

# Collecteur de type discovery-import ( Scan NMAP )

## Sommaire

- [Concept](#)
- [Activation du collecteur](#)
  - [Exemple d'activation de la source nommée "discovery" sur le Synchronizer \( configuration livrée par défaut par Shinken \)](#)
- [Configuration](#)
  - [Fichier de configuration](#)
  - [Détails des sections composant le fichier de configuration](#)
    - [Identification du module](#)
    - [Fonctionnement de la source](#)
    - [Options d'accès à la base de données](#)
    - [Options du module](#)

## Concept

Ce module source permet de détecter automatiquement des équipements réseau et des serveurs physiques dans l'infrastructure pour faciliter et accélérer leur import dans la configuration.

- Cette source utilise la commande nmap pour la découverte des équipements.
- pour cela la commande nmap :
  - Scanne les machines présentes sur le réseau et détecte les ports ouverts ;
  - Essaye de déterminer le constructeur de l'équipement en fonction de son adresse MAC ;
  - Si possible, détermine son FQDN ( *Fully Qualified Domain Name* ) ;

La source Discovery permet de définir des règles qui :

- suivant les valeurs remontées par la commande nmap ;
- apportent un complément d'information sur les équipements découverts ;
- Ce complément d'information peut être :
  - Des modèles d'hôtes suivant le type d'équipement ;
  - L'ajout d'un préfixe au nom de l'équipement ;

Cette page explique comment définir ce type de collecteur.

La page "Collecteur de type ( discovery-import ) - Import depuis un scan réseau" décrit comment l'utiliser ( voir la page [Collecteur de type \( discovery-import \) - Import depuis un scan réseau](#) ).

## Activation du collecteur

La source de type "discovery-import" est une source qui doit être activée sur le démon Synchronizer.

- L'activation de la source s'effectue en ajoutant le **nom** de la source dans la configuration du Synchronizer.
  - Par défaut, l'installation de Shinken Entreprise va mettre à disposition cette source sous le nom "discovery".
    - Le fichier de configuration de la source est disponible sous **/etc/shinken/sources/discovery.cfg**.
  - Pour cela, il faut ouvrir le fichier de configuration du Synchronizer et ajouter dans le paramètre **sources**, le nom de la source de type "discovery-import".
- Contraintes :
  - Activable uniquement sur le Synchronizer ( voir la page [Définition du démon \( synchronizer-master.cfg \)](#) ).
  - ⚠ Il ne peut y avoir **qu'une seule** source de type "discovery-import". ⚠

Pour prendre en compte le changement de configuration, il faut redémarrer le Synchronizer :

```
service-shinken-synchronizer restart
```

## Exemple d'activation de la source nommée "discovery" sur le Synchronizer ( configuration livrée par défaut par Shinken )

L'exemple suivant :

- active la source "discovery",
- sur le Synchronizer, dont la configuration est dans le fichier **/etc/shinken/synchronizers/synchronizer-master.cfg**

Modification dans le fichier du module **/etc/shinken/synchronizers/synchronizer-master.cfg** :

```
define synchronizer{
    [...]          #===== Sources =====
    # syncui                Automatically added
    # discovery              Automatically added
    # listener-shinken      Automatically added
    # server-analyzer       Automatically added
    # cfg-file-shinken      Mandatory Standard Shinken Enterprise packs
    # listener-rest         SAMPLE for REST listener
    # active-dir-example    SAMPLE for active directory
    # sync-vmware           SAMPLE for VMWare (deprecated)
    # cfg-file-nagios       SAMPLE for nagios import
    # openldap-example     SAMPLE for OpenLDAP import
    # cfg-file-sample       SAMPLE for Shinken framework import
    # synchronizer-collector-vmware SAMPLE for VMWare
    sources              discovery, Source 2, Source 3
    [...]
}
```

Puis redémarrage du Synchronizer:

```
service-shinken-synchronizer restart
```

## Configuration

La configuration du module se trouve par défaut dans le fichier **/etc/shinken/sources/discovery.cfg**.

### Fichier de configuration

**/etc/shinken/sources/discovery.cfg**

```
# CFG_FORMAT_VERSION 1 ( SHINKEN : DON'T TOUCH THIS LINE )

#=====
# discovery
#=====
# Daemons that can load this source:
# - synchronizer
# This source module allows you to automatically detect network devices and physical servers in your
# infrastructure and import them in the configuration.
# MANDATORY SOURCE
#=====

define source {

    # #
    #     SOURCE IDENTITY     #
    # #

    # Source name [ Must be unique ]                                [ MANDATORY ]
}
#

    source_name                                discovery

    # Source module type [ Do not edit ]                            [ MANDATORY ]
]
#

    module_type                                discovery-import
```

```

# Interval between each automatic
import
# Interval in minutes between each automatic import of the
source
# -> Setting it to 0 will deactivate the automatic import and can only be done
manually
# Default :
5

#

import_interval 5

# Order of priority when merging
data
# The final element will take the value of the element from the source with the highest
priority
# -> Priority at source with the order closest to
1
# Default :
10

#

order 10

# #
# DATABASE OPTIONS #
# #

# General #

# Database
backend

#

# Default : mongodb => Use Mongo as database
backend
#

data_backend mongodb

# MongoDB parameters #

# USE ONLY IF "data_backend" IS SET TO
"mongodb"

# MongoDB uri definition . You can find the mongodb uri syntax
at
# https://docs.mongodb.com/manual/reference/connection-
string/

#

# Default : mongodb://localhost/?
w=1&fsync=false
#

mongodb_uri mongodb://localhost/?w=1&fsync=false

# Database to
use

#

# Default :
synchronizer

```

```

#

mongodb_database                                synchronizer

# username/password to authenticate to
MongoDB.
# Both parameters must be provided for authentication to function
correctly.
#

# synchronizer__source_discovery-import__database__username

#

# synchronizer__source_discovery-import__database__password

# SSH tunnel activation to secure your mongodb
connection
# That will allow all mongodb to be encrypted & authenticated with
SSH

#

#           Default : 0 => Disable ( disable ssh tunnel
)
#           ...      : 1 => Enable  ( enable ssh tunnel
)
#

mongodb_use_ssh_tunnel                            0

# If the SSH connection goes wrong, then retry use_ssh_retry_failure time
before_shinken_inactive

#

#           Default : 1 ( number of retry
)
#

mongodb_use_ssh_retry_failure                      1

# SSH user to connect to the mongodb
server.

#

#           Default :
shinken
#

mongodb_ssh_user                                  shinken

# SSH keyfile to connect to the mongodb
server.

#

#           Default : ~shinken/.ssh
/id_rsa
#

mongodb_ssh_keyfile                              ~shinken/.ssh/id_rsa

```

```

# SSH Timeout used to test if the SSH tunnel is viable or not, in
seconds.

#
#           Default : 10 ( seconds
)
#

mongodb_retry_timeout                                10

# Number of connection tries to do before considering a request as an
error.

#
#           Default : 15 ( tries
)
#

discovery-import__database__retry_connection_X_times_before_considering_an_error 15

# Time interval between each
attempt.

#
#           Default : 5 ( seconds
)
#

discovery-import__database__wait_X_seconds_before_reconnect 5

# #
#   INTERNAL OPTIONS      #
# #

# Path to your discovery rules
file.

#

#           Default : /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery
/discovery_rules.json
#

rules_path                                           /etc/shinken-user/configuration/daemons/synchronizers
/sources/discovery/discovery_rules.json

# Path to your nmap-mac-prefixes
file.

#

#           Default : /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-
mac-prefixes
#

nmap_mac_prefixes_path                             /etc/shinken-user/configuration/daemons/synchronizers
/sources/discovery/nmap/nmap-mac-prefixes
}

```

## Détails des sections composant le fichier de configuration

### Identification du module

| Nom         | Type  | Unité | Défaut           | Description                                                                                                       |
|-------------|-------|-------|------------------|-------------------------------------------------------------------------------------------------------------------|
| source_name | Texte | ---   | discovery        | Valeur obligatoire et non modifiable.                                                                             |
| module_type | Texte | ---   | discovery-import | Valeur obligatoire et non modifiable ( permet au <i>Synchronizer</i> de charger le code logiciel correspondant ). |

### Fonctionnement de la source

```
define source {
    ...
    # Interval between each automatic
import
    # Interval in minutes between each automatic import of the
source
    # -> Setting it to 0 will deactivate the automatic import and can only be done
manually
    # Default :
5
#
import_interval 5
# Order of priority when merging
data
    # The final element will take the value of the element from the source with the highest
priority
    # -> Priority at source with the order closest to
1
    # Default :
10
#
order 10 ...
}
```

| Nom             | Type   | Unité  | Défaut | Description                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|--------|--------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 ). <ul style="list-style-type: none"><li>Un nombre.</li><li>Voir la page <a href="#">Le mélange des sources &amp; les clés de synchronisation (sync-key)</a> pour plus d'information au sujet des fusions.</li></ul> 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. <ul style="list-style-type: none"><li>Un nombre ( en minutes ).</li><li>Si 0, la source ne sera jamais exécutée automatiquement.</li></ul>                                                                                                                                                                                                                                                      |

### Options d'accès à la base de données

/etc/shinken/sources/discovery.cfg

# #

```

#      DATABASE OPTIONS      #
# #

#   General   #

#   Database
backend

#

#           Default : mongodb => Use Mongo as database
backend
#

data_backend                                mongodb

#   MongoDB parameters   #

#   USE ONLY IF "data_backend" IS SET TO
"mongodb"

#   MongoDB uri definition . You can find the mongodb uri syntax
at
#   https://docs.mongodb.com/manual/reference/connection-
string/

#

#           Default : mongodb://localhost/?
w=1&fsync=false
#

mongodb_uri                                mongodb://localhost/?w=1&fsync=false

#   Database to
use

#

#           Default :
synchronizer
#

mongodb_database                            synchronizer

#   username/password to authenticate to
MongoDB.
#   Both parameters must be provided for authentication to function
correctly.
#

#   synchronizer__source_discovery-import__database__username

#

#   synchronizer__source_discovery-import__database__password

#   SSH tunnel activation to secure your mongodb
connection
#   That will allow all mongodb to be encrypted & authenticated with
SSH

#

#           Default : 0 => Disable ( disable ssh tunnel
)

```

```

#           ...           : 1 => Enable ( enable ssh tunnel
)
#

mongodb_use_ssh_tunnel                                0

# If the SSH connection goes wrong, then retry use_ssh_retry_failure time
before_shinken_inactive

#

#           Default : 1 ( number of retry
)
#

mongodb_use_ssh_retry_failure                        1

# SSH user to connect to the mongodb
server.

#

#           Default :
shinken
#

mongodb_ssh_user                                    shinken

# SSH keyfile to connect to the mongodb
server.

#

#           Default : ~shinken/.ssh
/id_rsa
#

mongodb_ssh_keyfile                                ~shinken/.ssh/id_rsa

# SSH Timeout used to test if the SSH tunnel is viable or not, in
seconds.

#

#           Default : 10 ( seconds
)
#

mongodb_retry_timeout                                10

# Number of connection tries to do before considering a request as an
error.

#

#           Default : 15 ( tries
)
#

discovery-import__database__retry_connection_X_times_before_considering_an_error 15

# Time interval between each
attempt.

#

```

```
#           Default : 5 ( seconds
)
#

discovery-import__database__wait_X_seconds_before_reconnect 5
```

| Nom                                                                              | Type           | Unité   | Défaut                                 | Description                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------|----------------|---------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data_backend                                                                     | Texte          | ---     | <b>mongodb</b>                         | Base de données où les informations de la source vont être stockées.                                                                                                                                                                                                  |
| mongodb_uri                                                                      | url            | ---     | <b>mongodb://localhost/?safe=false</b> | URL d'accès à MongoDB.                                                                                                                                                                                                                                                |
| mongodb_database                                                                 | Texte          | ---     | <b>synchronizer</b>                    | 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.<br><br>Utile uniquement si l'activation par mot de passe a été activé ( voir la page <a href="#">MongoDB - activation de l'authentification par mot de passe</a> )                           |
| 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.<br><br>Utile uniquement si l'activation par mot de passe a été activé ( voir la page <a href="#">MongoDB - activation de l'authentification par mot de passe</a> ) |
| mongodb_use_ssh_tunnel                                                           | 0 ou 1         | ---     | <b>0</b>                               | Défini si la connexion à la base de données est directe ou doit être encapsulée dans un tunnel SSH.                                                                                                                                                                   |
| mongodb_use_ssh_retry_failure                                                    | Entier positif | ---     | <b>1</b>                               | Défini le nombre d'essais à réaliser si la connexion à la base de données est perdue.                                                                                                                                                                                 |
| mongodb_ssh_user                                                                 | Texte          | ---     | <b>shinken</b>                         | L'utilisateur qui sera utilisé si la connexion à la base de données est encapsulée dans un tunnel SSH.                                                                                                                                                                |
| mongodb_ssh_keyfile                                                              | Texte          | ---     | <b>~shinken/.ssh/id_rsa</b>            | 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 | <b>10</b>                              | 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 | ---     | <b>15</b>                              | Nombre de tentatives à effectuer avant de considérer une requête mongo comme étant en erreur.                                                                                                                                                                         |

|                                                                          |                |         |   |                                                          |
|--------------------------------------------------------------------------|----------------|---------|---|----------------------------------------------------------|
| <pre>discovery- import__database__wait_X_seconds_before _reconnect</pre> | Entier positif | Seconde | 5 | Temps d'attente entre chaque tentative de requête mongo. |
|--------------------------------------------------------------------------|----------------|---------|---|----------------------------------------------------------|

### Options du module

| /etc/shinken/sources/discovery.cfg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <pre># # #     INTERNAL OPTIONS     # # #  # Path to your discovery rules file.  #  #           Default : /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery /discovery_rules.json  #  rules_path                                     /etc/shinken-user/configuration/daemons/synchronizers /sources/discovery/discovery_rules.json  # Path to your nmap-mac-prefixes file.  #  #           Default : /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap- mac-prefixes  #  nmap_mac_prefixes_path                       /etc/shinken-user/configuration/daemons/synchronizers /sources/discovery/nmap/nmap-mac-prefixes</pre> |  |

| Nom                    | Type | Unité | Défaut                                                                                         | Description                                                                                                                                                                                            |
|------------------------|------|-------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rules_path             | Path | ---   | /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/discovery_rules.json   | Fichier .json comportant les règles de découvertes ( voir la page <a href="#">Les règles de découvertes du scan réseau ( discovery-import )</a> ).                                                     |
| nmap_mac_prefixes_path | Path | ---   | /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-mac-prefixes | Fichier comportant les propres nmap-mac-prefixes ( pour la orrespondance entre l'adresse MAC et le constructeur ( voir la page <a href="#">Voir la configuration du module ( discovery-import )</a> ). |