

Configuration d'un analyseur

Sommaire

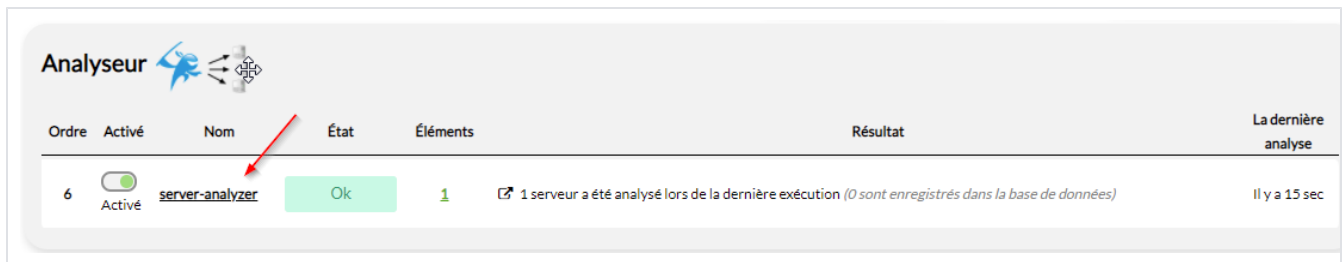
- Création
- Présentation de l'interface
 - Configuration avec les identifiants génériques
 - La liste des plages réseaux définies
 - Ajouter ou configurer une plage
 - Correspondances des modèles
 - Résumé des dernières exécutions
 - Liste des éléments

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.



Ordre	Activé	Nom	État	Éléments	Résultat	La dernière analyse
6	<input checked="" type="checkbox"/> Activé	server-analyzer	Ok	1	1 serveur a été analysé lors de la dernière exécution (0 sont enregistrés dans la base de données)	Il y a 15 sec

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**).

Clé	Valeur
Ordre	7
Dernière synchronisation	11/04/2018 10:05
Intervalle d'Import	0
Modules	module-server-analyzer
Description	The server analyzer allow to launch an analyze script on distant servers

Windows

Identifiant	administrator
Mot de passe
Identifiant (via une donnée)	DOMAINUSER
Mot de passe (via une donnée)	DOMAINPASSWORD

Linux

Identifiant	root
Mot de passe
Clé SSH	~shinken/.ssh/id_rsa
Identifiant (via une donnée)	ANALYZER_USER
Mot de passe (via une donnée)	ANALYZER_PASSWORD
Clé SSH (via une donnée)	ANALYZER_SSH_KEY

Envoyer

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.

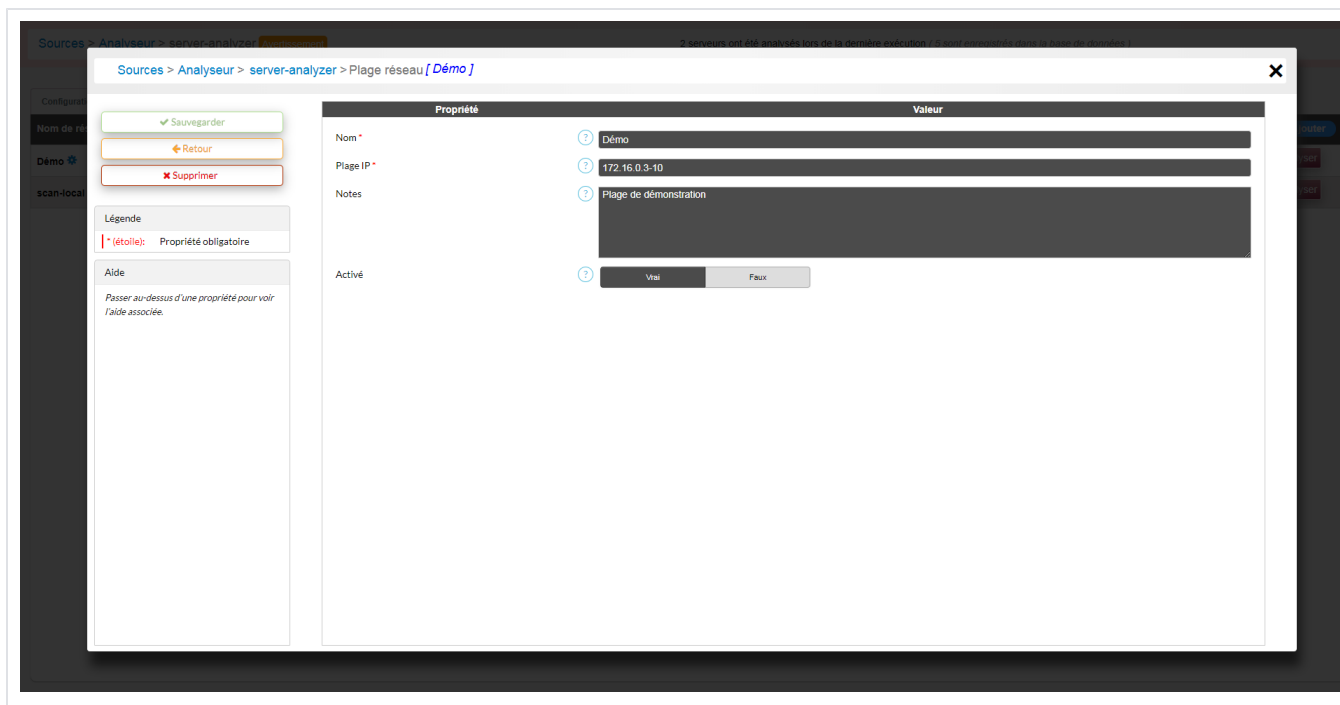
Nom de réseau	Plage IP	Notes	Activé
demo	192.168.1.58	plage de démonstration	Activé

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)**.

Configuration | Liste des plages réseaux définies | **Correspondance des modèles** 1 | Résumé des dernières exécutions | Liste des éléments

Modèles d'hôte trouvés	Modèles d'hôte utilisés
Distributions	
alpine	alpine
amazon-linux	amazon-linux
centos	linux1
debian	linux2
fedora	fedora
opensuse	opensuse
oracle-linux	oracle-linux
redhat	redhat
ubuntu	ubuntu
windows	windows
Hyperviseur	
aws	aws
docker-container	docker-container
docker-host	docker-host
ec2	ec2
hyperv	hyperv
kvm	kvm
openvz	openvz

Envoyer 2

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 **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)**.

Shinken 0.10.0

Accueil | Zone de travail | Nouveau [1] | Staging | Production | admin

Sources > Analyseur > server-analyzer Ok | 1 serveur a été analysé lors de la dernière exécution (3 sont enregistrés dans la base de données)

Configuration | Liste des plages réseau définies [11] | Correspondance des modèles | **Résumé des dernières exécutions** 1 | Liste des éléments enregistrés dans la base de données [2] | Lancer une analyse

Liste des exécutions :

- 01/09/2020 10:58 Ok 2
- 01/09/2020 10:54 Avertissement
- 01/09/2020 10:53 Avertissement
- 01/09/2020 10:27 Ok

Ok 1 serveur a été analysé lors de la dernière exécution (3 sont enregistrés dans la base de données) 01/09/2020 10:58

Résultat d'exécution :

Éléments analysés :

Hôtes:

Ajout:

Clé	Valeur
_AGENT_UUID	d0e4a58f256214b33f039c464254b559b4a47f63
_COUNTRY	FR
_FQDN	lab-validation282
_LAT	44.8404
_LINUX_DISTRIBUTION	centos
_LONG	-0.5805
_PUBLIC_IP	172.16.0.191
_SYNC_KEYS	d0e4a58f256214b33f039c464254b559b4a47f63,172.16.0.191
_TIMEZONE	CEST
_VOLUMES	/boot/
_id	172.16.0.191
address	172.16.0.191

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)**.

Shinken 2.12.0-rc1

Accueil Zone de travail Nouveau [1] Staging Production admin

Sources > Analyseur > server-analyzer OK 1 serveur a été analysé lors de la dernière exécution (3 sont enregistrés dans la base de données)

Configuration Liste des plages réseau définies [11] Correspondance des modèles Résumé des dernières exécutions 1 Liste des éléments enregistrés dans la base de données [4]

Statut	Type	Nom	Clés de synchronisation	Dernière modification	Déplier	Supprimer
OK	Hôtes	172.16.0.191	d0e4a58f256214b33fd39c464254b559b4a47f63, 172.16.0.191	01/09/2020 10:58	2	3

Élément proposé au mélange des sources

Clé	Valeur
address	172.16.0.191
display_name	lab-validation282
host_name	172.16.0.191
import_date	01/09/2020 10:58
imported_from	server-analyzer
source	server-analyzer
use	centos.kvm.linux.mongodb.postfix.shinken-arbiter.shinken-broker.shinken-enterprise.shinken-poller.shinken-reactionner.shinken-receiver.shinken-scheduler.shinken-synchronizer
_AGENT_UUID	d0e4a58f256214b33fd39c464254b559b4a47f63
_COUNTRY	FR
_FQDN	lab-validation282
_LAT	44.8404
_LINK_DISTRIBUTION	centos
_LONG	-0.5905
_PUBLIC_IP	172.16.0.191
_SYNC_KEYS	[/d0e4a58f256214b33fd39c464254b559b4a47f63; /172.16.0.191]
_TIMEZONE	CEST
_VOLUMES	/boot/

Erreur	Hôtes	192.168.1.58	192.168.1.58	01/09/2020 10:54	4
Erreur	Hôtes	192.168.1.58	192.168.1.58	01/09/2020 10:53	4
Erreur	Hôtes	192.168.1.58	192.168.1.58	01/09/2020 10:27	4

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)

Êtes-vous sûr de vouloir supprimer tous les éléments?

OK Annuler