cette clé dans le fichier "authorized_keys" de l'utilisateur de supervision :

```
[root@linux-1 ~]# su - user-service-shinken
[-bash-4.1]$ vi .ssh/authorized_keys

-> collez la clé
```

Test de connexion

Test de connexion au serveur "**linux-1**" en tant qu'utilisateur "**user-service-shinken**" via l'utilisateur du Poller (shinken) :

```
[root@shinken-poller ~]# su - shinken
[shinken@shinken-poller ~]# ssh user-service-shinken@linux-1 -i .ssh/user-service-shinken_id_rsa.pub
```

La connexion doit s'établir avec succès.

Côté interface de configuration

Dans chaque hôte héritant du modèle d'hôte "linux_by_ssh", "linux_by_ssh_advanced" ou "linux_by_ssh_extra",

- vous aurez 4 données concernant la connexion SSH (*SSH_KEY, SSH_KEY_PASSPHRASE, SSH_PORT, SSH_USER*)
- Ces 4 données seront par la suite utilisées par tous les checks.
  - Par défaut, ces données sont configurées pour utiliser des variables globales défini par défaut dans le fichier /etc/shinken/resource.d/ssh.cfg (*sur le* serveur central hébergeant l'Arbiter).
  - Si vous souhaitez les changer globalement,
    - vous pouvez modifier le fichier "**/etc/shinken/resource.d/ssh.cfg**",
    - ou faire vos propres modèles qui héritent des modèles d'hôtes proposés par ce pack en surchargeant ces 4 valeurs (*ainsi vous aurez vos propres valeurs par défaut*).

Donnée	Description	Valeur par défaut	Valeur par défaut à l'installation de shinken
SSH_KEY	Répertoire de la clé générée sur votre serveur hébergeant le démon Poller	SSH_KEY	~/.ssh/id_rsa
SSH_KEY_PASSPHRASE	Mot de passe utilisé pour l'authentification de l'utilisateur ou pour utiliser la clé privée ("Passphrase") si nécessaire	$SSH_KEY_PASSPHRASE$	''
SSH_PORT	Port de connexion SSH	SSH_PORT	22
SSH_USER	Utilisateur pour la connexion SSH	SSH_USER	shinken

Remarque

- Toutes les valeurs par défaut renvoient à une globale (voir la page LES VARIABLES (Remplacement dynamique de contenu - Anciennement les MACROS)) qui sont modifiables dans le fichier /etc/shinken/resource.d/ssh.cfg, attention cependant, la modification dans le fichier direct entraînera une modification sur tous les hôtes utilisant ces globales.
- La modification des valeurs par défaut présentes dans le fichier du serveur (/etc/shinken/resource.d/ssh.cfg) nécessite un redémarrage intégral du service shinken (service shinken restart).

Par exemple, voici le paramétrage d'une connexion via clé SSH par défaut :

? Unknown Attachment

? Unknown Attachment

Par exemple, voici le paramétrage d'une connexion via Utilisateur/Mot de passe :

? Unknown Attachment

Mise à jour d'OpenSSH

Ce script peut ne pas fonctionner correctement avec les versions d'OpenSSH antérieure à la 6, dû à une impossibilité de modifier les droits des fichiers et donc de faire fonctionner le script hors root lors des accès à la commande "lastb" à distance.

- Nous vous conseillons donc de mettre à jour votre version d'OpenSSH, ce qui garantira également une meilleure sécurité sur votre environnement.
- Attention, par précaution, assurez-vous d'avoir une session console au serveur sur lequel vous souhaitez réaliser la mise à jour.
    - Si vous rencontrez des soucis dans la mise à jour, avec cette console, vous aurez la possibilité d'intervenir sur le serveur.

En général

Sur la plupart des distributions encore à jour, les versions d'OpenSSH 6 ou supérieures se trouvent déjà dans les dépôts officiels, il vous suffit donc de réaliser votre commande de mise à jour, quelques exemples :

Centos 7 et Redhat

```
yum update openssh
```

AlmaLinux

XXXX

RockyLinux

XXXX

Debian et Ubuntu

```
apt-get upgrade openssh
```

ArchLinux et autres

```
pacman -Syu openssh
```

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".

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

> **Remarque**
>
> Cette série de commandes 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.

Pour donner un accès en lecture seule au fichier /var/log/btmp et au fichier /etc/ssh/sshd_config au groupe **shinken** , 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
```