Configuration d'un analyseur

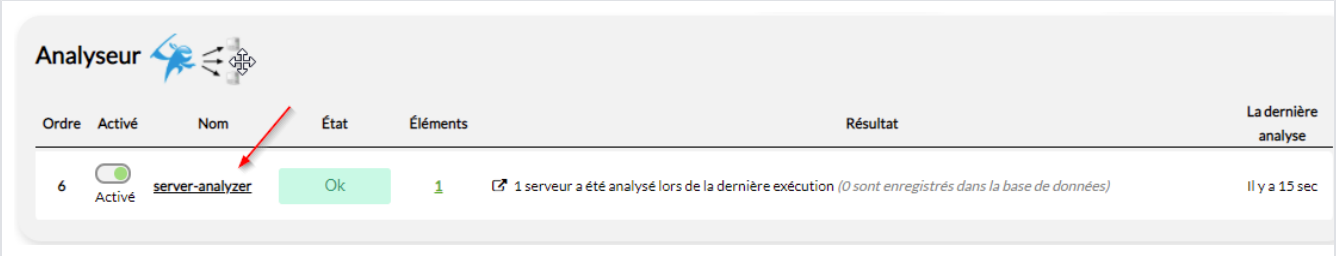
Sommaire

Création

Les analyseurs sont paramétrables via un fichier de configuration (*Voir Définition des modules Analyseur*) .

Présentation de l'interface

Dans la page principale, en cliquant sur le nom de la source, vous ouvrirez l'interface qui lui est dédiée.



En préambule, vous pouvez

- Importer la source à partir de l'interface de source en cliquant en haut à droite de l'écran sur l'icône

Dans cette interface, vous aurez 5 onglets qui vous permettront de visualiser la configuration de la source et le résultat des imports :

- Configuration avec les identifiants génériques ;
- La liste des plages réseau définies ;
- La correspondance des modèles ;
- Le résumé des dernières exécutions ;
- La liste des éléments ;

Configuration avec les identifiants génériques

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

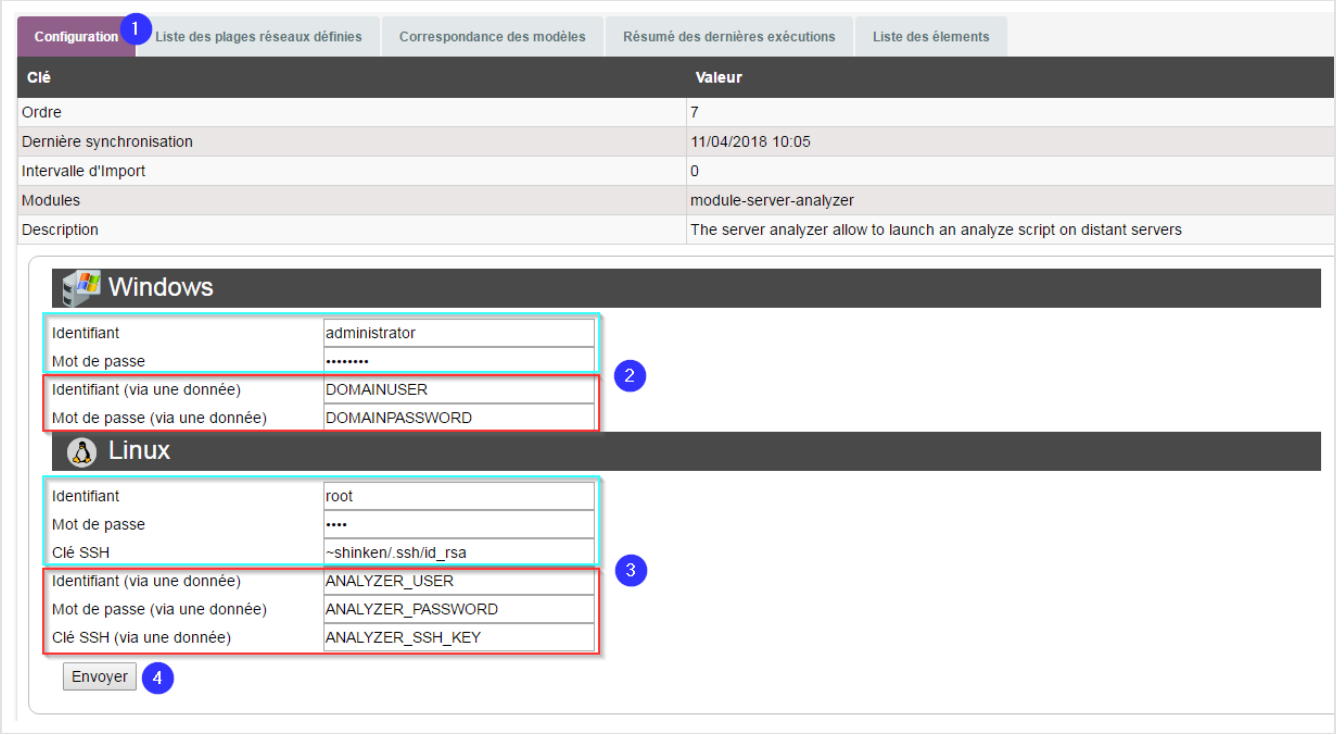
Ces identifiants seront utilisés par défaut pour chaque analyse lancée, mais il sera possible de lancer une analyse avec des identifiants différents (*voir la partie du lancement de l'analyse*).

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 puisse 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.

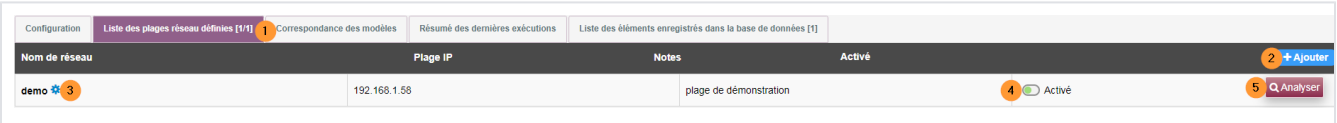
Une fois vos identifiants paramétrés, soumettez le formulaire pour enregistrer ces données **(4)**.



La liste des plages réseaux définies

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

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

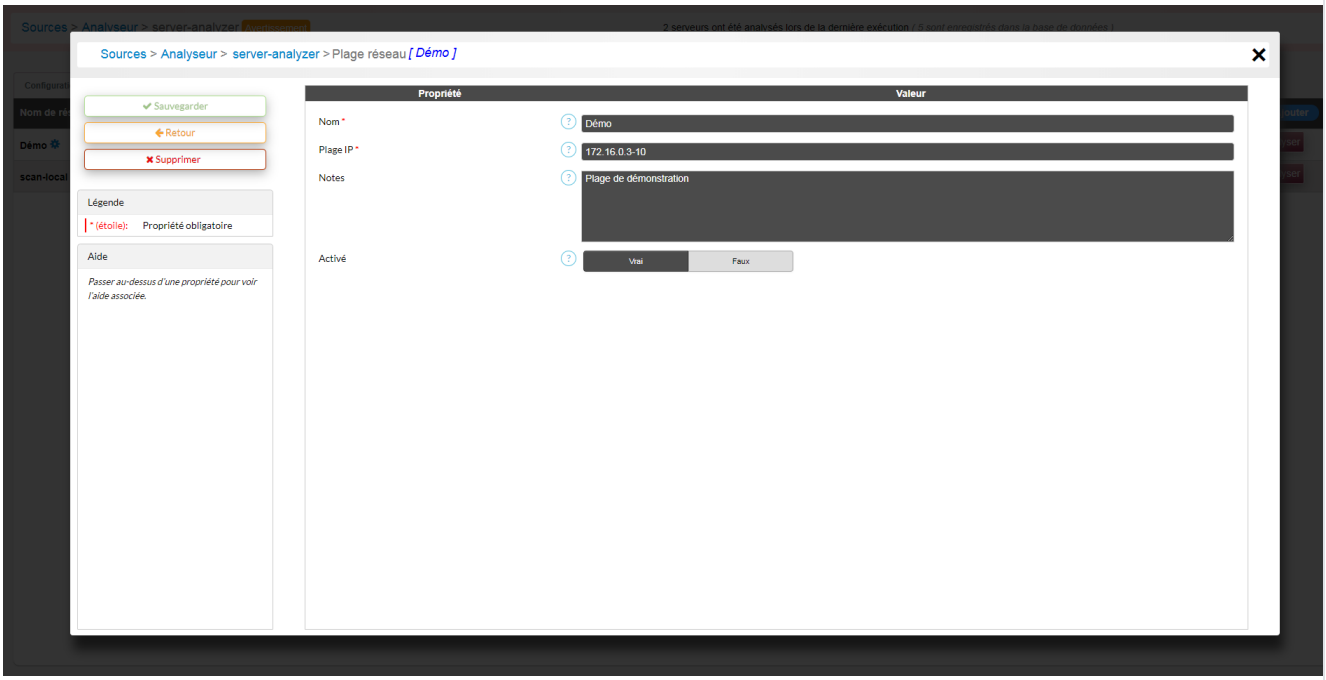


Dans cette liste de plage, il est possible :

- D'ajouter une nouvelle plage **(2)**
- De configurer une plage existante **(3)**
- D'activer ou désactiver une plage existante **(4)**
- De lancer une analyse sur cette plage **(5)**
  (*disponible seulement 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" (où 24 est le masque de sous-réseau)*
  - 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

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.

Dans la propriété **Plage IP**, un masque de sous réseau ne peut pas être inférieur à 16.

Le masque de sous-réseau définit le nombre de bit de l'IP qui seront utilisés pour la recherche. Une IP étant composée de 32 bits (8 par partie), choisir un masque de sous-réseau inférieur à 16 reviendrait à faire une recherche sur un ensemble d'IP trop large, ce qui réduirait les performances et risquerait de rendre le résultat de la recherche inutilisable.

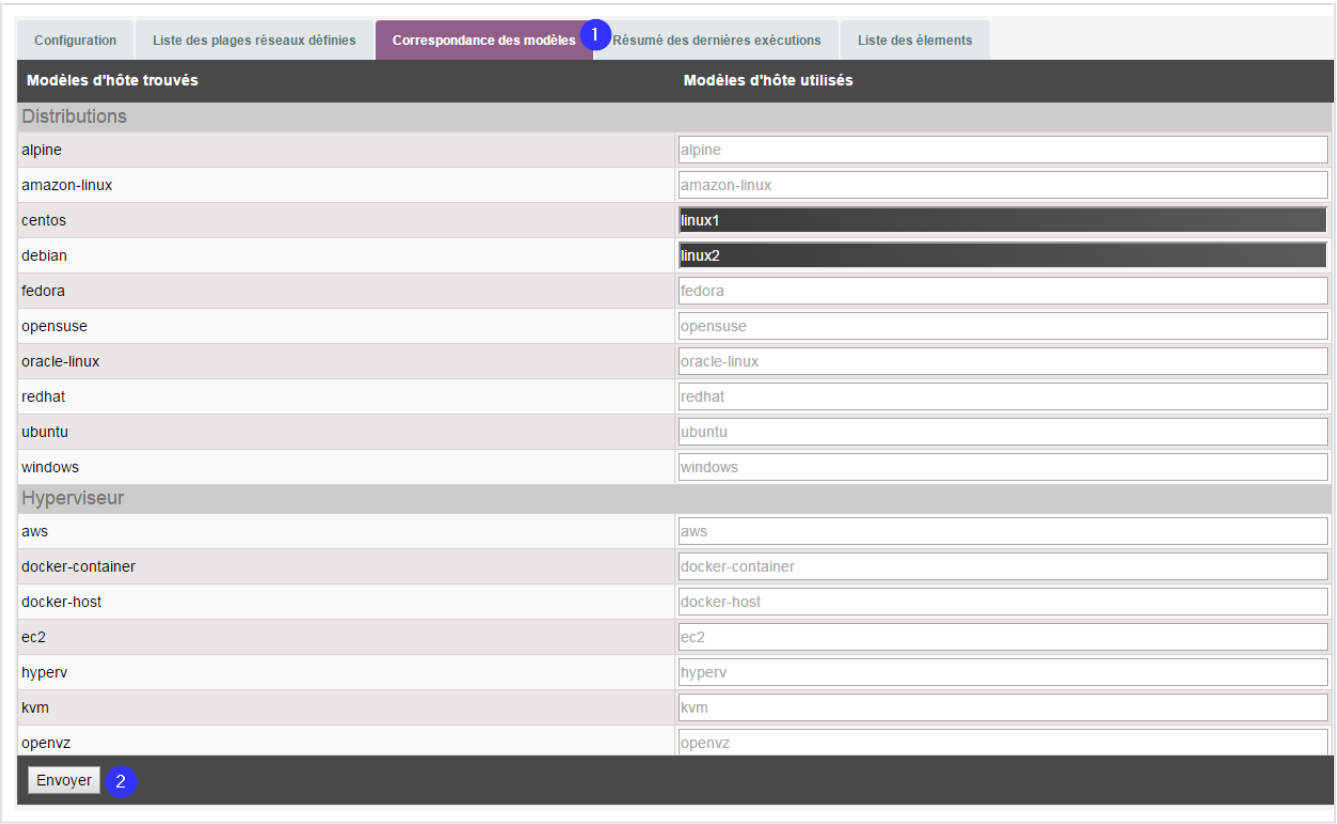
Exemples de masques de sous-réseau avec l'IP 192.168.1.1 :

16 => 192.168.X.X
24 => 192.168.1.X

X représente toutes les valeurs entre 0 et 255.

Correspondances des modèles

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



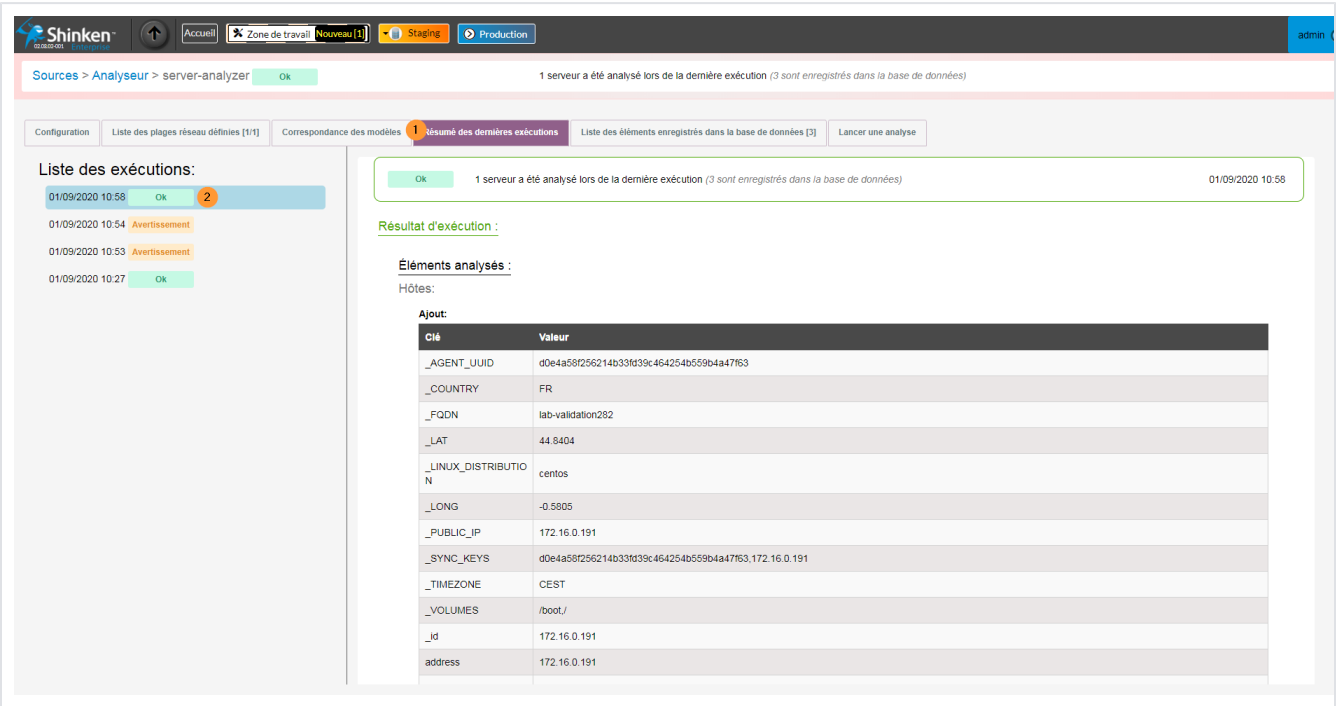
Cette page permet d'associer les modèles d'hôtes que l'analyseur remonte avec un modèle d'hôte défini dans Shinken.

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 définis par l'utilisateur. Pour les modifier, il suffit de saisir le nom d'un modèle dans la ligne correspondante et cliquer sur **E nvoyer (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).**

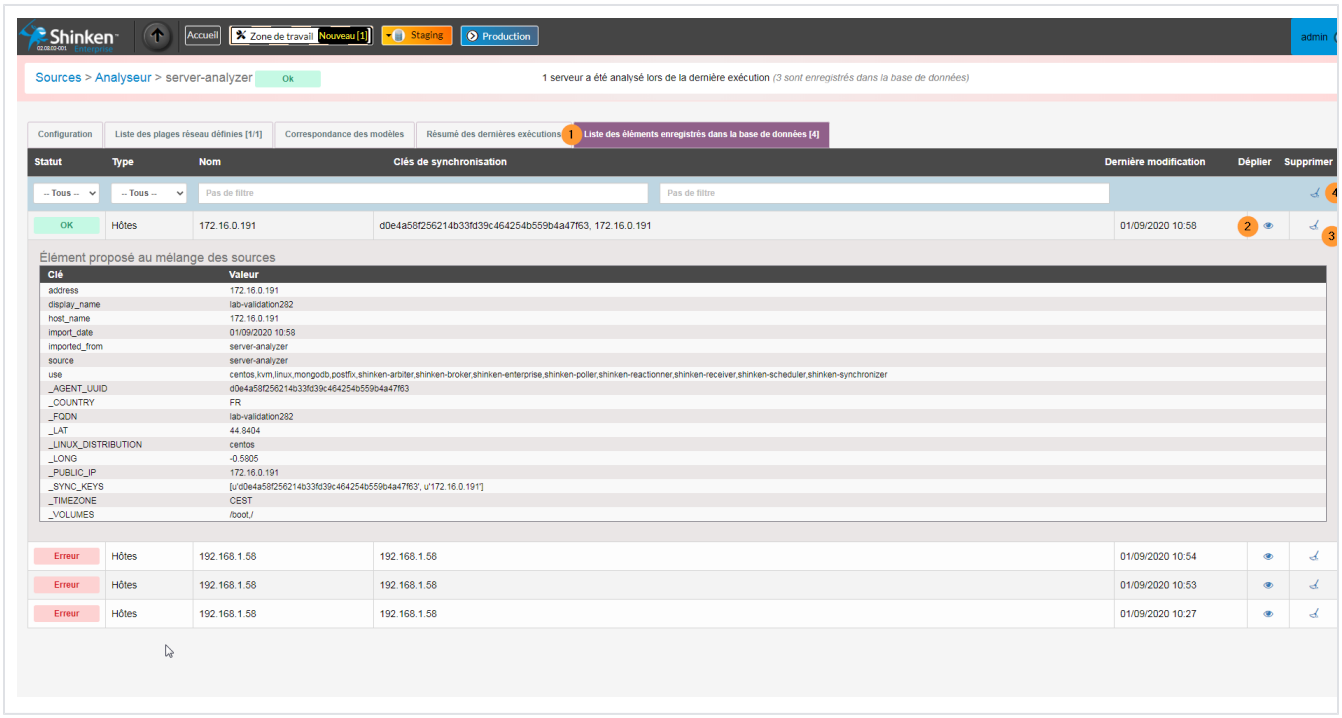


Elle permet de garder la liste de la dernière journée d'exécution de l'analyseur.

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*)