

# Module de source discovery ( de type discovery-import )

## Sommaire

- [Concept](#)
- [Activation du collecteur](#)
- [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](#)

## Description

Ce module source vous permet de détecter automatiquement des équipements réseau et des serveurs physiques dans votre 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.

## Activation du collecteur

Vous pouvez avoir **uniquement une** source de type discovery-import.

Par défaut, l'installation de Shinken Entreprise va mettre à disposition cette source sous le nom "discovery".

- Le fichier est disponible sous **/etc/shinken/sources/discovery.cfg**
- Pour avoir cette source disponible
  - Le nom "discovery" doit être présent dans le paramètre **sources** du fichier **/etc/shinken/synchronizers/synchronizer-master.cfg**

Exemple:

```
define synchronizer {
    ...
    sources          Source 1, Source 2, Source 3, discovery
    ...
}
```

Pour prendre en compte le changement de configuration, redémarrer le 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**

```
#####
# 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

#   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	Unités	Défaut	Commentaire
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

```

# 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	Unités	Défaut	Commentaire
-----	------	--------	--------	-------------

order	Entier	---	10	<p>L'ordre de la source dans l'interface de configuration ( A un impact dans la fusion des données lors des imports de sources ).</p> <ul style="list-style-type: none"> <li>• Un nombre</li> <li>• ( voir la page <a href="#">Le Synchronizer</a> pour plus d'information au sujet des fusions )</li> </ul> <p>Remarque : Si vous changez l'ordre depuis l'interface ( page d'accueil ), le fichier .cfg sera mis à jour.</p>
import_inter val	Entier	minutes	5	<p>Délai écoulé entre les imports automatiques de la source.</p> <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

# 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	Unités	Défaut	Commentaire
data_backend	Texte	---	mongodb	Base de données où les informations de la source vont être stockées
mongodb_uri	url	---	<a href="#">mongodb://localhost/?safe=false</a>	URL d'accès à MongoDB
mongodb_database	Texte	---	synchronizer	Base Mongo où sont stockées les données de la source
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
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

## Options du module

## /etc/shinken/sources/discovery.cfg

```
# #
# 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
```

Nom	Type	Unités	Défaut	Commentaire
rules_path	Path	---	/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/discovery_rules.json	Fichier .json comportant vos règles de découvertes ( voir <a href="#">règles de découvertes</a> )
nmap_mac_prefixes_path	Path	---	/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-mac-prefixes	Fichier comportant vos propres nmap-mac-prefixes ( voir <a href="#">mécanisme de correspondance entre adresse MAC et constructeur</a> )