

Protection des données sensibles de l'UI de Configuration

Fonctionnement

Les données affichées sur l'interface de configuration peuvent être partagées et visibles par plusieurs utilisateurs. De ce fait, il est possible de protéger certaines données grâce au mécanisme de protection des données sensibles.

Cette fonctionnalité est divisée en deux parties : la protection et le chiffrement. Ces deux parties sont dissociées et ont des objectifs différents.

Protection

Cette partie permet à l'administrateur Shinken de protéger des données sensibles en les définissant une liste avec les mots-clés de celles-ci.

Si l'un des mots-clés se trouve dans le nom d'une donnée, celle-ci sera protégée pour les administrateurs de SI :

- Les données globales d'un service ou de l'argument d'une commande seront masquées
- Les données venant d'un modèle d'hôte et ayant un mot-clé dans le nom de la donnée seront masqués.
- Les données ci-dessus ne transiteront pas entre le serveur ayant le démon Synchronizer et le navigateur web (pour éviter toute interception).
- Les données de l'hôte seront visibles, donc accessibles pour les Administrateurs de SI.



Les administrateurs Shinken ont accès à toutes les données dans l'Interface de Configuration. Pour configurer ce mécanisme : [Configuration de la protection des données sensibles](#)

Chiffrement

Une seconde protection vient compléter ce mécanisme en ajoutant un chiffrement de toutes les données identifiées comme sensibles en base.

Le comportement est le même pour tous les utilisateurs :

- De chiffrer en base toutes les données contenant les mots-clés.
- De masquer sur l'interface de configuration toutes ces données, même celles définies sur les hôtes, quel que soit les utilisateurs.
- De ne faire transiter aucune donnée protégée entre le serveur ayant le démon Synchronizer (portant l'Interface de Configuration) et les navigateurs web.



Pour mettre en place ce mécanisme : [Chiffrement des données sensibles](#)

Mise en œuvre

L'utilisation de ces fonctionnalités ne change en rien la manière d'utiliser Shinken mais les données sensibles sont protégées :

- Dans les pages d'édition, leur valeur est cachée par des étoiles.
- Dans les autres pages, un texte "Ce champ est protégé" est affiché à la place de la valeur originale.

Kernel Stats	Note
Load Average	0.000000 0.000000 0.000000
Ligne de commande:	
\$PLUGINS/SSH/ssh, load_average, ssh_key="B4C57ACD08158" "c"8,HOSTSSH_USER" "8,HOSTSSH_KEY"	
Evaluation:	
Paramètres:	
Item	Valeur trouvée
PLUGINS	ssh-key, ssh-key, ssh-key
HOSTSSH_KEY_PASSPHRASE	Ce champ est protégé
HOSTLOAD_CRIT	0.5
HOSTADDRESS	192.168.1.70
HOSTSSH_KEY	ssh-key
HOSTLOAD_WARN	0.5, 0.5, 0.5
HOSTSSH_USER	Ce champ est protégé
Ligne de commande avec les données interpolées:	
\$ssh-key, ssh-key, ssh-key "B4C57ACD08158" "c"8,HOSTSSH_USER" "8,HOSTSSH_KEY"	
Exécution sur la plateforme de configuration (test) [synchroniser master]:	
Statut	Résultat
OK	OK: load_average 0.000000 0.000000 0.000000 host=192.168.1.70 user=ssh-key

SSH_KEY	SSH_KEY [Dans le module ssh]	SSH_KEY	SSH_KEY [Dans le module ssh]
SSH_KEY_PASSPHRASE	*****	SSH_KEY_PASSPHRASE	Ce champ est protégé
SSH_PORT	SSH_PORT [Dans le module ssh]	SSH_PORT	Ce champ est protégé
SSH_USER	SSH_USER [Dans le module ssh]	SSH_USER	Ce champ est protégé

Tous	Tous	Aucun filtre	Aucun filtre
Différence	Active	admin	
Clé d'import	Propriété	Valeur validée	Valeur
password	Mot de passe	Ce champ est protégé	