Security SSH

Contexte

Le check Security SSH va vérifier les fichiers de configuration de votre serveur SSH et vous les afficher dans un tableau. Si vous le souhaitez vous pouvez, en modifiant une donnée, comparer la configuration précédemment récupérée à la configuration suggérée dans les données de l'hôte.

Les données du check sont modulables et vous pouvez aussi choisir d'activer ou non l'alerte en changeant les données dans la configuration de votre hôte, la donnée pour activer ou non le "warning" est SSH_WARN, les autres sont énumérées dans le tableau ci-dessous.

- Le check renverra OK si vous avez désactivé le warning ou que tous les paramètres de votre serveur sont conformes à ceux choisis dans la configuration. [PAR DEFAUT]
- Le check renverra WARNING si vous avez activé le warning et que un ou plusieurs paramètre(s) ne sont pas en accord avec ceux choisis dans la configuration.

Sommaire

- Contexte
- Exemple
  - Exemples de résultat
  - Cas spécifique
- Données et métriques
  - Données
  - Métriques

Exemple

Exemples de résultat

Statut OK si la donnée SSH_WARN a pour valeur False :

[OK] SSH configuration successfully found and displayed in the table below.

Option	Current value
clientalivecountmax	3
clientaliveinterval	0
maxauthtries	6
passwordauthentication	yes
permitemptypasswords	no
permitrootlogin	yes
permituserenvironment	no

Notes:
The current values can be changed in "/etc/ssh/sshd_config" on the host localhost.

To compare those current values with recommended values, please set SSH_WARN True in localhost configuration UI.
Please refer to the Shinken documentation for additionnal information.

La capture d'écran ci-dessous résume toutes les possibilités du check.

Dans la partie gauche nous avons les options qui ne sont pas en accord avec la configuration, cette partie n'apparaîtra que si vous choisissez d'activer le warning du check.

Ensuite la partie droite elle représente un tableau de toutes les options avec une mise en évidence de ceux dont les valeurs ne correspondent pas avec l'attente de la configuration de l'hôte.

[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

Notes:
The current values can be changed in "/etc/ssh/sshd_config" on the host localhost.

Please refer to the Shinken documentation for additional information.

Cas spécifique

Si le check a le statut "Unknown" :

Appliquez le script advanced_pack_read_rights.py disponible dans la page Modèle Linux avancé.

Données et métriques

Données

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_WARN		**Active/désactive les alertes dûes 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_WARN est à **True**.

Métriques

Remarque

Aucune métrique n'est renvoyée par ce check.