

# Collecteur de type ( discovery-import ) - Import depuis un scan réseau

## Sommaire

- [Introduction](#)
- [Fonctionnement](#)
- [Définition de la source](#)
- [Utilisation de la source](#)
  - [Import via la page principale](#)
  - [Présentation de l'interface](#)

## Introduction

Ce collecteur 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 :

- 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.

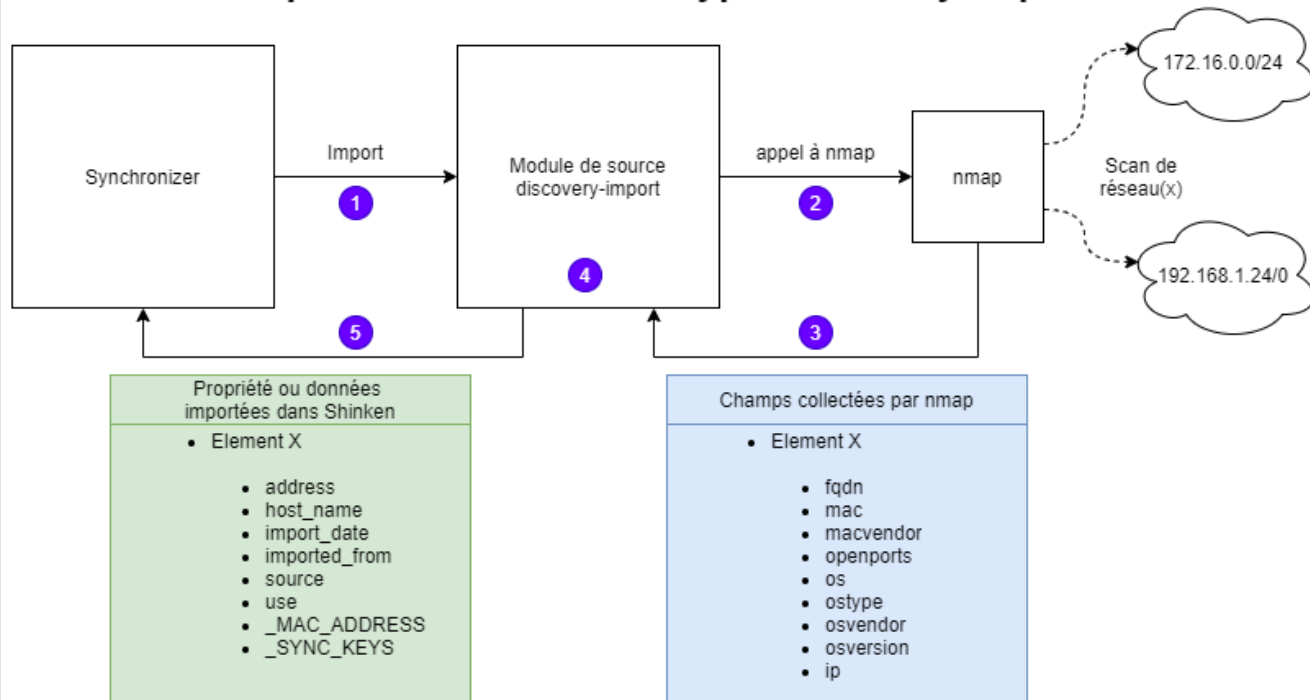
Une fois la découverte exécutée, les équipements détectés et qualifiés sont alors présentés en tant que nouveautés ou différences dans l'interface de Configuration.

## Fonctionnement

Lors de l'import de la source discovery, la séquence se décompose en 5 étapes :

1. Le module va lancer un scan réseau par plage ( **1** )
2. Ce scan est réalisé à l'aide de nmap ( **2** )
3. À la fin du scan réseau, le module reçoit les éléments et leurs champs collectés ( **3** )
4. Des règles de découvertes permettent de qualifier les éléments en ajoutant des modèles d'hôte ou un préfixe sur le nom de l'élément ( **4** )
5. Les éléments sont alors proposés dans le Synchronizer. ( **5** )

## Import d'une source de type discovery-import



Regardons en détail comment est construit un hôte proposé par la discovery :

Propriété ou données importées dans Shinken <span style="color: purple;">5</span>	Correspondance directe <span style="color: purple;">4</span>	Champs collectés par nmap <span style="color: purple;">3</span>																																				
<table border="1"> <thead> <tr> <th>Propriété ou donnée</th> <th>Valeur</th> </tr> </thead> <tbody> <tr> <td>host_name</td> <td>mon_hote.localdomain</td> </tr> <tr> <td>address</td> <td>192.168.1.125</td> </tr> <tr> <td>_MAC_ADDRESS</td> <td>AA:BB:CC:DD:EE:FF</td> </tr> <tr> <td>_SYNC_KEYS</td> <td>192.168.1.125, mon_hote.localdomain</td> </tr> </tbody> </table> <p>use: windows2008r2, pop3</p> <p>source: dicovery</p> <p>import_date: 11/10/2021 09:16</p>	Propriété ou donnée	Valeur	host_name	mon_hote.localdomain	address	192.168.1.125	_MAC_ADDRESS	AA:BB:CC:DD:EE:FF	_SYNC_KEYS	192.168.1.125, mon_hote.localdomain	<p>application des règles <span style="color: purple;">4</span></p> <p>SI ( os=windows ET osversion=7 ) ALORS AJOUTER dans use windows2008r2</p> <p>SI ( openports contient 110 ) ALORS AJOUTER dans use pop3</p>	<table border="1"> <thead> <tr> <th>Champ collecté</th> <th>Valeur</th> </tr> </thead> <tbody> <tr> <td>fqdn</td> <td>mon_hote.localdomain</td> </tr> <tr> <td>ip</td> <td>192.168.1.125</td> </tr> <tr> <td>mac</td> <td>AA:BB:CC:DD:EE:FF</td> </tr> <tr> <td>macvendor</td> <td>DELL</td> </tr> <tr> <td>openports</td> <td>110</td> </tr> <tr> <td>os</td> <td>windows</td> </tr> <tr> <td>ostype</td> <td>server</td> </tr> <tr> <td>osvendor</td> <td>Microsoft</td> </tr> <tr> <td>osversion</td> <td>7</td> </tr> </tbody> </table> <p>Paramètre de l'import <span style="color: purple;">1</span></p> <table border="1"> <thead> <tr> <th>Paramètre de l'import</th> <th>valeur</th> </tr> </thead> <tbody> <tr> <td>source_name</td> <td>dicovery</td> </tr> <tr> <td>import_date</td> <td>10/11/2021 09:16</td> </tr> </tbody> </table>	Champ collecté	Valeur	fqdn	mon_hote.localdomain	ip	192.168.1.125	mac	AA:BB:CC:DD:EE:FF	macvendor	DELL	openports	110	os	windows	ostype	server	osvendor	Microsoft	osversion	7	Paramètre de l'import	valeur	source_name	dicovery	import_date	10/11/2021 09:16
Propriété ou donnée	Valeur																																					
host_name	mon_hote.localdomain																																					
address	192.168.1.125																																					
_MAC_ADDRESS	AA:BB:CC:DD:EE:FF																																					
_SYNC_KEYS	192.168.1.125, mon_hote.localdomain																																					
Champ collecté	Valeur																																					
fqdn	mon_hote.localdomain																																					
ip	192.168.1.125																																					
mac	AA:BB:CC:DD:EE:FF																																					
macvendor	DELL																																					
openports	110																																					
os	windows																																					
ostype	server																																					
osvendor	Microsoft																																					
osversion	7																																					
Paramètre de l'import	valeur																																					
source_name	dicovery																																					
import_date	10/11/2021 09:16																																					

### Définition de la source

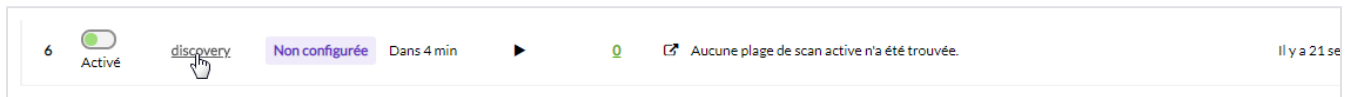
Vous trouverez la procédure de mise en place et de configuration dans la page suivante [Collecteur de type discovery-import \( Scan NMAP \)](#)

### Utilisation de la source

### Import via la page principale

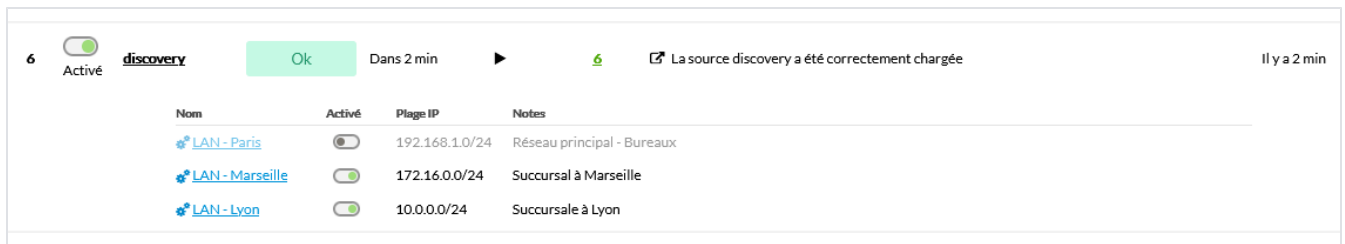
Lorsque vous activez le collecteur, il sera non configuré.

- Vous devez entrer dans les pages de configuration. Pour cela, dans la [Page Principale](#), cliquez sur le nom de la source "discovery" pour accéder aux détails de la source.



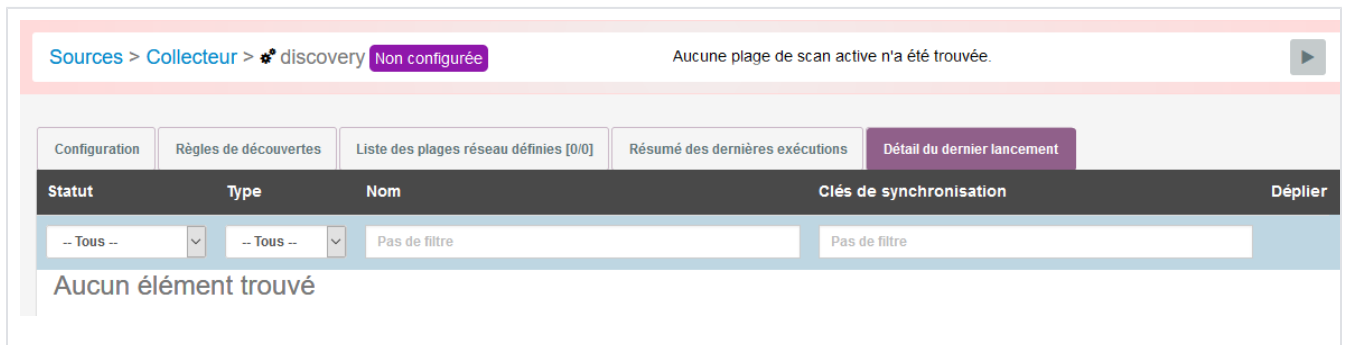
Une fois la source configurée, la liste des plages réseau est affichée sur la page principale.

- Vous pouvez importer la source en cliquant sur l'icône ▶
- Pour en savoir plus sur les plages réseaux, voir [Liste des plages réseau](#)



## Présentation de l'interface

Vous trouverez une présentation détaillée des onglets composants l'interface du collecteur de type `discovery-import`



Afin d'utiliser rapidement la source en main, vous pouvez utiliser le guide [Les premiers pas avec le Collecteur de type discovery-import](#).