Connection Failed by 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.

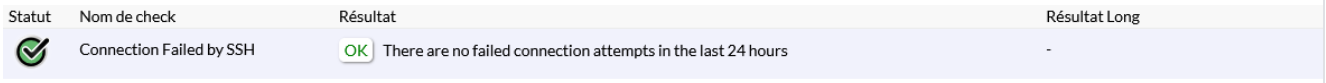
Le check **Connection Failed by SSH** va vérifier vos logs dans un laps de temps donné (*24h par défaut, modifiable dans les données*) et vous donner le nombre total de tentatives de connexions échouées, et un tableau comportant une ligne par trio IP-Host-Interface (*dans le cas d'une connexion réseau*)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

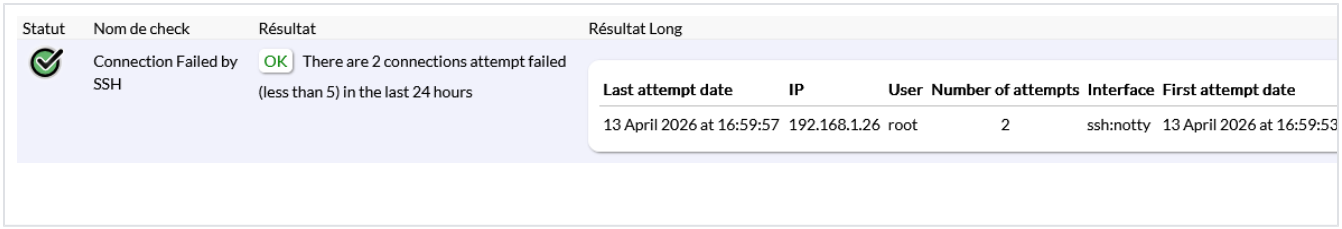
- Vous obtiendrez alors le nombre de tentatives au cas par cas, la date de la première et de la dernière tentative, et les informations précédemment énoncées.
  - Le tableau est classé par le nombre total de tentatives de connexion pour le trio IP-Host-Interface ou Host-Interface.
- Deux seuils configurables permettent de déterminer quand le check passe en **ATTENTION**, puis en **CRITIQUE**.

Le check ne supporte pas certaines distributions, où la commande 'lastb' n'est plus disponible :

- >= Debian 12
- >= Ubuntu 22
- >= FreeBSD 13
- >= OpenSuse 13

Un status **INCONNU** sera renvoyé si le check ne peut pas s'exécuter.





Paramétrage

Le check utilise la ligne de commande suivante :

```
$LINUXBYSSH_SHINKEN_PLUGINSDIR$/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

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
SSH_KEY	l'Hôte *(Onglet Données)*	--	SSH_KEY_KEY	**~/.ssh/id_rsa**	Chemin vers la clé SSH privé de l'**utilisateur shinken**, sur le serveur hébergeant le Poller qui exécutera le check. • Cette clé doit être présente dans les clefs autorisées du **compte utilisateur utilisé pour se connecter** sur le serveur linux supervisé (*voir la donnée SSH_USER si dessous*).
SSH_KEY_PASSPHRASE	l'Hôte *(Onglet Données)*	--	$SSH_KEY_PASSPHRASE$	**''**	Phrase secrète utilisée pour déchiffrer la clé privée de l'utilisateur (*si celle-ci est protégée par une passphrase*). La clé privée déchiffré est ensuite utilisée pour authentifier l'utilisateur.
SSH_PORT	l'Hôte *(Onglet Données)*	--	SSH_PORT	**22**	Port de connexion SSH.
SSH_USER	l'Hôte *(Onglet Données)*	--	SSH_USER	**shinken**	Nom de l'utilisateur pour se connecter sur le serveur supervisé.

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*	Filtres des interfaces de connexion à prendre en compte dans le check, séparées par des virgules. Les interfaces prises en compte doivent commencer par au moins un des filtres de cette liste. Exemples : • 'ssh' prendra en compte 'ssh:notty' • 'tty' ne prendra pas en compte 'ssh:notty' • 'tty' prendra en compte 'tty/0' La valeur **ALL** peut être utilisé afin de prendre en compte toutes les interfaces.

Données utilisées provenant du check

Pas de données spécifiques pour ce check

Résultat

Exemple

Statut	Nom de check	Résultat	Résultat Long
✓	Connection Failed SSH	OK There are no failed connection attempts in the last 24 hours	-

Statut	Nom de check	Résultat	Résultat Long
✓	Connection Failed by SSH	OK There are 2 connections attempt failed (less than 5) in the last 24 hours	

Last attempt date	IP	User	Number of attempts	Interface	First attempt date
13 April 2026 at 16:59:57	192.168.1.26	root	2	ssh:notty	13 April 2026 at 16:59:53

Interprétation des données

Statut

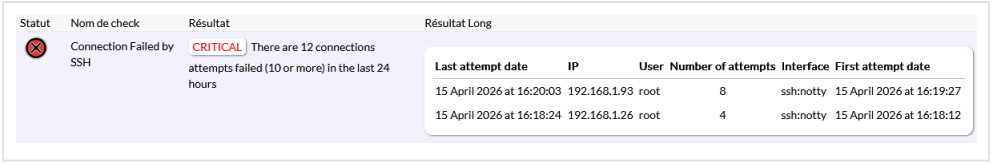
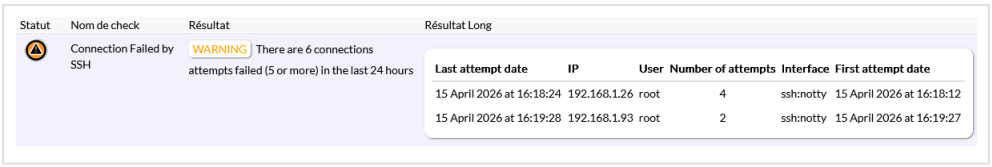
- Il peut prendre 4 valeurs ***OK*** / ***CRITIQUE*** / ***ATTENTION*** / ***INCONNU*** .
  - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
    - **CONNECTION_WARNING**
    - **CONNECTION_CRITICAL**
  - Voici un tableau récapitulatif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

	Critical	Warning
Failed connections	> 10 *CONNECTION_CRITICAL*	> 5 *CONNECTION_WARNING*

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

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
total	--	Nombre de connexions échouées	**CONNECTION_WARNING**	**CONNECTION_CRITICAL**

Exemple

Métriques :

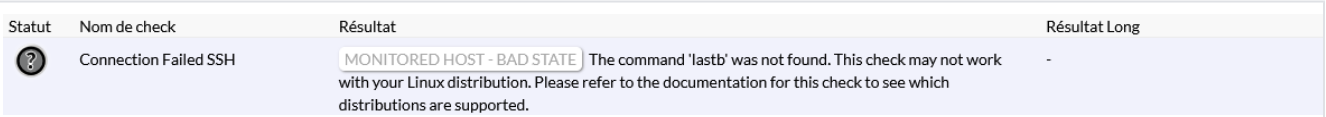
Métrique	Valeur	Seuil d'avertissement	Seuil critique
total	12.00	5.00	10.00

Les Erreurs

Erreurs spécifiques à ce check

MONITORED HOST - BAD STATE – The command 'lastb' was not found.

Le check va exécuter à distance la commande '*lastb*' mais qui n'est pas disponible sur votre machine.

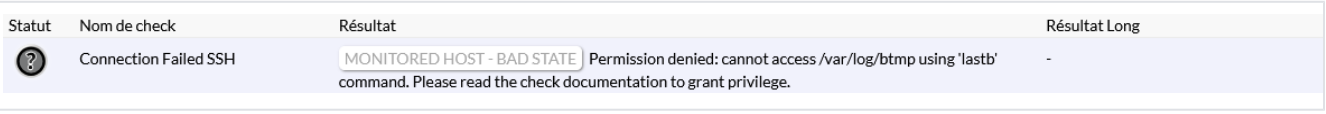


Les commandes 'lastb' et 'last' permettent de récupérer les dernières connexions réussies et échouées à une machine.
Ces commandes sont fournies par le paquet 'util-linux', installé par défaut sur la plupart des distributions Linux.
Cependant, sur certaines distributions récentes, 'lastb' n'est plus distribué et 'last' a été remplacé par une implémentation d'un nouveau paquet : 'wtmpdb'.
Alors le check ne supporte pas la supervision des hôtes aillants les distributions suivantes :

- >= Debian 12
- >= Ubuntu 22
- >= FreeBSD 13
- >= OpenSuse 13

MONITORED HOST - BAD STATE – Permission denied

L'utilisateur de supervision n'a pas accès aux fichiers de logs btmp (*/var/log/btmp*)



Les commandes suivantes 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 exécuter :

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.

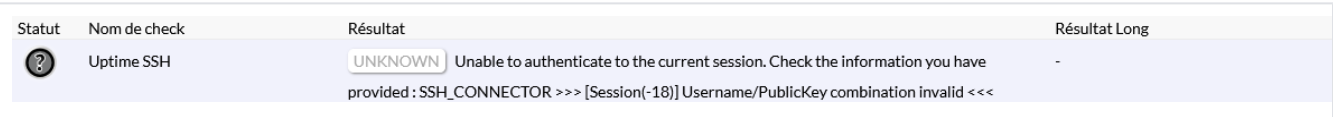
3. La commande **usermod -aG utmp user-service-shinken** ajoute l'utilisateur **user-service-shinken** au groupe **utmp**, qui a la responsabilité des logs système.

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

Erreurs de connexion (communes à tous les checks)

UNKNOWN – Username/PublicKey combination invalid

La connexion a échoué, car la paire utilisateur / clef public n'est pas reconnu par l'hôte supervisée.



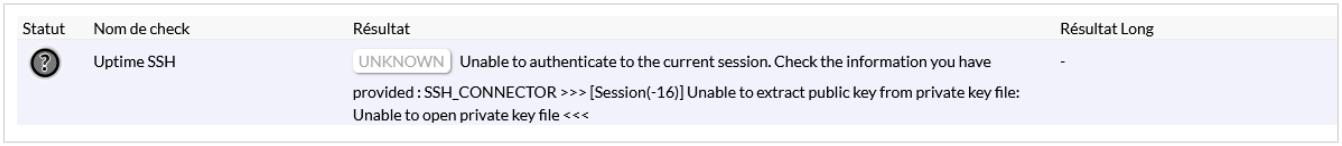
Résolution :

Possibles raisons :

- L'utilisateur utilisé n'existe pas
- La paire utilisateur / clef public n'est pas autorisé pour se connecter sur la machine supervisée.

UNKNOWN – Unable to extract public key from private key file : Unable to open private key file

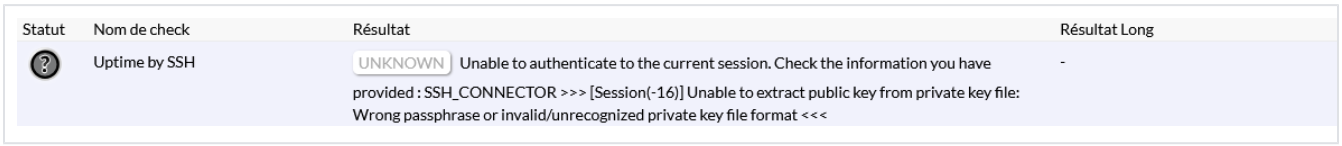
La clef privée configurée par la donnée SSH_KEY n'existe pas.



Statut	Nom de check	Résultat	Résultat Long
	Uptime SSH	UNKNOWN Unable to authenticate to the current session. Check the information you have provided : SSH_CONNECTOR >>> [Session(-16)] Unable to extract public key from private key file: Unable to open private key file <<<	-

UNKNOWN – Unable to extract public key from private key file : Wrong passphrase or invalid/unrecognized private key file format

Le mot de passe pour déchiffrer la clef privé n'est pas correct.



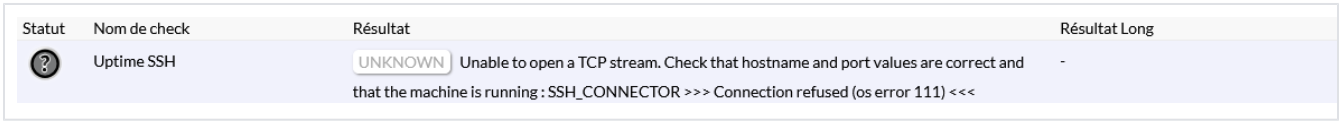
Statut	Nom de check	Résultat	Résultat Long
	Uptime by SSH	UNKNOWN Unable to authenticate to the current session. Check the information you have provided : SSH_CONNECTOR >>> [Session(-16)] Unable to extract public key from private key file: Wrong passphrase or invalid/unrecognized private key file format <<<	-

Résolution :

Vérifier la donnée SSH_KEY_PASSPHRASE.

UNKNOWN – Connection refused (os error 111)

La résolution DNS a échoué.



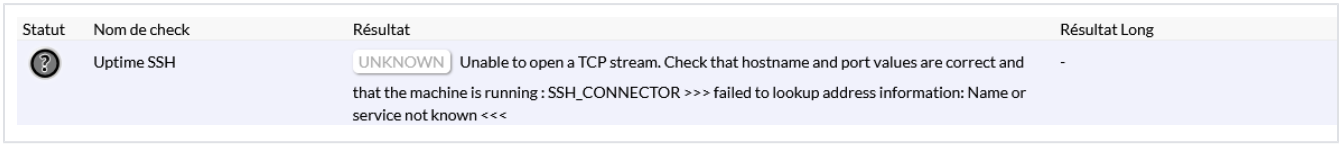
Statut	Nom de check	Résultat	Résultat Long
	Uptime SSH	UNKNOWN Unable to open a TCP stream. Check that hostname and port values are correct and that the machine is running : SSH_CONNECTOR >>> Connection refused (os error 111) <<<	-

Résolution :

Vérifier l'adresse ou le nom utilisé pour se connecter à l'hôte

UNKNOWN – Name or service not known

La résolution DNS a échoué.



Statut	Nom de check	Résultat	Résultat Long
	Uptime SSH	UNKNOWN Unable to open a TCP stream. Check that hostname and port values are correct and that the machine is running : SSH_CONNECTOR >>> failed to lookup address information: Name or service not known <<<	-

Résolution :

Vérifier l'adresse ou le nom utilisé pour se connecter à l'hôte