Configuration d'un analyseur

Accès à la configuration

La configuration d'un analyseur ne peut se finaliser qu'après avoir ajouté la source dans le synchronizer et redémarré celui-ci (procédure décrite dans la page de configuration des sources).

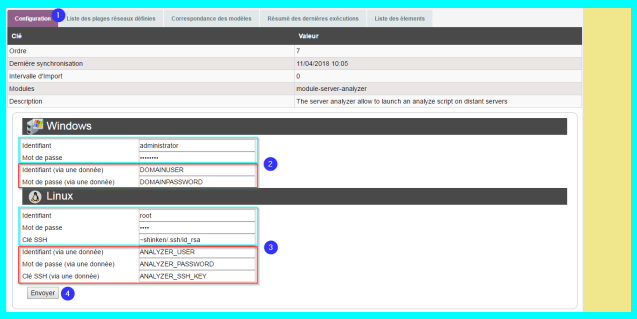
Pour accéder à la configuration de la source, sur la page principale, cliquez sur le nom de la source. La configuration d'un Analyseur est composée de différentes parties :

- Les identifiants génériques
- La liste des plages réseaux
- La correspondance des modèles
- Le résumé des dernières exécutions
- La liste des éléments

Cette page va vous présenter les différentes configurations.

Identifiants génériques

Cette partie est accessible depuis l'onglet **configuration (1)**.



Ces identifiants seront utilisés par défaut pour chaque analyse lancée, mais il sera possible de lancer une analyse avec des identifiants différents (voir la partie du lancement de l'analyse).

Pour chacun des différents systèmes d'exploitation supportés **(2)** et **(3)**, il est possible

- d'utiliser des identifiants prédéfinis (entouré en bleu sur l'image). Exemple : root/root
- d'utiliser une donnée attachée à un hôte, modèle d'hôte, ... afin que chaque hôte ou ensemble d'hôtes puissent avoir son identifiant (entouré en rouge sur l'image)

Dans tous les cas, les identifiants utilisés ont besoin des droits d'accès d'administrateur pour que l'analyse se déroule correctement.

Une fois vos identifiants paramétrés, soumettez le formulaire pour enregistrer ces données **(4)**.

Définir une nouvelle plage réseau

Cette partie est accessible depuis l'onglet **Liste des plages réseaux définies (1)**.

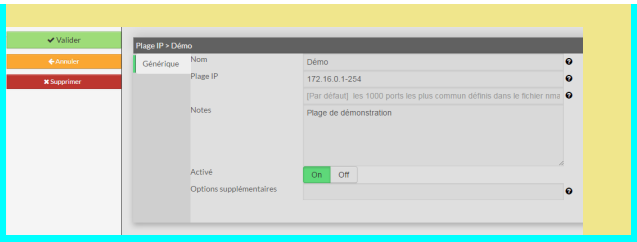
Les plages définies permettent de lancer un scan afin de détecter les hôtes présent dans cette plage. Ces hôtes sont ensuite analysés en fonction du système d'exploitation qui a été détecté.

Dans cette liste de plage, il est possible :

- d'ajouter une nouvelle plage **(2)**
- de configurer une plage existante **(3)**
- de lancer une analyse sur cette plage **(4)** si la plage est activée

Ajouter ou configurer une plage

Après avoir cliqué sur le bouton ajouter **(2)** ou configurer **(3)** sur l'image précédente, la page de configuration d'une plage réseau est affichée.



Remplissez le formulaire :

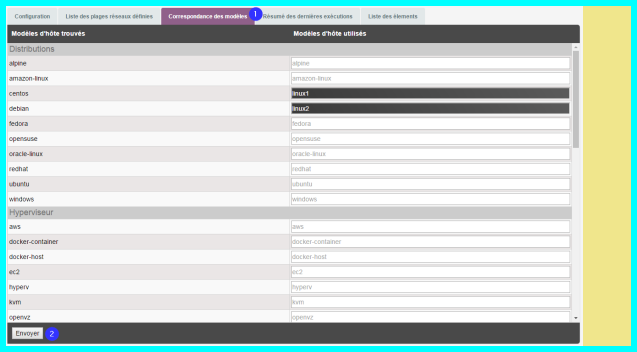
- Nom : Le nom à donner à la plage réseau
- Plage IP : la plage à scanner. Il peut s'agir:
  - D'une adresse IP unique. Exemple : "*192.168.1.254*"
  - D'une suite d'IP distinctes. Exemple : "*192.168.1.13 10.0.0.86 172.16.0.25*"
  - D'une plage au format CIDR. Exemple : *"192.168.1.0/24"*
  - D'une plage par intervalles. Exemple : "*192.168.1.1-254*"
- Notes : une description de la plage
- Activé : S'il est possible d'analyser la plage
- Options supplémentaires : les options qui seront passé à nmap pour effectuer le scan du réseau.

Puis dans le menu de gauche, plusieurs actions sont possibles:

- Sauvegarder la configuration de la plage réseau
- Annuler les modifications
- Si la configuration existait, la supprimer.

Correspondances des modèles

Cette partie est accessible depuis l'onglet **Correspondance des modèles (1)**.



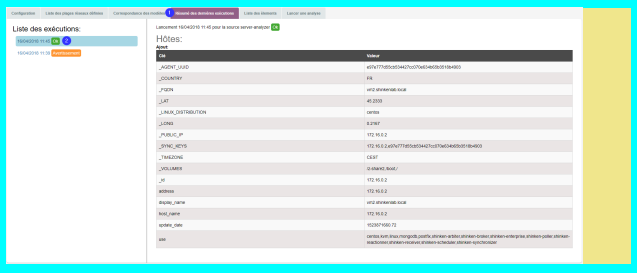
Cette page permet d'associer les modèles d'hôtes que l'analyseur remonte avec un modèle d'hôte défini dans Shinken.

Des associations sont déjà réalisées par défaut : les champs par défaut sont ceux surlignés en blanc avec un texte gris. Les champs surlignés en noir, sont les champs qui ont été défini par l'utilisateur. Pour les modifier, il suffit de saisir le nom d'un modèle dans la ligne correspondante et cliquer sur **Envoyer (2)** en bas de la page.

Lorsque la prochaine analyse sera effectuée, les modèles correspondant à ceux trouvés sur l'hôte seront utilisés.

Résumé des dernières exécutions

Cette partie est accessible depuis l'onglet **Résumé des dernières exécutions (1).**



Elle permet de garder la liste de la dernière journée d'exécution de l'analyseur.

Cliquez alors sur l'exécution **(2)** pour afficher les détails.

Liste des éléments

Cette partie est accessible depuis l'onglet **Liste des éléments (1).**

Elle permet d'afficher l'ensemble des éléments analysés par cette source.

Cliquez alors sur l'œil **(2)** pour afficher les détails.

Vous pouvez également supprimer l'élément analysé via le balai **(3)**.

Enfin, tous les éléments de la liste peuvent être supprimés d'un coup avec le balai dans les en-têtes de la liste **(4)**,

(une confirmation sera demandée)