

Les premiers pas avec le Collecteur de type discovery-import

Sommaire

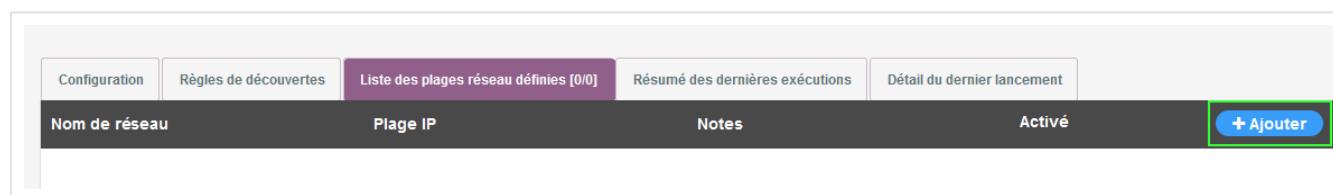
Réalisons un scan étape par étape
Étape 1 : Editer et ajouter une plage réseau
Étape 2 : Lancer un scan
Étape 3 : Les équipements trouvés

Réalisons un scan étape par étape

Étape 1 : Editer et ajouter une plage réseau

Les plages réseau scannées par le collecteur discovery peuvent être créées et modifiées dans l'onglet "**Liste des plages réseau définies**".

Le bouton "**+ Ajouter**" permet d'ajouter une nouvelle plage réseau à scanner.



The screenshot shows a web interface with a navigation bar containing five tabs: 'Configuration', 'Règles de découvertes', 'Liste des plages réseau définies [0/0]', 'Résumé des dernières exécutions', and 'Détail du dernier lancement'. Below the tabs is a table with the following columns: 'Nom de réseau', 'Plage IP', 'Notes', and 'Activé'. A blue button with a white plus sign and the text '+ Ajouter' is located at the end of the table header.

Après avoir cliqué sur le bouton, le formulaire de configuration d'une nouvelle plage réseau va apparaître dans un popup.

Pour créer une plage réseau, vous devez définir les paramètres suivants :

- **Nom**
- **Plage IP** : Plage(s) d'adresses à scanner dans le format accepté par la commande nmap.

Exemples

- 172.16.1.1-254
- 172.16.0.0/24
- 172.16.0.0/24 192.168.1.10-100

- **Plage de ports** : Plage de ports scannés pour chaque adresse. Les 1000 ports les plus répandus sont utilisés par défaut.
 - Vous pouvez restreindre le nombre de ports scannés avec une liste.
 - Cette liste peut comporter plusieurs plages en les séparant par des virgules.
 - *Ex* : **1-1024,2000-8000**
- **Notes** : Texte descriptif au sujet de cette plage réseau
- **Activé** : Activer ou désactiver les scans sur cette plage réseau pour les prochaines exécutions de la source.

Sources > Collecteur > discovery > Plage réseau [demo] ✕

✓ Sauvegarder

← Retour

✕ Supprimer

Légende

* (étoile) : Propriété obligatoire

Violet : Valeur héritée [nom de modèle]

Aide

Passer au-dessus d'une propriété pour voir l'aide associée.

Propriété	Valeur
Nom *	demo
Plage IP *	192.168.1.45
Plage de ports	Par défaut [Les 1000 ports les plus communs définis dans le fichier nmap-services de votre OS.]
Notes	Démonstration ?
Activé	<input checked="" type="checkbox"/> Vrai <input type="checkbox"/> Faux
Options supplémentaires	

Après la sauvegarde, vous aurez la plage réseau disponible dans l'interface

Sources > Collecteur > discovery Prêt à être importé ▶

Configuration
Règles de découvertes
Liste des plages réseau définies [1/1]
Résumé des dernières exécutions
Détail du dernier lancement

Nom de réseau	Plage IP	Notes	Activé	+ Ajouter
demo *	192.168.1.20-30	Démonstration	<input checked="" type="checkbox"/> Activé	

Étape 2 : Lancer un scan

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.

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 ▶

6

Activé

discovery

Non configurée

Dans 4 min

▶

0

Aucune plage de scan active n'a été trouvée.

Il y a 21 se

Une fois la ou les plages réseau définies, vous pourrez réaliser un scan en utilisant le bouton en haute à droite (*le bouton play*)

Sources > Collecteur > discovery Prêt à être importé Forcer l'import

Configuration Règles de découvertes **Liste des plages réseau définies [1/1]** Résumé des dernières exécutions Détail de la dernière exécution [1]

Nom de réseau	Plage IP	Notes	Activé	+ Ajouter
Démonstration	172.16.0.7		<input checked="" type="checkbox"/> Activé	

Le collecteur va scanner l'ensemble des plages réseau **activées** dans votre configuration.

Étape 3 : Les équipements trouvés

Dans l'onglet "*Détail de dernier lancement*" est listé chaque équipement détecté par le collecteur discovery en fonction des plages réseau actives lors de l'import.

Pour chaque équipement, l'œil à droite vous permet de voir le détail de l'opération.

Deux tableaux fournissent respectivement:

- Les **informations collectées par nmap**
 - Toutes les informations présentes dans ce tableau peuvent être utilisées dans les conditions d'une règle.
- **L'Hôte proposé** au Synchronizer:
 - Le collecteur va utiliser certaines données collectées pour les mettre au format du Synchronizer (*Clé / Valeur*).
 - Il peut suivant son paramétrage (des règles par défaut ou définies par l'utilisateur) modifier les valeurs. Cela sera alors mentionné dans la colonne "*Informations supplémentaires*" la règle utilisée.

Configuration Règles de découvertes Liste des plages réseau définies [3/3] Résumé des dernières exécutions **Détail du dernier lancement [6]**

Statut	Classe	Nom	Clés de synchronisation	Déplier
-- Tous --	-- Tous --	Pas de filtre	Pas de filtre	
OK	Hôtes	VM7	172.16.0.7, 172.16.0.7	

Informations collectées par NMAP

Clé	Valeur
fqdn	Aucune donnée remontée
mac	08:00:27:7A:E6:4A
macvendor	Oracle VirtualBox virtual NIC
openports	22,80,123,443,2003,2004,7002,7777,50000
os	Linux
ostype	general purpose
osvendor	Linux
osversion	3.X

Élément importé

Clé	Valeur	Informations supplémentaires
_MAC_ADDRESS	08:00:27:7A:E6:4A	
_SYNC_KEYS	[u'VM7', u'172.16.0.7']	
address	172.16.0.7	
host_name	VM7	
import_date	16/05/2019 13:35	
imported_from	discovery	
source	discovery	
use	http,https,linux,ssh	Modifié par les règles : Http, Https, linux, ssh