V2 - (READ) /api/v2/hosts

Principe

Shinken Enterprise vous permet de détecter automatiquement des équipements réseau et des serveurs physiques dans votre infrastructure pour faciliter et accélérer leur import dans la configuration. Il vous permet aussi de créer des règles basées sur les retours nmap qui appliqueront des modifications spécifiques sur vos équipements découverts.

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 **(non modifiable pour le moment)**
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)**
rules_path	/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/discovery_rules.json	Fichier json comportant vos règles de découvertes (voir règles de découvertes)
nmap_mac_prefixes_path	/etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-mac-prefixes	Fichier comportant vos propres nmap-mac-prefixes (voir nmap)

> **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

    rules_path /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/discovery_rules.json
    nmap_mac_prefixes_path /etc/shinken-user/configuration/daemons/synchronizers/sources/discovery/nmap/nmap-
mac-prefixes
}
```

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 .

? Unknown Attachment

Puis cliquez sur "Listes des plages réseaux définies"

? Unknown Attachment

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

? Unknown Attachment

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

? Unknown Attachment

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.

Les règles de découvertes

Sans règles, les données générées par la découverte sont vides. Elles comportent simplement les adresses des éléments découverts. Les règles sont définies par défaut dans le fichier /etc/shinken-user /configuration/daemons/synchronizers/sources/discovery/discovery_rules.json et doivent être au format json.

Voici un exemple qui est disponible par défaut dans Shinken:

Il y a 4 parties principales dans une règle:

- **name**: le nom et l'id de votre règle (**doit être unique**)
- **condition[1-9]**: représente une condition qui appliquera la règle si elle est respectée (**il suffit qu'une seule condition soit bonne pour que la règle soit appliquée**)
- **prefix_name**: ce préfixe sera ajouté au nom des éléments pour lesquels la règle s'applique (**opti onnel**)
- **use**: Les modèles d'hôtes qui seront ajoutés en cas d'application de règles. Vous pouvez en mettre autant que vous voulez en les séparant d'une virgule.

```
{
        "rules":[
                        {

"name": "myRuleExample",

"condition1": "os=myOS AND
osversion=^2",

"condition2":
"osversion=^2.6.0$",

"condition3":
"macvendor=^myMacVendor",

"condition4":
"ostype=myType$",

"condition5":
"openports=1|2",

"prefix_name":
"myRulePrefix",

"use": "myTemplate,
myTemplate2"
                        }
        ]
}
```

Il peut y avoir plusieurs problèmes au niveau de vos règles et donc plusieurs comportements:

Problèmes	Résultat
Votre fichier n'est pas au format json	Le fichier n'est pas lu et une erreur apparaît
Votre fichier est introuvable	Le fichier n'est pas lu et une erreur apparaît
Votre fichier comporte des clés inconnues	Le fichier n'est pas lu et une erreur apparaît
Votre fichier est vide	Le fichier n'est pas lu mais aucune erreur n'apparaît
Il manque une clé obligatoire dans une de vos règles	Le fichier est lu mais la règle sera désactivée
Une erreur se trouve dans vos conditions	Le fichier est lu mais la règle sera invalide
Une de vos règles est dupliquée	Le fichier est lu, seule la première itération de la règle sera prise en compte, mais le statut de la règle sera en avertissement

Onglet de règles

Un onglet listant les règles de découvertes par défaut et celles de l'utilisateur est disponible dans la page de la discovery.

Si le fichier de règles est correctement chargé

? Unknown Attachment

Il existe 6 statuts pour les règles de découvertes :

Cas	Statut
La règle est en un seul exemplaire dans votre fichier	Définir par l'utilisateur
Le nom de la règle existe déjà quand le fichier par défaut	Surchargé par l'utilisateur
Le nom de la règle est défini plusieurs fois dans le fichier utilisateur	Défini plusieurs fois
La règle comporte une erreur	Invalide
La règle ne comporte pas de conditions ou de modèles d'hôtes	Désactivé

Vous pouvez rafraîchir la liste des règles directement en appuyant sur le bouton de refresh en haut à droite, ou en appuyant sur F5.

Si le fichier de règles n'est pas correctement chargé

? Unknown Attachment

Dans le cas où le fichier de règles n'est pas correctement chargé (voir les problèmes liés aux règles dans les règles de découvertes), seules les règles par défaut sont prises en compte et un message d'erreur apparaît en haut du tableau.

Les conditions

Il existe plusieurs possibilités pour les conditions de vos règles :

Commence par (=^...)

Si l'expression commence par '^', la condition signifiera que le résultat attendu DOIT **commencer** par l'expression.

```
macvendor=^myMacVendor
```

Fini par (=...$)

Si l'expression finie par '$', la condition signifiera que le résultat attendu DOIT **finir** par l'expression.

```
ostype=myType$
```

Est égal (=^...$)

Si l'expression comment par '^' ET finie par '$', la condition signifiera que le résultat attendu DOIT **être** l'expression exacte.

```
osversion=^2.6.0$
```

Contient (=...)

Si l'expression ne contient aucun des paramètres précédents, la condition signifiera que le résultat attendu DOIT **contenir** l'expression

```
os=myOS
```

Condition ET condition (condition AND condition)

Si la condition contient un ou plusieurs AND, cela signifie que **tout** ce qui est dans cette condition doit être respecté pour que la règle soit appliquée.

```
os=myOS AND osversion=^2
```

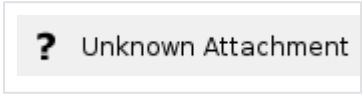
Cas spécifique des openports (X|X)

La condition openports est un cas spécifique. En terme de port on ne fait pas de contient, commence ou termine par. Il faut donc rentrer simplement le port exact. Si vous souhaitez faire un OU, il suffit de mettre un '|' entre les ports.

```
openports=1|2
```

Le résultat

Dans votre onglet de Détail de dernier lancement, vous aurez des indications sur les règles appliquées sur votre hôtes découverts. Si une valeur a été modifiée par une règle, vous saurez laquelle.



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

Les préfixes nmap

Lors du scan nmap effectué par la discovery, nmap utilise un fichier nommé nmap-mac-prefixes qui comporte des adresses mac associés à des macvendor (ce qui sera récupéré par nmap).

Par exemple, si votre machine récupérée par la discovery a pour MAC-address : 0050BAXXXXX, sa mac-vendor sera D-Link.
Shinken fourni par défaut un fichier nmap-mac-prefixes qui sera la référence d'nmap. Il sera mis à jour à chaque update de Shinken.

Vous pouvez cependant créer un fichier nmap-mac-prefixes dans /etc/shinken-user/configuration /daemons/synchronizers/sources/discovery/nmap/ par défaut qui surchargera celui que shinken met à votre disposition.

Votre fichier doit être au format de l'exemple donné et peut contenir des commentaires en commençant la ligne par un #.

Le retour nmap

Vous pouvez dans l'onglet "Détail du dernier lancement" voir toutes les informations récupérées par nmap, après récupération de votre fichier nmap-mac-prefixes, au sujet des machines découvertes.

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