Connection Failed SSH

Sommaire

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

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 de tentatives de connexions échouées, et un tableau comportant une ligne par trio IP-Host-Interface (*dans le cas d'une connexion réseau*) ou couple Host-Interface (*dans le cas d'une connexion locale sans adresse IP*).

- Vous obtiendrez alors le nombre de tentatives au cas par 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 tentatives de connexion pour le trio IP-Host-Interface ou Host-Interface.
- Deux seuils configurables permettent de déterminer quand le check passe en **ATTENTION**, puis en **CRITIQUE**.

Statut	Nom de check	Résultat	Résultat Long
✓	Connection Failed SSH	OK There are 3 connections attempt failed (less than 5) in the last 24 hours.	

Last attempt date	IP	User	Number of attempts	Interface	First attempt date
20 June 2024 at 14:18:17	192.168.1.58	f.garcia	3	ssh:notty	20 June 2024 at 14:18:0

Paramétrage

Le check utilise la ligne de commande suivante :

```
$SHINKEN_LINUXBYSSH_PLUGINSDIR$/check_linux_health_by_ssh_rust --check check_connection_failed -H
"$HOSTADDRESS$" -u "$_HOSTSSH_USER$" -p "$_HOSTSSH_PORT$" -i "$_HOSTSSH_KEY$" -P "$_HOSTSSH_KEY_PASSPHRASE$"
-w "$_HOSTCONNECTION_WARNING$" -c "$_HOSTCONNECTION_CRITICAL$" -l "$_HOSTCONNECTION_INTERFACE$" -t
"$_HOSTCONNECTION_TIME_LIMIT$"
```

Données utilisées provenant du modèle

Données communes pour les checks des modèles

Authentification

Données spécifiques pour ce check

Donnée	Modifiable sur	Unité	Valeur par défaut	Description
`CONNECTION_WARNING`	l'Hôte *(Onglet Données)*	--	*5*	Définit le nombre de connexions échouées à partir duquel le check passe en **ATTENTION**.
`CONNECTION_CRITICAL`	l'Hôte *(Onglet Données)*	--	*10*	Définit le nombre de connexions échouées à partir duquel le check passe en **CRITIQUE**.

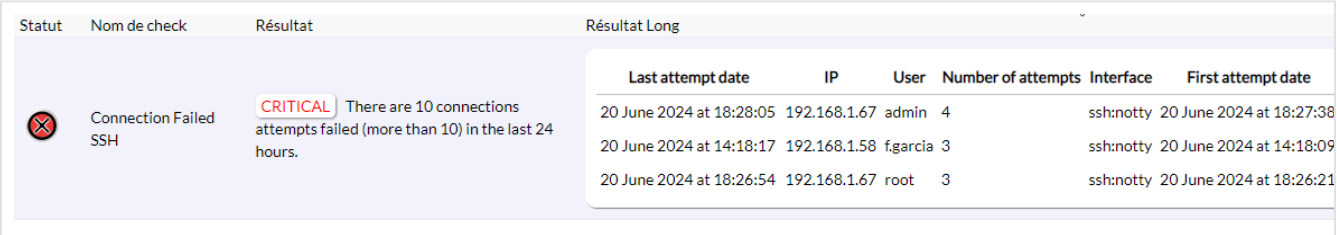
`CONNECTION_TIME_LIMIT`	l'Hôte *(Onglet Données)*	heures	*24*	Les **X dernières heures** de logs lus, pour identifier les connexions échouées.
`CONNECTION_INTERFACE`	l'Hôte *(Onglet Données)*		*ssh,tty*	Interface de connexion à prendre en compte dans le check, séparées par des virgules. Les interfaces supportées sont : **pts**,**tty**,**ssh**,**all**

Données utilisées provenant du check

Pas de données spécifiques pour ce check

Résultat

Exemple



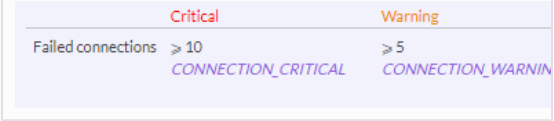
Interprétation des données

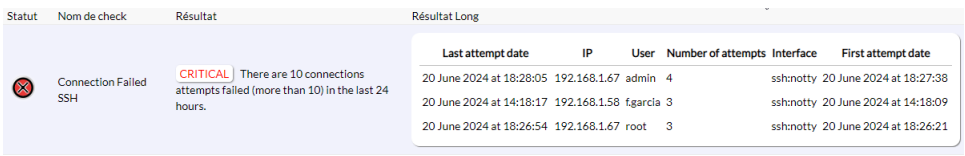
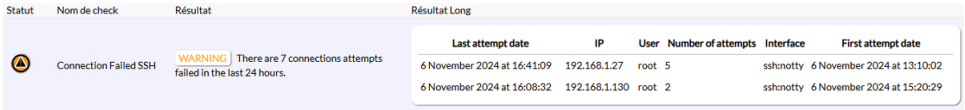
Statut

- Il peut prendre 4 valeurs ***OK*** / ***CRITIQUE*** / ***ATTENTION*** / ***INCONNU*** .
    - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
        - **CONNECTION_WARNING**
        - **CONNECTION_CRITICAL**
    - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

Affichage des Seuils

Le texte de la colonne "Affichage des seuils" montre les DONNÉES utilisées et leur valeur définie sur l'équipement supervisé.



Situation	*Statut*	*Exemple*
• Les nombre de tentatives de connections échoués est supérieur ou égal à **CONNECTION_CRITICAL**.	***CRITIQUE***	
• Les nombre de tentatives de connections échoués est supérieur ou égal à **CONNECTION_WARNING**.	***ATTENTION***	

Métriques

Nom de la métrique	Description
total	Nombre de connexions échouées

Mise en place (pré-requis pour ce check)

Certains checks requièrent un accès spécifique à des fichiers.

- Pour ce faire, nous vous mettons à disposition une série de commandes.
  - Ces commandes permettront au groupe de l'utilisateur choisi pour votre supervision Shinken d'avoir un accès (*en lecture seule*) au fichier **/var/log/btmp**, fichier comportant vos logs de connexions échouées.
- Sans cet accès, la sonde ne fonctionnera pas et vous renverra le statut **INCONNU**.

> **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.

Commandes à éxecuter :

Utilisation

```
sed -i -e "s/btmp 0600/btmp 0640/g" /usr/lib/tmpfiles.d/var.conf
chmod 640 /var/log/btmp
usermod -aG utmp user-service-shinken
```

1. La commande **sed -i -e "s/btmp 0600/btmp 0640/g" /usr/lib/tmpfiles.d/var.conf** modifie les droits par défaut du fichier **/var/log/btmp** dans le fichier de configuration des fichiers temporaires.

- Cette modification garantit que, même après un redémarrage, les permissions de **btmp** resteront correctes (lecture pour le groupe).
- **Note :** Si le fichier **/usr/lib/tmpfiles.d/var.conf** n'existe pas sur votre système, une erreur "no such file or directory" peut apparaître. Cela n'affecte en rien l'application de la commande.

2. La commande **chmod 640 /var/log/btmp** applique immédiatement les droits nécessaires sur le fichier.

- Les utilisateurs du groupe pourront lire les journaux des tentatives de connexion échouées.

3. La commande **usermod -aG utmp user-service-shinken** ajoute l'utilisateur **user-service-shinken** au groupe **utmp**, qui a la responsabilité des logs système.

- Cela permet à l'utilisateur de supervision de lire le fichier **/var/log/btmp**.