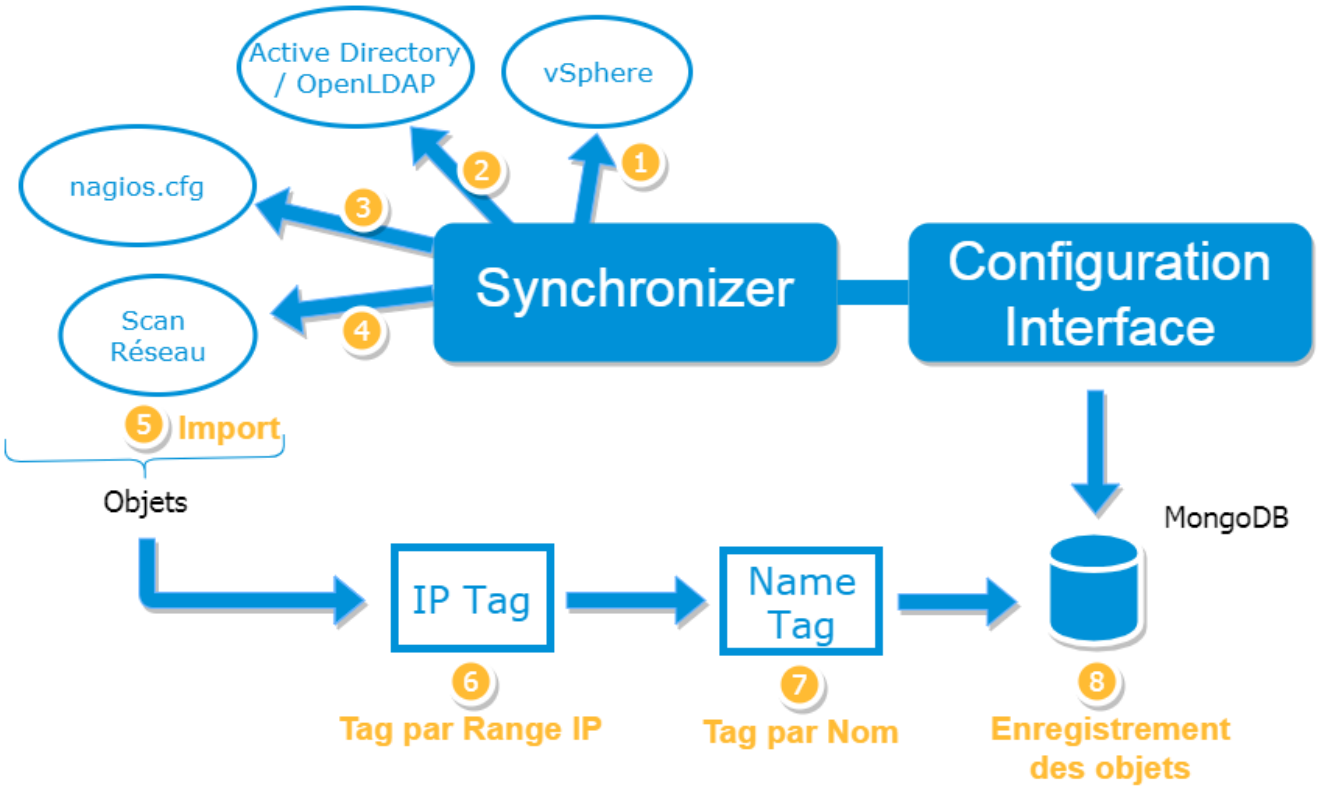
Le Synchronizer

Rôle

Le Synchronizer gère toute la configuration. Il utilise différentes sources pour détecter les nouveaux éléments ou les modifications sur les existants.

Il présente la configuration en interface web aux administrateurs. Voici les sources optionnelles que le démon peut utiliser :

- Active Directory / Open LDAP
- VSphere (VMWare)
- Fichiers de configuration Nagios ou Shinken framework
- Scans réseau



Active Directory / OpenLDAP

La découverte de l'Active Directory ou OpenLDAP se fait avec un compte domaine et ne nécessite qu'un accès en lecture. La connexion peut être faite dans LDAPS pour être sûr que la connexion est sécurisée.

Il est possible de définir un niveau haut d'organisation (OU = Organizational Unit) afin de lister les éléments seulement sous ce niveau.

Les informations que ce module récupère sont les noms de serveurs, FDQN, l'OS du serveur, et si il est défini, son entrée LDAP et son emplacement. La configuration pour la source Active Directory est située ici et OpenLDAP ici.

VSphere de VMWare

La découverte VSphere est faite pour trouver les serveurs physiques (ESX) et leurs serveurs virtuels. Elle va également récupérer leur OS et leur adresse IP, mais seulement si les outils VMware sont activés et tournent sur le serveur virtuel.

La connexion du Synchronizer vers VMware connexion se fait toujours via le serveur VSphere, et ne nécessite qu'un accès en lecture. Le serveur Shinken Enterprise ne nécessite pas un accès direct aux serveurs ESX.

La communication de Shinken Enterprise vers VSphere se fait via une API SOAP de VMWare, à travers une connexion HTTPS. La configuration pour cette source est située dans une autre page.

Fichiers de configuration Nagios ou Shinken Framework

Shinken Enterprise est capable de charger des fichiers de configuration Nagios ou Shinken Framework. Il va automatiquement charger les objets définis. La configuration pour cette source est située dans une autre page.

Scan réseau

La découverte via scan réseau est optionnelle. Elle se fait via une commande nmap, lancée par le Synchronizer.

Les scans sont faits sur les ports TCP et UDP. Il va également essayer de récupérer des données complémentaires depuis les serveurs ou les services qui tournent dessus (il utilise l'option -O dans la commande nmap). La configuration pour cette source est située dans une autre page.

Stockage de données dans la configuration

Toutes les données découvertes par le Synchronizer sont stockées dans une base Mongodb. Si possible, il est préférable que la base soit sur le même serveur que le Synchronizer ; elle n'est pas partagée avec d'autres démons, donc ses communications doivent être limitées au serveur local.

Configuration de l'interface et de ses accès

L'interface de configuration est stockée par le Synchronizer, et utilise un autre port TCP pour l'UI de visualisation. Vous pouvez utiliser 2 systèmes d' accréditation:

- gestion directe dans l'interface de configuration
- gestion des droits avec les comptes Active directory ou OpenLDAP. Le démon va alors utiliser les connexions LDAP pour vérifier les autorisations. La procédure est ici.

Les utilisateurs non-admin auront une visibilité restreinte sur les hôtes auxquels ils sont attachés directement, ou au groupe auquel ils sont rattachés.

Cette interface utilise la même base Mongodb que le Synchronizer. Le port par défaut est le 7766.

Interface	Démon	Port
Configuration	Synchronizer	7766

Plus d'information sur le paramétrage de l'interface de configuration ici.

Résumé des connexions du Synchonizer

Source	Destination	Port	Protocole	Note
Arbiter	Synchronizer	7765	HTTP/HTTPS	
Synchronizer	Synchronizer	27017	TCP/IP	Accès à la base Mongo

Connexions possibles liées aux différentes sources :

Source	Connexion à	Port	Protocole	Note
Synchronizer	Active Directory ou OpenLDAP	389	LDAP	
Synchronizer	Active Directory ou OpenLDAP	636	LDAPS	Accès en lecture seule
Synchronizer	VSphere	443	HTTPS	Accès en lecture seule
Synchronizer	Scan Réseau	x	TCP/IP	

Descriptions des variables

Property	Default	Description
synchronizer_name	N/A	Cette variable est utilisée pour identifier le nom court du Synchronizer auquel les données sont attachées.
address	N/A	Cette directive est utilisée pour définir l'adresse permettant à ce que l'Arbiter joigne ce Synchronizer. Par défaut "localhost", changez le par un nom DNS ou une adresse IP.
port	7765	Cette directive est utilisée pour définir le port TCP utilisé par le démon.
spare	0	Cette variable est utilisée pour définir si le Synchronizer doit être géré en tant que spare (chargera la configuration seulement si le master est en erreur). La valeur par défaut est **0** (master).
modules	N/A	Cette variable est utilisée pour définir tous les modules que le synchronizer va charger.
use_ssl	0	Cette variable est utilisée pour définir si le Synchronizer doit être contacté en HTTPS (*1*) ou HTTP (*0*). La valeur par défaut est *0* (HTTP).
sources	N/A	Liste des sources que le synchronizer va charger.
taggers	N/A	Liste des taggers que le synchronizer va charger.
enabled	N/A	Cette variable est utilisée pour définir si le Synchronizer est activé ou non.

Exemple de définition d'un synchronizer

```
#================================================================================
# SYNCHRONIZER
#================================================================================
# Description: The Synchronizer is responsible for:
# - Hosting the Configuration UI
#================================================================================
define synchronizer {

    synchronizer_name    synchronizer-master
    #host_name       node1       ; CHANGE THIS if you have several Arbiters
    address         node1.mydomain   ; DNS name or IP
    port            7765
    spare           0           ; 1 = is a spare, 0 = is not a spare

    modules      Cfg_password

    use_ssl          0

    ## Uncomment these lines in a HA architecture so the master and slaves know
    ## how long they may wait for each other.
    #timeout              3   ; Ping timeout
    #data_timeout         120 ; Data send timeout
    #max_check_attempts   3   ; If ping fails N or more, then the node is dead
    #check_interval       60  ; Ping node every N seconds

    sources              syncui,cfg-file-shinken,active-dir-example,sync-vmware,cfg-file-nagios,discovery,
openldap-example
    taggers              ip-tags,regexp-tags


    enabled    1 ;   If you set enabled 0, Don't forget to disable daemon on distant host
}
```