Voir la configuration du module (discovery-import)

Sommaire

Concept

Cet onglet permet de consulter la configuration de la source définie dans son fichier de configuration (voir la page Collecteur de type discovery-import (Scan NMAP)).

Remarque : *Cet onglet ne permet pas encore d'éditer la configuration (Sera implémenté dans une prochaine version)*

Configuration générale

Clé	Valeur
Ordre	6
Intervalle d'import	5
Modules	discovery
Type de module	discovery-import

Ce chapitre contient tous les paramètres pour le chargement et fonctionnement des sources en général.

Nom	Type	Unité	Défaut	Commentaire
`source_name`	Texte	---	**discovery**	**Shinken conseille de choisir un nom en fonction de l'utilisation du module pour que la configuration soit simple à maintenir.** Doit être unique.
`module_type`	Texte	---	**discovery-import**	**Valeur obligatoire et non modifiable** (*permet au **Synchronizer** de charger le code logiciel correspondant*).
`order`	Entier	---	**10**	L'ordre de la source dans l'interface de configuration (*A un impact dans la fusion des données lors des imports de sources*, voir la page Le mélange des sources & les clés de synchronisation (sync-key)). Remarque : *Si l'ordre est changé depuis l'interface (page d'accueil), le fichier .cfg sera mis à jour.*
`import_interval`	Entier	Minute	**5**	Délai écoulé entre les imports automatiques de la source. • Si 0, la source ne sera jamais exécutée automatiquement.

Clés spécifiques à la source

Clé	Valeur
discovery-import__database__retry_connection_X_times_before_considering_an_error	15
discovery-import__database__wait_X_seconds_before_reconnect	5
mongodb_database	synchronizer
mongodb_retry_timeout	10
mongodb_ssh_keyfile	~shinken/.ssh/id_rsa
mongodb_ssh_user	shinken
mongodb_uri	mongodb://lab-validationSW1/?w=1&fsync=false
mongodb_use_ssh_retry_failure	1
mongodb_use_ssh_tunnel	1
nmap_mac_prefixes_path	/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-mac-prefixes
rules_path	/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/discovery_rules.json
synchronizer__source_discovery-import__database__password	
synchronizer__source_discovery-import__database__username	

Ce chapitre liste tous les paramètres qui sont spécifiques au fonctionnement de cette source.

Paramètres de connexion à Mongo

La discovery conserve sa configuration (ses plages réseau, ses règles de découvertes, ...) dans une base MongoDB. Ces paramètres permettent de s'y connecter.

Il est préférable d'utiliser la même base que le Synchronizer

Nom	Type	Unité	Défaut	Commentaire
`data_backend`	Texte	---	**mongodb**	Base de données où les informations de la source vont être stockées.
`mongodb_uri`	Url	---	**mongodb://localhost/?safe=false**	URL d'accès à MongoDB.
`mongodb_database`	Texte	---	**synchronizer**	Base MongoDB où sont stockées les données de la source.
`synchronizer__source_discovery-import__database__username`	Texte	---		Utilisateur pour l'authentification avec mot de passe à la base MongoDB. Utile uniquement si l'activation par mot de passe a été activé (*voir la page* MongoDB - activation de l'authentification par mot de passe)
`synchronizer__source_discovery-import__database__password`	Texte	---		Mot de passe de l'utilisateur utilisé pour l'authentification avec mot de passe à la base MongoDB. Utile uniquement si l'activation par mot de passe a été activé (*voir la page* MongoDB - activation de l'authentification par mot de passe)
`mongodb_use_ssh_tunnel`	0 ou 1	---	**0**	Défini si la connexion à la base de données est directe ou doit être encapsulée dans un tunnel SSH. • 1 : Connexion par tunnel SSH • 0 : Connexion directe
`mongodb_use_ssh_retry_failure`	Entier positif	---	**1**	Défini le nombre d'essais à réaliser si la connexion à la base de données est perdue.
`mongodb_ssh_user`	Texte	---	**shinken**	L'utilisateur qui sera utilisé si la connexion à la base de données est encapsulée dans un tunnel SSH.

`mongodb_ssh_keyfile`	Texte	---	**~shinken/.ssh/id_rsa**	La clé SSH qui sera utilisée si la connexion à la base de données est encapsulée dans un tunnel SSH.
`mongodb_retry_timeout`	Entier positif	Seconde	**10**	Temps de connexion maximum avant que la connexion ne soit considérée comme trop longue et cause un échec de connexion.
`discovery-import__database__retry_connection_X_times_before_considering_an_error`	Entier positif	---	**15**	Nombre de tentatives à effectuer avant de considérer une requête mongo comme étant en erreur.
`discovery-import__database__wait_X_seconds_before_reconnect`	Entier positif	Seconde	**5**	Temps d'attente entre chaque tentative de requête mongo.

Règles de découvertes

Permet de définir le fichier de règle de découverte de la discovery.

Nom	Type	Unité	Défaut	Commentaire
`rules_path`	Path	---	**/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/discovery_rules.json**	Fichier .json comportant les règles de découvertes (voir la page Les règles de découvertes du scan réseau (discovery-import)).

Correspondance entre l'adresse MAC et le constructeur

Nom	Type	Unité	Défaut	Commentaire
`nmap_mac_prefixes_path`	Path	---	**/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-mac-prefixes**	Fichier comportant les propres nmap-mac-prefixes (Correspondance entre l'adresse MAC et le constructeur).

Lors du scan d'une plage réseau, le collecteur discovery peut remonter le constructeur du matériel à l'aide de nmap.

Cette détection du constructeur se fait par identification de l'adresse MAC de l'équipement détecté sur le réseau. Pour la correspondance entre adresse MAC et constructeur, nmap utilise un fichier nommé *nmap-mac-prefixe*s qui comporte des adresses MAC associées à des constructeurs (macvendor).

Par exemple, si la machine récupérée par la discovery a pour adresse MAC "*0050BAXXXXX*", le constructeur détecté (macvendor) est "*D-Link*". Shinken fournit par défaut un fichier *nmap-mac-prefixes* qui sert de référence à nmap. Ce fichier est mis à jour à chaque mise à jour de Shinken.

```
# $Id$ generated with make-mac-prefixes.pl
# Original data comes from http://standards.ieee.org/regauth/oui/oui.txt
# These values are known as Organizationally Unique Identifiers (OUIs)
# See http://standards.ieee.org/faqs/OUI.html
# We have added a few unregistered OUIs at the end.
E043DB Shenzhen ViewAt Technology
2405F5 Integrated Device Technology (Malaysia) Sdn. Bhd.
3CD92B Hewlett Packard
9C8E99 Hewlett Packard
B499BA Hewlett Packard
1CC1DE Hewlett Packard
3C3556 Cognitec Systems GmbH
0050BA D-Link
00179A D-Link
18622C Sagemcom Broadband SAS
7C03D8 Sagemcom Broadband SAS
E8F1B0 Sagemcom Broadband SAS
00F871 DGS Denmark A/S
20BB76 COL Giovanni Paolo SpA
2C228B CTR SRL
348AAE Sagemcom Broadband SAS
BCEC23 Shenzhen Chuangwei-rgb Electronics
```

Pour créer des associations entre adresses MAC et constructeur personnalisées, il est possible créer un fichier *nmap-mac-prefixes* dans **/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/**, qui surchargera celui que Shinken met à disposition lors de l'installation. Un fichier d'exemple est disponible dans **/etc/shinken-user-example/configuration/daemons/synchronizers/sources/discovery**

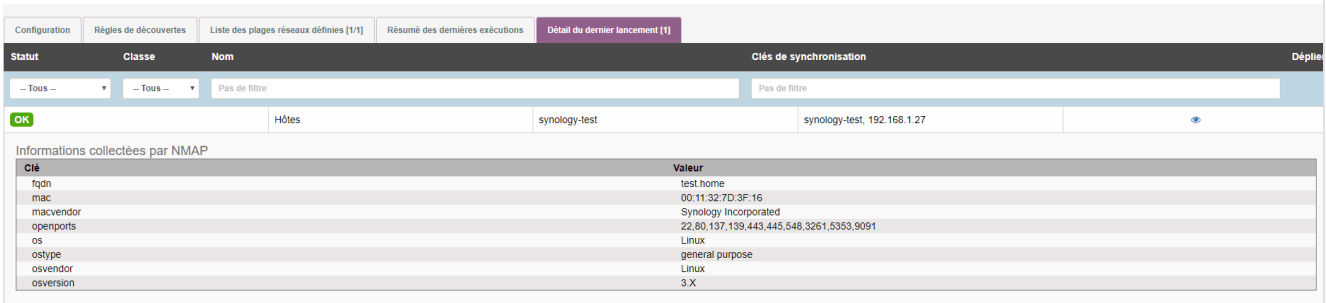
Ce fichier doit être au format de l'exemple donné et peut contenir des commentaires en commençant la ligne par un #.

Le fichier surcharge la liste présente par défaut dans l'installation de Shinken Entreprise.

Le fichier par défaut à utiliser comme modèle est le suivant: nmap-mac-prefixes.

Pour plus d'informations sur la syntaxe à respecter pour ce fichier, la documentation de nmap décrit la syntaxe requise pour ce fichier de préfixes: https://nmap.org/book/nmap-mac-prefixes.html

L'exemple suivant fournit une illustration sur la découverte d'un NAS Synology et la détection automatique du constructeur.



Précisions techniques

Sécurité : paramètres de la commande nmap

La commande nmap lancée par la source discovery utilise les paramètres suivants:

- **-PE** : Ping Scan (*Echo Request*)
- **-sU** : Scan UDP
- **-sT** : Scan TCP
- **--min-rate 1000** : Envoie un minimum de 1000 paquets par seconde
- **--max-retries 3** : Effectue au maximum 3 retransmissions en cas d'erreur sur les scan de ports

- **-T4** : Optimisation de performances
- **-O** : Détection des systèmes d'exploitation
- **-oX** : Export XML (*utilisé pour l'interprétation des données par Shinken*)

Clés de synchronisation

Les clés de synchronisation sont des valeurs utilisées lors de l'étape du mélange des sources (*voir la page* Modules de Sources (imports) et de Taggers (qualification)) qui permet de choisir quel élément de cette source se mélange avec quel élément d'une autre source (*voir la page* ***Le mélange des sources & les clés de synchronisation (sync-key)***).

Propriétés par défaut utilisé pour la construction des clés de synchronisation

Propriétés par défaut utilisé pour la construction des clés de synchronisation :

Nom	Type	Unité	Défaut	Commentaire
`Nom de l'élément`	Texte	---	**---**	Cette propriété ne peut pas être retirée des propriétés utilisées pour faire les clés de synchronisation
`_SE_UUID`	Texte	---	**---**	Cette propriété ne peut pas être retirée des propriétés utilisées pour faire les clés de synchronisation
`address`	Texte	---	**---**	Présente que pour les hôtes