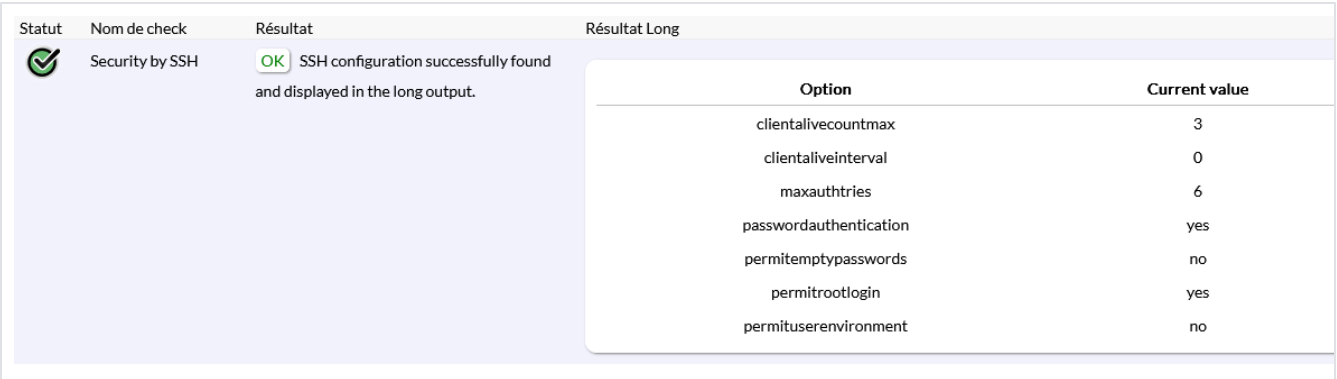
Security by SSH

Sommaire

Contexte

Le check **Security by SSH** lit les fichiers de configuration de votre serveur SSH les affiche sous forme de tableau.

- Ce qui vous permet de consulter accès simplement la configuration de votre serveur SSH, sans devoir vous connecter dessus (*dans ce cas le check sera toujours en* ***OK***).
- En plus, si vous le souhaitez, vous pouvez détecter si la configuration correspond à vos standards de sécurité en fournissant les valeurs des paramètres comme référence.
  - Par exemple, le standard sur le nombre maximum de clients connectés simultanément au serveur pourra être de 2, et le check sera en ***CRITIQUE***, si un de vos serveurs est paramétré à 4.



Paramétrage

Le check utilise la ligne de commande suivante :

```
$LINUXBYSSH_SHINKEN_PLUGINSDIR$/check_linux_health_by_ssh_rust --check check_ssh_security
    -H "$HOSTADDRESS$"
    -u "$_HOSTSSH_USER$"
    -p "$_HOSTSSH_PORT$"
    -i "$_HOSTSSH_KEY$"
    -P "$_HOSTSSH_KEY_PASSPHRASE$"
    -w "$_HOSTSSH_SECURITY_WARN$"
    -v
"$_HOSTSSH_PROTOCOL$","$_HOSTSSH_ROOT_LOGIN$","$_HOSTSSH_EMPTY_PASS$","$_HOSTSSH_PASS_AUTH$","$_HOSTSSH_USER_
ENV$","$_HOSTSSH_MAX_AUTH$","$_HOSTSSH_ALIVE_INTERVAL$","$_HOSTSSH_ALIVE_MAX$"
    -T "$_HOSTSHINKEN_TMP_DIRNAME$"
```

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.

Fichiers temporaires

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
SHINKEN_TMP_DIRNAME	l'Hôte *(Onglet Données)*	--	shinken	**shinken**	Nom de dossier temporaire où seront stockés les fichiers temporaires générés par les sondes. Ne peut contenir uniquement des caractères alphanumériques. Le dossier est généré dans **/tmp**.

Données spécifiques pour ce check

Donnée	Modifiable sur	Valeur par défaut	Description	Nom dans la configuration sshd
SSH_ALIVE_MAX	l'Hôte *(Onglet Données)*	2	Nombre maximum de clients connectés simultanément au serveur	clientalivecountmax

SSH_ALIVE_INTERVAL	l'Hôte *(Onglet Données)*	60	Secondes avant que le client soit déconnecté pour inactivité	clientaliveinterval
SSH_MAX_AUTH	l'Hôte *(Onglet Données)*	2	Maximum de tentatives de connexion autorisées	maxauthtries
SSH_PASS_AUTH	l'Hôte *(Onglet Données)*	no	Autorisation ou non d'accès au serveur par mot de passe	passwordauthentication
SSH_EMPTY_PASS	l'Hôte *(Onglet Données)*	no	Autorisation ou non d'accéder au serveur par des comptes sans mot de passe	permitemptypasswords
SSH_ROOT_LOGIN	l'Hôte *(Onglet Données)*	no	Autorisation ou non d'accéder au serveur par le compte root	permitrootlogin
SSH_USER_ENV	l'Hôte *(Onglet Données)*	no	Autorisation ou non au client connecté de modifier l'environnement	permituserenvironment
SSH_PROTOCOL	l'Hôte *(Onglet Données)*	2	Version du protocole SSH utilisée	protocol
SSH_SECURITY_WARN	l'Hôte *(Onglet Données)*	False	Active/désactive les alertes dues au check	

Remarque

Dans l'optique de proposer une sécurité stricte, nos valeurs par défaut ont été choisies pour une installation basique d'un serveur linux, nous vous conseillons fortement de les modifier pour les adapter à la sécurité que vous souhaitez fixer sur votre/vos serveur(s).

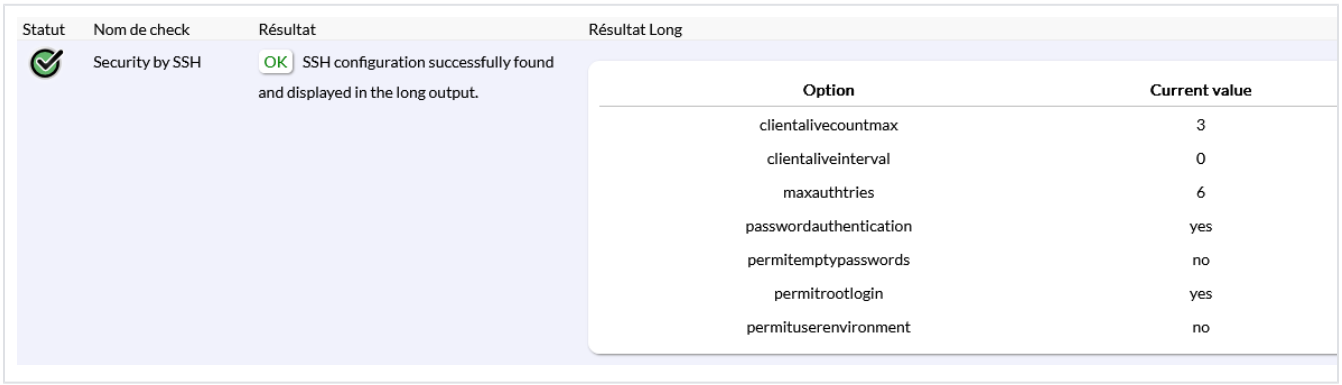
Comme expliqué précédemment, ces données sont utilisées uniquement si la donnée **SSH_SECURITY_WARN** est à **True**.

Données utilisées provenant du check

Pas de données spécifiques pour ce check

Résultat

Dans ce premier résultat le paramètre **SSH_SECURITY_WARN** est défini à False, le check passe donc en OK, car il a réussi à trouver le fichier de configuration :

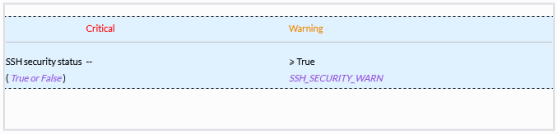


Interprétation des données

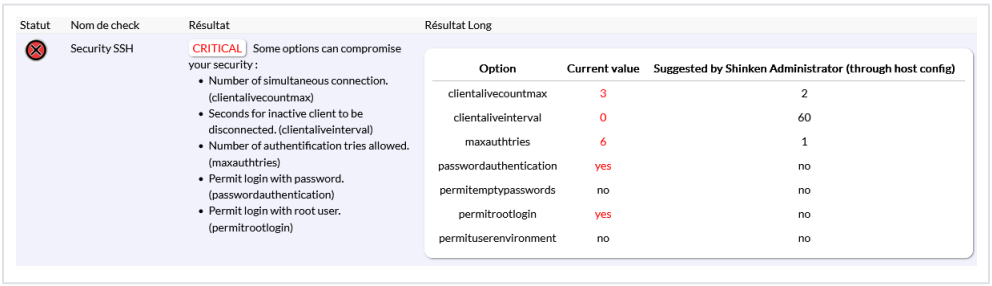
Statut

- Il peut prendre quatre valeurs ***OK*** / ***CRITIQUE*** / ***INCONNU*** .
  - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour la donnée suivante :
    - **SSH_SECURITY_WARN**
  - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

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



Critical	Warning
SSH security status -- (*True or False*)	= True *SSH_SECURITY_WARN*

Situation	*Statut*	*Exemple*
• **SSH_SECURITY_WARN** est définit à "True".	***CRITIQUE***	

Statut	Nom de check	Résultat	Résultat Long
	Security SSH	CRITICAL Some options can compromise your security : • Number of simultaneous connection. (clientalivecountmax) • Seconds for inactive client to be disconnected. (clientaliveinterval) • Number of authentification tries allowed. (maxauthtries) • Permit login with password. (passwordauthentication) • Permit login with root user. (permitrootlogin)	

Option	Current value	Suggested by Shinken Administrator (through host config)
clientalivecountmax	3	2
clientaliveinterval	0	60
maxauthtries	6	1
passwordauthentication	yes	no
permitemptypasswords	no	no
permitrootlogin	yes	no
permituserenvironment	no	no

Métriques

Aucune métrique n'est renvoyée pour ce check

Les Erreurs

Erreurs spécifiques à ce check

MONITORED HOST - BAD STATE – Can't read sshd configuration: Permission denied.

L'utilisateur de supervision n'a pas accès aux fichiers de configuration sshd.

Statut	Nom de check	Résultat	Résultat Long
	Security SSH	MONITORED HOST - BAD STATE Can't read sshd configuration: Permission denied. Read the doc for more informations.	-

Résolution

Les commandes suivantes permettront au groupe de l'utilisateur choisi pour votre supervision Shinken d'avoir un accès (*en lecture seule*) aux fichiers de configuration sshd.

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.

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 **/etc/ssh/sshd_config**, fichier comportant votre configuration SSH ainsi qu'au dossier **/tmp** (*en lecture, écriture et execution*).
- Sans cet accès, la sonde ne fonctionnera pas et vous renverra le statut **INCONNU**.

Commandes à exécuter :

Utilisation

```
sed -i -e "s/create 0600/create 0640/g" /etc/logrotate.conf
chmod 640 /etc/ssh/sshd_config
chown root:user-service-shinken /etc/ssh/sshd_config
```

1. La commande **sed -i -e "s/create 0600/create 0640/g" /etc/logrotate.conf** modifie les droits par défaut dans le fichier de configuration de **logrotate.**

    - Cela garantit que, lors de la rotation des fichiers logs (*par défaut, chaque mois*), les permissions de lecture sur **/etc/ssh/sshd_config** pour le groupe ne seront pas rétablies à des niveaux plus restrictifs.

2. La commande **chmod 640 /etc/ssh/sshd_config** applique immédiatement les droits nécessaires.

    - Le fichier de configuration SSH devient lisible par le groupe.

3. La commande **chown root:user-service-shinken /etc/ssh/sshd_config** modifie le groupe du fichier.

    - Le propriétaire reste **root**, mais le groupe est désormais **user-service-shinken**. Cela permet à l'utilisateur de supervision d'accéder au fichier en lecture seule.

MONITORED HOST - BAD STATE – Failed to load temporary ssh key.
MONITORED HOST - BAD STATE – Permission denied when creation [...]

Le check n'a pas la permission d'écrire dans le dossier temporaire.

Statut	Nom de check	Résultat	Résultat Long
?	Security SSH	MONITORED HOST - BAD STATE Failed to load temporary ssh key. Ensure user shinken has read write permissions on file : /tmp/shinken/linux_by_ssh-shinken/tmp_key_rsa	-

Statut	Nom de check	Résultat	Résultat Long
?	Security SSH	MONITORED HOST - BAD STATE Permission denied when creating /tmp/shinken/linux_by_ssh-shinken. Please grant privilege or read the check documentation	-

Resolution

> **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.

Utilisation

```
shinken_tmp_dirname="shinken"
mkdir --parents /tmp/$shinken_tmp_dirname
chown root:user-service-shinken /tmp/$shinken_tmp_dirname
chmod g+rwx /tmp/$shinken_tmp_dirname
```

1. La commande **mkdir --parents /tmp/$shinken_tmp_dirname** crée un récursivement un répertoire.

   - Le répertoire créé est **/tmp/shinken**.
   - Si un autre dossier de stockage des fichiers temporaire doit être utilisé, modifiez la première ligne : **shinken_tmp_dirname=" NouveauDossier"** ainsi que la variable **SHINKEN_TMP_DIRNAME** attaché au modèle d'hôte.

2. La commande **chown root:user-service-shinken /tmp/shinken** modifie le groupe du dossier **/tmp/shinken**.

   - Cela garantit que des droits peuvent être appliqués au groupe shinken sur ce dossier.

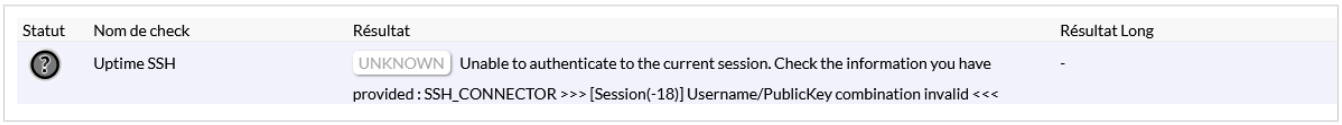
3. La commande **chmod g+rwx /tmp/shinken** applique immédiatement les droits nécessaires au dossier **/tmp/shinken** pour le groupe **user-service-shinken**.

   - Les droits de lecture, d'écriture et d'exécution sont ajoutés au dossier. Cela permet aux sondes de créer et lire des fichiers dans le dossier **/tmp/shinken**.

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.



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(-18)] Username/PublicKey combination invalid <<<	-

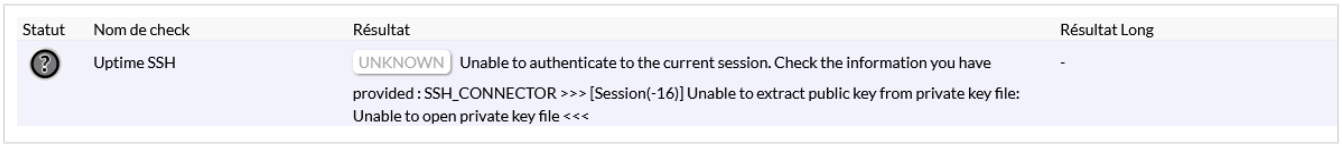
Résolution :

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

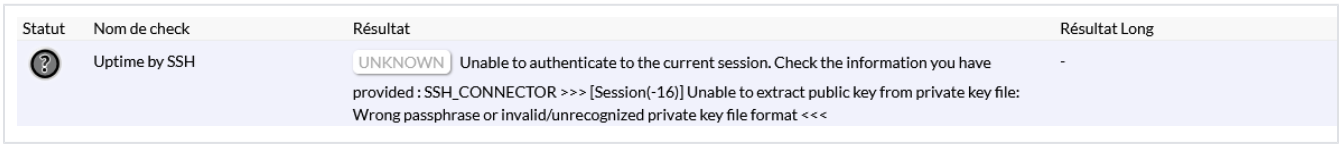
La clef privée configurée par la donnée SSH_KEY n'existe pas.



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.



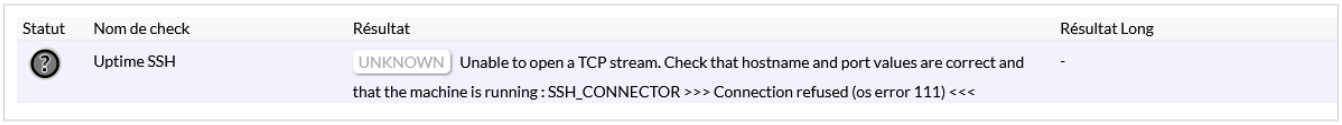
Statut	Nom de check	Résultat	Résultat Long
?	Uptime by SSH	UNKNOWN Unable to authenticate to the current session. Check the information you have provided : SSH_CONNECTOR >>> [Session(-16)] Unable to extract public key from private key file: Wrong passphrase or invalid/unrecognized private key file format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

Résolution :

Vérifier la donnée SSH_KEY_PASSPHRASE.

UNKNOWN – Connection refused (os error 111)

La résolution DNS a échoué.



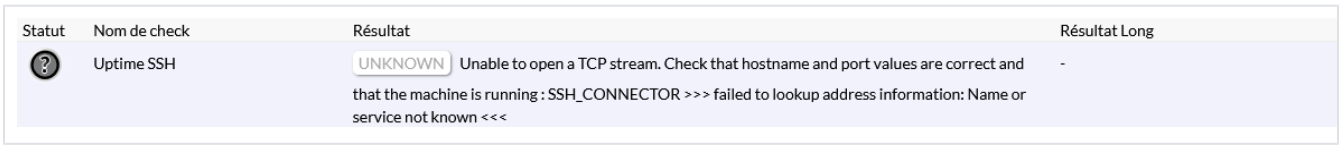
Statut	Nom de check	Résultat	Résultat Long
	Uptime SSH	UNKNOWN Unable to open a TCP stream. Check that hostname and port values are correct and that the machine is running : SSH_CONNECTOR >>> Connection refused (os error 111) <<<	-

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