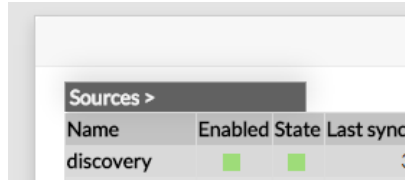


Shinken Enterprise vous permet de détecter des checks réseau et des serveurs physiques dans votre infrastructure.

Editer et ajouter une liste de scan réseau

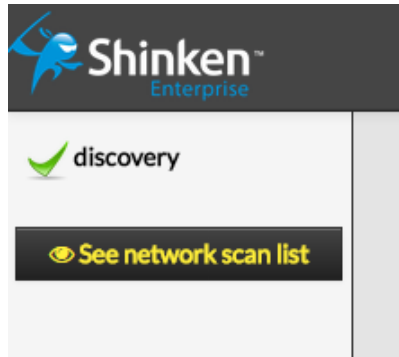
Le scan réseau peut être défini dans le [Administration Interface](#).

Commencez par cliquer sur la source "discovery" dans la page principale .

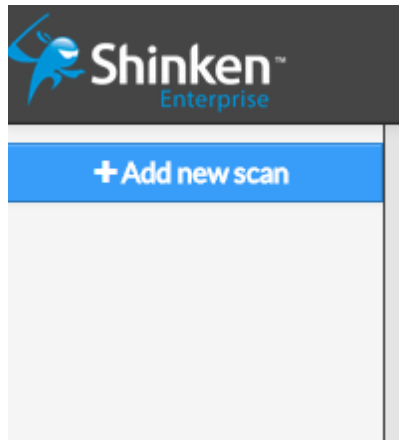


Sources >			
Name	Enabled	State	Last sync
discovery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Puis cliquer sur "voir la liste des scan réseau"



Vous pouvez activer un nouveau scan avec le bouton **Ajouter un nouveau scan** .



ET vous verrez la configuration d'un nouveau scan

Generic

Name

IP Range

Scan Interval (min) 60

Notes

Enabled On Off

Vous devez définir les paramètres suivants:

- Nom
- IP range: doit correspondre à la définition de la commande *nmap*

Par exemple: 172.16.1.1-254

- intervalle de scan en minutes
- vous pouvez rajouter des notes au sujet de ce scan

Ajouter un nouveau scan va le rendre automatiquement actif et vous verrez très rapidement apparaître de nouveaux éléments.

Ajouter un nouveau port dans une règle de host template

Sans règles, les données générées par la découverte sont sans intérêt. Les règles sont définies dans le fichier the **/etc/shinken/discovery_rules.cfg**

Voici un exemple de comment définir le ftp host template pour tout ce qui est détecté par nmap avec le port TCP/21 ouvert:

Il y a 3 parties principales dans la règle:

- **discoveryrule_name**: doit être unique
- **creation_type**: doit être un hôte
- **openports**: regexp au sujet du port qui correspondra. Le **^** et **\$** est pour le regexp, Donc **21** et seulement **21** correspondre, et pas **210** par exemple.
- **+use**: template dont sera hérité l'objet. Vous pouvez ajouter autant de propriétés que souhaité. .

```
define discoveryrule {
    discoveryrule_name    FtpRule
    creation_type         host
    openports             ^21$
    +use                  ftp
}
```

List des ports par défaut pour les règles de Host templates

Port	Host template
27017	<i>mongodb</i>
53	<i>dns</i>
25	<i>smtp</i>
465	<i>smtps</i>
3306	<i>mysql</i>
22	<i>ssh</i>
110	<i>pop3</i>
995	<i>pop3s</i>
9100	<i>printer-hp</i>
1521	<i>oracle</i>
80	<i>http</i>
443	<i>https</i>
1433	<i>mssql</i>
2301	<i>hp-asm</i>
143	<i>imap</i>
993	<i>imaps</i>
389	<i>ldap</i>
636	<i>ldaps</i>

Sécurité: paramètres de commande nmap

- -sU
- -sT
- --min-rate 1000
- --max-retries 3
- -T4
- -O