Collecteur Discovery (Découverte réseau)

Principe

Shinken Enterprise vous permet de détecter automatiquement des équipements réseau et des serveurs physiques dans votre infrastructure pour faciliter et accélerer leur import dans la configuration.

Configuration

Pour définir le module source Discovery:

1. Configurer la source dans le fichier **/etc/shinken/sources/discovery.cfg**
2. La source **Discovery** est déclarée dans le fichier **/etc/shinken/synchronizers/synchronizer-master.cfg**.

> **Note**
>
> Durant l'installation de Shinken Enterprise une source effectuant des découvertes réseau appelée ***discovery*** est créée.

sources/discovery.cfg

Propriété	Exemple	Description
source_name	discovery	Nom de la source. doit être unique
order	10	Ordre dans la consolidation de l'algorithme pour cette source . Voir dans la page Synchronizer page pour plus d'information
import_interval	5	Intervalle en minute de chargement de la source.
modules	discovery-import	module à lancer
enabled	0	1 - Activer la source 0 - Vue dans l'interface, mais ne collecte pas de données.
data_backend	mongodb	Backend où les données de la source est stockée **(non modifiable)**
mongodb_url	mongodb://localhost/?safe=false	URL d'accès à MongoDB **(non modifiable)**
mongodb_database	synchronizer	Base Mongo où sont stockées les données de la source **(non modifiable)**

> **Note**
>
> La colonne **Exemple** montre la valeur utilisée par le module si l'administrateur ne le saisit pas .

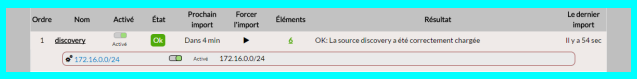
Exemple de définition:

```
define source {
    source_name             discovery
    order                   10
    import_interval         5
    module_type             discovery-import
    data_backend            mongodb
    mongodb_uri             mongodb://localhost/?safe=false
    mongodb_database        synchronizer
}
```

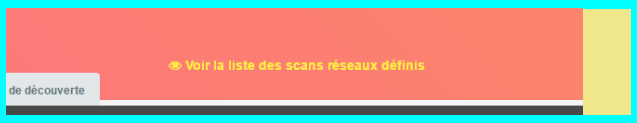
Editer et ajouter une liste de scan réseau

Le scan réseau peut être défini dans la Page Principale

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

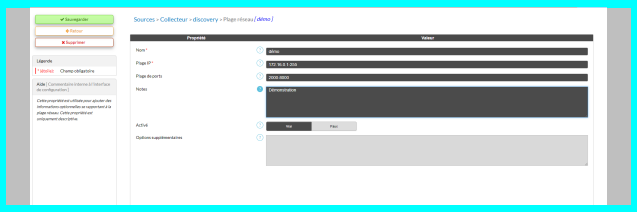


Puis cliquez sur "voir la liste des scan réseau"



Vous pouvez activer un nouveau scan avec le bouton "+ Ajouter".

Puis vous verrez la page de configuration d'un nouveau scan.



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

- Vous pouvez également ajouter 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

Sans règles, les données générées par la découverte sont sans intérêt. Les règles sont définies dans le fichier /etc/shinken/discovery_rules.cfg
Voici un exemple de comment ajouter le modèle d'hôte "ftp" 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 : host

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

- **openports**: regexp au sujet du port qui correspondra .Le ^ et $ font partie de la syntaxe de la regexp, et permettent de garantir que le port 21 sera pris en compte, et pas d'autres ports contenant "21" (comme 210).
- **+use**: les modèles d'hôte qui seront ajoutés à l'objet. Vous pouvez ajouter autant de modèles que souhaité.

Liste des ports par défaut pour les règles de modèles d'hôtes

Selon les ports ouverts détectés suite aux différents scans, des modèles d'hôtes seront ajoutés automatiquement aux machines détectées.

Les ports par défaut ainsi que leur modèles associés sont les suivants:

Port	Modèle d'hôte appliqué
27017	*mongodb*
53	*dns*
25	*smtp*
465	*smtps*
3306	*mysql*
22	ssh
110	pop3
995	pop3s
9100	printer-hp
1521	oracle
80	http
443	https
1433	mssql
2301	hp-asm
143	imap
993	imaps
389	ldap
636	ldaps

Sécurité: paramètres de la commande nmap

La commande nmap lancée par la source discovery utilise les paramètres suivants:

- **-PE** : Ping Scan (Echo Request)
- **-sU** : Scan UDP
- **-sT** : Scan TCP
- **--min-rate 1000** : Envoie un minimum de 1000 paquets par secondes
- **--max-retries 3** : Effectue au maximum 3 retransmissions en cas d'erreur sur les scan de ports
- **-T4** : Optimisation de performances
- **-O** : Detection des systèmes d'exploitation
- **-oX** : Export XML (utilisé pour l'interprétation de données par Shinken)

Précisions techniques

Clés de synchronisation

Les clés de synchronisation sont des propriétés des objets utilisées pour les identifier dans les sources. Le fonctionnement et l'utilité des clés de synchronisation sont décrits de manière plus détaillée dans la page de documentation dédiée: Précision techniques sur le fonctionnement de l'import des sources.

Les informations suivantes de la découverte réseau sont ajoutées en tant que clés de synchronisation de l'objet dans Shinken:

- host_name
- address