Permettre aux administrateurs de SI de pouvoir visualiser les données sensibles sur les hôtes (uniquement, mais pas celles héritées)

Afin de permettre aux administrateur de SI de pouvoir voir les données sensibles sur les hôtes, il faut activer la propriété suivante dans le fichier :

/etc/shinken-user/configuration/daemons/synchronizers/synchronizer_cfg_overload.cfg

```
protect_fields__are_viewable_by_admin_si=1
```

Protection

Si l'un des mots-clés servant à protéger les données 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 masquées.
    - 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, quels que soient 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