Connections Failed SSH

Contexte

Les tentatives d'intrusion pour corruption ou vol de données ne doivent pas être sous estimées dans le cadre de votre supervision de vos postes et serveurs Linux.

Ce script a donc été conçu pour vous permettre de garder le maximum de vigilance sur les échecs de connexion sur votre parc.

Description

Le check "Connections Failed SSH" va vérifier vos logs dans un laps de temps donné (24h par défaut, modifiable dans les données) et vous donner le nombre total, et un tableau comportant une ligne par, trio IP-Host-Interface (dans le cas d'une connexion réseau) et couple Host-Interface (dans le cas d'une connexion locale sans adresse IP).

Vous obtiendrez alors le nombre de tentatives au cas pas cas, la date de la première et de la dernière tentative, et les informations précédemment énoncées. Le tableau est classé par le nombre total de tentative de connexion pour le trio IP-Host-Interface ou Host-Interface.

Les deux seuils configurables concernent le total des connexions échouées.

Sommaire

- Contexte
- Description
- Mise à jour d'OpenSSH
  - En général
    - Centos 7 et Redhat
    - Debian et Ubuntu
    - ArchLinux et autres
  - Sur Centos 6.6
    - Installation de quelques paquets
    - Télécharge ment
    - Extractions et copies
    - Paramétrag e Specs
    - Build du RPM et installation
- Exemple
  - Exemples de résultat
  - Cas spécifiques (Retour UNKNOWN)
- Données et métriques
  - Données
  - Métriques

Mise à jour d'OpenSSH

Sur CentOS 6.6, 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.

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 :

> **Note**
>
> Les commandes peuvent s'étendre à d'autres distributions non répertoriées

Centos 7 et Redhat

```
yum update openssh
```

Debian et Ubuntu

```
apt-get upgrade openssh
```

ArchLinux et autres

```
pacman -Syu openssh
```

Sur Centos 6.6

Voici les différentes commandes : (un exemple ici avec la version OpenSSH 7.6 Officielle, mais vous pouvez prendre la dernière version disponible sur le site officiel d'OpenSSH)

Installation de quelques paquets

```
yum install rpm-build gcc make wget openssl-devel krb5-devel pam-devel libX11-devel xmkmf libXt-devel
```

Téléchargement

```
wget https://mirrors.ircam.fr/pub/OpenBSD/OpenSSH/portable/openssh-7.6p1.tar.gz
```

Extractions et copies

```
tar xvf openssh-7.6p1.tar.gz
mkdir -p /root/rpmbuild/{SOURCES,SPECS}
cp ./openssh-7.6p1/contrib/redhat/openssh.spec /root/rpmbuild/SPECS/
cp openssh-7.6p1.tar.gz /root/rpmbuild/SOURCES/
```

Paramétrage Specs

```
cd /root/rpmbuild/SPECS/
sed -i -e "s/%define no_gnome_askpass 0/%define no_gnome_askpass 1/g" openssh.spec
sed -i -e "s/%define no_x11_askpass 0/%define no_x11_askpass 1/g" openssh.spec
sed -i -e "s/BuildPreReq/BuildRequires/g" openssh.spec
```

Build du RPM et installation

```
rpmbuild -bb openssh.spec

cd /root/rpmbuild/RPMS/x86_64/

rpm -Uvh *.rpm
```

Redémarrez votre service sshd :

```
service sshd restart
```

Vous pouvez vérifier votre version avec :

```
rpm -qa | grep openssh
```

Si vous avez quelconques problèmes vous pouvez revenir sur l'ancienne version avec :

```
yum downgrade openssh-server
```

Si vous utilisez l'utilisateur "shinken" (par défaut) avec une connexion via clé RSA, il se peut que suite à la mise à jour, vos scripts affichent un message de problème d'authentification (**[ERROR]** Connection failed 'Authentification failed'), sur le serveur sur lequel vous avez mis à jour SSH, veuillez réinitialiser l'utilisateur en lui supprimant son mot de passe (par défaut) avec la commande :

passwd -d shinken

Exemple

Exemples de résultat

[OK] There are less than 90 connections attempts failed.

Last attempt date	IP	User	Number of attempts	Interface	First attempt date
There is no connection failed !					

[CRITICAL] There are more than 80 connections attempts failed (161) in the last 2 hours.

Last attempt date	IP	User	Number of attempts	Interface	First attempt date
2017-11-02-16:01:46	[illegible]	test3	105	ssh:notty	2017-11-02-14:37:19
2017-11-02-14:36:27	[illegible]	test2	42	ssh:notty	2017-11-02-14:02:49
2017-11-02-14:24:18	[illegible]	root	6	ssh:notty	2017-11-02-14:24:02
2017-11-02-15:22:05	[illegible]	test	2	ssh:notty	2017-11-02-15:22:04
2017-11-02-14:57:11	[illegible]	public	2	ssh:notty	2017-11-02-14:57:10
2017-11-02-15:57:12	[illegible]	admin	1	ssh:notty	2017-11-02-15:57:12
2017-11-02-15:57:09	[illegible]	admin	1	ssh:notty	2017-11-02-15:57:09
2017-11-02-15:47:15	[illegible]	root	1	ssh:notty	2017-11-02-15:47:15
2017-11-02-14:57:31	[illegible]	nodeserver	1	ssh:notty	2017-11-02-14:57:31

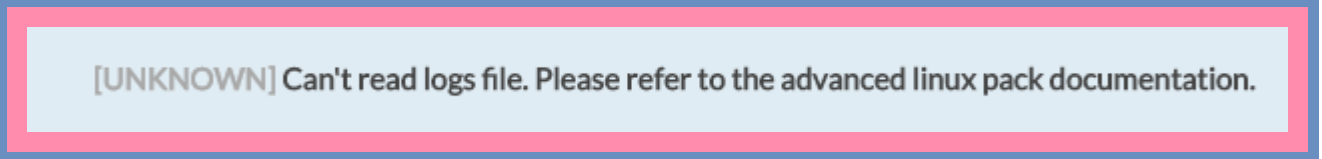
Remarque

Si vous souhaitez archiver ponctuellement les logs de tentatives de connexion, vous pouvez utiliser la commande : logrotate -f /etc /logrotate.conf

Si vous purger les logs de tentatives de connexion, vous pouvez utiliser la commande : cat /dev/null > /var/log/btmp

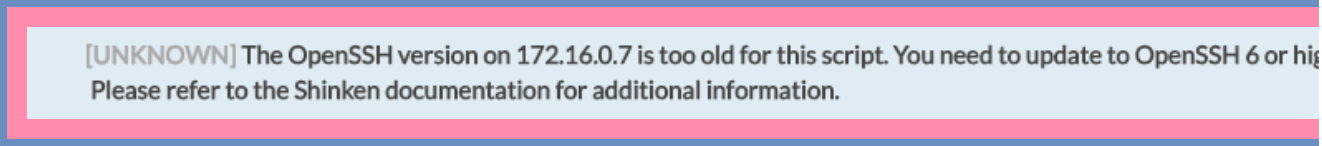
Cas spécifiques (Retour UNKNOWN)

- Si le check a le statut "Unknown" avec le message :



Appliquez la ligne de commande ou le script advanced_pack_read_rights.py disponible dans la page Modèle Linux avancé. (droits spécifiques à des fichiers)

- Si vous recevez ce message :



Référez vous à la section de Mise à jour d'OpenSSH

Remarques

Si vous avez trop de connexions échouées sur votre serveur dans le délai donné (plus de 20000), nous ne serons pas en mesure de vous donner le nombre total de connexions échouées et devrons nous arrêter à 20000 dans des soucis d'optimisation.

Pareillement un tableau de plus de 50 lignes sera tronqué à ce stade, et ce afin d'empêcher des soucis de visibilité.

Si le check n'aboutit pas, vous pouvez purger les logs de tentatives de connexion avec la commande : cat /dev/null > /var/log/btmp (si besoin, faites un backup de /var/log/btmp au préalable)

Données et métriques

Données

Donnée	Description	Valeur par défaut
CONNECTION_CRITICAL	Définit le nombre de connexions échouées à partir duquel le check passe en critical	10
CONNECTION_INTERFACE	Interface de connexion à prendre en compte dans le check, séparées par des virgules	ssh,tty
CONNECTION_TIME_LIMIT	Nombre d'heures prises en compte dans le check	24
CONNECTION_WARNING	Définit le nombre de connexions échouées à partir duquel le check passe en warning	5

Métriques

Nom de la métrique	Description

connection_failed	Nombre de connexion échouées