Voir la configuration du module (discovery-import)

Sommaire

Contexte

Le check Security SSH lire les fichiers de configuration de votre serveur SSH et vous les afficher dans un 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.

? Unknown Attachment

Paramétrage

Le check utilise la ligne de commande suivante :

```
$SHINKEN_LINUXBYSSH_PLUGINSDIR$/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
"$_HOSTSSH_PROTOCOL$","$_HOSTSSH_ROOT_LOGIN$","$_HOSTSSH_EMPTY_PASS$","$_HOSTSSH_PASS_AUTH$","$_HOSTSSH_USER_
ENV$","$_HOSTSSH_MAX_AUTH$","$_HOSTSSH_ALIVE_INTERVAL$","$_HOSTSSH_ALIVE_MAX$"
```

Données utilisées provenant du modèle

Données communes pour les checks des modèles

Authentification

Error rendering macro 'excerpt-include'

No link could be created for 'Modèle linux_by_ssh'.

Données spécifiques pour ce check

Donnée	Nom dans la configuration sshd	Description	Valeur par défaut
SSH_ALIVE_MAX	clientalivecountmax	Nombre maximum de clients connectés simultanément au serveur	2
SSH_ALIVE_INTERVAL	clientaliveinterval	Secondes avant que le client soit déconnecté pour inactivité	60
SSH_MAX_AUTH	maxauthtries	Maximum de tentatives de connexion autorisées	2

SSH_PASS_AUTH	passwordauthentication	Autorisation ou non d'accès au serveur par mot de passe	no
SSH_EMPTY_PASS	permitemptypasswords	Autorisation ou non d'accéder au serveur par des comptes sans mot de passe	no
SSH_ROOT_LOGIN	permitrootlogin	Autorisation ou non d'accéder au serveur par le compte root	no
SSH_USER_ENV	permituserenvironment	Autorisation ou non au client connecté de modifier l'environnement	no
SSH_PROTOCOL	protocol	Version du protocole SSH utilisée	2
SSH_SECURITY_WARN		Active/désactive les alertes dues au check	False

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 :

? Unknown Attachment

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.

? Unknown Attachment

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

Métriques

Aucune métrique n'est renvoyée pour ce check

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 **/etc/ssh/sshd_config**, fichier comportant votre configuration SSH.
- 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/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.