# Source OpenLDAP

## Vue d'ensemble

Ce document décrit comment vous pouvez importer des hôtes et des utilisateurs depuis OpenLDAP.

**Après avoir pris soin de lire notre page sur la Définition et ordre des sources, certaines étapes sont nécessaires afin de pouvoir importer des hôtes et des utilisateurs depuis un annuaire OpenLDAP :**

- Personnaliser la source OpenLDAP (à partir de la source d'exemple)
- Configurer les 3 fichiers pour :
  - la connection à OpenLDAP pour les extractions de données
  - le "mapping" pour la correspondance entre les champs de l'annuaire OpenLDAP et ceux de Shinken
  - les règles de configuration pour appliquer des filtres si besoin et réaliser des actions

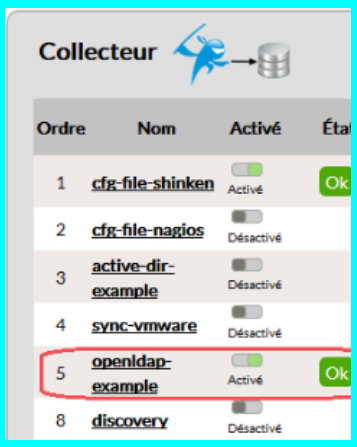
**Sommaire**



## Personnaliser la source pré-installée

Le script d'installation et de mise à jour de Shinken permet de mettre en place une source Active Directory déjà configurée.

Vous pouvez la voir sur la page d'accueil de l'UI de Configuration, dans le tableau des sources.




Cette source utilise 2 sortes de fichiers de configuration :

- **Le fichier de définition de source OpenLDAP**
  - Pour OpenLDAP, le fichier en place pour l'exemple est /etc/shinken/sources/openldap.cfg
- **Les 3 fichiers de configuration de la source afin de personnaliser les extractions de données**
  - Disponible dans le répertoire /etc/shinken-user/source-data/source-data-openldap-sample/_configuration :
    - connection_configuration_file,
    - mapping_configuration_file
    - rules_configuration_file

Vous pouvez directement utiliser cette source "openldap-example" en modifiant uniquement les fichiers de configuration pour extractions de vos données OpenLDAP (pour un test rapide par exemple). Cependant, nous vous conseillons de dupliquer la source "example" en suivant l'astuce ci-dessous.

Pour personnaliser votre source (et donc modifier le terme "example"), **copiez votre répertoire de configuration de la source** (*source-data-openldap-sample* vers *source-data-openldap-monServeurOpenLDAP* par exemple) et modifiez votre définition de source (le nom de votre source et les chemins à vos 3 fichiers de configuration).

Bien entendu, votre Synchronizer devra appeler ce nouveau nom de source, modifiez donc également le fichier de configuration du Shinken Synchronizer.

### Définition de la source

Le fichier préalablement créé pour la source OpenLDAP  exemple est : /etc/shinken/sources/openldap.cfg. (de la même manière qu'avec le répertoir de configuration, vous pouvez dupliquer ce fichier et effectuer les modifications afin de personnaliser votre source)

C'est ici que vous pouvez changer le nom de votre source via la propriété **source_name**

Une source OpenLDAP est caractérisée par son module_type qui doit être : **ldap-import**

**Pour les autres valeurs, merci de vous référer à la Définition et ordre des sources.**

## Configuration de la connexion

Les fichiers suivants sont utilisés pour effectuer la connexion à votre serveur Active Directory (le chemin peut varier si vous avez personnalisé votre répertoire) :

| Property | Value | Description |
|---|---|---|
| connection_configuration_file | /etc/shinken-user/source-data/source-data-openldap-*sample*/_configuration/openldap-connection.json | ***Connexion LDAP***<br><br>Information de connexion à l'annuaire LDAP.<br>Ce fichier est à modifier obligatoirement |
| mapping_configuration_file | /etc/shinken-user/source-data/source-data-openldap-*sample*/_configuration/openldap-mapping.json | ***Règles de mapping***<br>Le mapping d'attributs peut être différent d'un annuaire OpenLDAP à l'autre.<br>Par exemple, vous pouvez spécifier dans ce fichier quel serait le nom d'attribut du numéro de téléphone des utilisateurs.<br>Ce fichier peut être utilisé tel quel |
| rules_configuration_file | /etc/shinken-user/source-data/source-data-openldap-*sample*/_configuration/openldap-rules.json | ***Règles de configuration***<br>Vous pouvez choisir quelles sortes d'hôtes et d'utilisateurs seront récupérés et permet également la définition de critères afin d'appliquer automatiquement des modèles.<br>Ce fichier est à modifier obligatoirement |
| | | |

Veuillez donc tout d'abord modifier le fichier **openldap-connection.json :**

| Propriété | Défaut | Description |
|---|---|---|
| url | ldap://YOUR-DC-FQDN/ | Adresse de votre serveur OpenLDAP |
| ldap_protocol | 3 | Version du protocole LDAP (par défaut à 3 si pas spécifié) |
| base | dc=YOUR,dc=DOMAIN,dc=com | OU (Organisation Unit) base pour la découverte de vos objets |
| hosts_base | OU=DataCenter Servers,dc=YOUR,dc=DOMAIN,dc=com | OU (Organisation Unit) base pour la découverte de vos hôtes |
| hostgroups_base | OU=computers,dc=shinkendom,dc=local | OU (Organisation Unit) base pour la découverte de vos groupes d'hôtes |
| contacts_base | dc=YOUR,dc=DOMAIN,dc=com | OU (Organisation Unit) base pour la découverte de vos contacts |
| username | SHINKEN@YOURDOMAIN.com | Utilisateur utilisé pour la connexion au serveur OpenLDAP |
| password | PASSWORD | Mot de passe utilisé pour la connexion au serveur OpenLDAP |

**Note Importante**

Si vous n'avez pas de distinction de type entre les objets que vous souhaitez importer depuis votre anuaire OpenLDAP (hôtes, groupes d'hôtes ou utilisateurs), veuillez mettre les mêmes chemins OpenLDAP pour les 3 types. Il en est de même si vous souhaitez importer une OU qui ne contient qu'un seul type d'objet, veuillez spécifier ce chemin d'OU pour les 3 propriétés (hosts_base, hostgroups_base et contacts_base). **Ne supprimez pas ces propriétés, elles sont obligatoires.**

Un moyen de ne pas importer des objets sera de placer des filtres via le fichier mapping_configuration_file et rules_configuration_file (voir plus bas).

Exemple :

**/etc/shinken-user/source-data/source-data-active-directory-sample/_configuration/openldap-connection.json**

```
{
  "url": "ldap://vm-w2k8r2.shinkendom.local/",
  "ldap_protocol":3,
  "base": "dc=shinkendom,dc=local",
  "hosts_base": "OU=serveurs,dc=shinkendom,dc=local",
  "hostgroups_base": "OU=serveurs,dc=shinkendom,dc=local",
  "contacts_base": " OU=utilisateurs,DC=shinkendom,DC=local",
  "username": "administrateur@shinkendom.local",
  "password": "P@ssword1"
}
```

**Tip**

Le compte utilisé pour envoyer des requêtes LDAP au serveur n'a besoin que d'un accès en "lecture seule". Vous devriez créer un compte de service OpenLDAP dédié à cet accès Shinken.

## Configuration des règles de "mapping"

Ce fichier vous permet d'effectuer une correspondance entre des propriétés OpenLDAP et Shinken. Les propriétés **host.filter** et **contact.filter** peuvent permettre de ne pas importer des types d'objets particuliers. (voir l'astuce plus bas)

**Si besoin (facultatif),** modifiez le fichier **openldap-mapping.json**

| Propriété Shinken | Propriété Active Directory | Description |
|---|---|---|
| host.name | name | La propriété OpenLDAP name, représentant le nom de l'objet OpenLDAP, sera importé et utilisé pour le nom de l'hôte Shinken |
| host.dNsHost | dNSHostName | La propriété OpenLDAP dNSHostName, représentant le nom DNS de l'objet OpenLDAP, sera importé et utilisé pour l'adresse de l'hôte Shinken |
| host. operatingSystem | operatingSystem | |
| host. operatingSystem ServicePack | operatingSystemService Pack | |
| host. distinguishedName | distinguishedName | |
| host.filter | (objectClass=computer) | Cette propriété permet le filtre des ordinateurs / hôtes seulement |
| contact.name | name | La propriété OpenLDAP name, représentant le nom de l'objet OpenLDAP, sera importé et utilisé pour le nom du contact Shinken |
| contact.mail | mail | La propriété OpenLDAP mail, représentant l'email de l'objet OpenLDAP, sera importé et utilisé pour l'email du contact Shinken |
| contact. displayName | name | La propriété OpenLDAP name, représentant le nom de l'objet OpenLDAP, sera importé et utilisé pour le nom d'affichage du contact Shinken |
| contact. categoryFilter | Person | |
| contact.member | member | |

| | | |
|---|---|---|
| contact.telephoneNumber | telephoneNumber | La propriété OpenLDAP telephoneNumber, représentant le numéro de téléphone de l'objet OpenLDAP, sera importé et utilisé pour le numéro de téléphone du contact Shinken |
| contact.mobile | mobile | |
| contact.co | co | |
| contact.l | l | |
| contact.company | company | |
| contact.filter | (&(objectCategory=person)(objectClass=user)) | Cette propriété permet le filtre des contacts seulement |
| hostgroup.filter | | |

**Astuce**

Si vous ne souhaitez pas importer d'objets OpenLDAP "computer" et donc de ne pas créer d'hôtes en "nouveau" dans Shinken, vous pouvez définir la propriété **host.filter** à : **(objectClass=)**
Si vous ne souhaitez pas importer d'objets OpenLDAP "contact" et donc de ne pas créer d'utilisateurs en "nouveau" dans Shinken, vous pouvez définir la propriété **contact.filter** à : **(&(objectCategory=person)(objectClass=)**

**/etc/shinken-user/source-data/source-data-active-directory-sample/_configuration/openldap-mapping.json**

```
# IMPORTANT: Do not edit this file.
# To have your own mapping, copy it under the /etc/shinken-users/source-data/YOUR_SOURCE_FOLDER
/_configuration/ directory and edit your copy instead.
# Note: comments should be with a # starting the line, NOT after a value
{
# first hosts propertyes (computer object in Active Directory)
   "host.name": "name",
   "host.dNSHostName": "dNSHostName",
   "host.operatingSystem": "operatingSystem",
   "host.operatingSystemServicePack":"operatingSystemServicePack",
   "host.distinguishedName": "distinguishedName",
   "host.filter": "(objectClass=computer)",

# Now contact properties
    "contact.name": "name",
    "contact.mail": "mail",
    "contact.displayName":"name",
    "contact.categoryFilter":"Person",
    "contact.member": "member",
    "contact.telephoneNumber":"telephoneNumber",
    "contact.mobile":"mobile",
# Co: for country
    "contact.co":"co",
# l: for city
    "contact.l":"l",
    "contact.company":"company",
    "contact.filter":"(&(objectCategory=person)(objectClass=user))",
# By default hostgroup are not requested. Setup a filter in your custom file to enabled it
    "hostgroup.filter":""

}
```

## Règles de configuration

Ce fichier est utilisé pour appliquer des **modèles d'hôtes** et des **modèles d'utilisateurs** sur les hôtes et utilisateurs durant l'import, provenant d'OU ciblées.
Ce fichier permet également de filtrer les utilisateurs à importer dans Shinken en se basant sur les membres d'un ou de plusieurs groupes d'utilisateurs de l'annuaire OpenLDAP ciblé.

Veuillez donc enfin modifier le fichier **openldap-rules.json**
**Attention la modification de ce fichier est obligatoire car certaines propriétés contenant des chemins OpenLDAP ne permettront pas un import valide si elles ne sont pas modifiées.**

**Tip**

Le modèle d'hôte **windows** est déjà disponible dans Shinken, ce modèle vérifie : l'utilisation Cpu, les Disques, les journaux d'évènements Application, les journaux d'évènements Système, la mémoire, l'interface réseau, le uptime, les services, les fichiers de paginations.

Pour un bon début, vous pouvez configurer la propriété **hosts_tag** de cette manière :

| | |
|---|---|
| hosts_tag | windows |

Pour que les fonctionnalités offertes par la propriété **memberOf**, décrites ci-dessous, fonctionnent sous OpenLDAP, il est nécessaire d'installer et de configurer l'Overlay **memberOf** dans le serveur.

| Property | Default | Description |
|---|---|---|
| hosts_tag | your-host-template | Le modèle d'hôte **your-host-template** sera appliqué à tous les hôtes découverts dans l'annuaire Active Directory |
| hosts_tag_**monmodele** | OU=Database Servers,OU=DataCenter Servers,DC=YOUR,dc=DOMAIN,dc=com | Le modèle d'hôte **montemplate** (ce nom est à modifier) sera appliquée aux hôtes découverts dans cette OU de l'annuaire Active Directory |
| AddFirst_template_(**windows**)_to_host_matching_[operatingSystem] | windows.* | Ajouter le modèle d'hôte **windows** (à modifier si besoin) à tous les hôtes ayant une valeur commencant par "windows" dans son attribut **operatingSystem** - premier à être appliquer (avant la règle de hosts_tag ). |
| AddLast_template_(**sp1**)_to_host_matching_[operatingSystemServicePack] | Service Pack 1 | Ajouter le modèle d'hôte **sp1** (à modifier si besoin) à tous les hôtes ayant une valeur égale à "Service Pack 1" dans son attribut **operatingSystemServicePack** - dernier à être appliquer (après la règle de hosts_tag ). |
| contacts_tag | generic-contact | Le modèle de contact **generic-contact** sera appliqué à tous les contacts découverts dans l'annuaire OpenLDAP |
| contacts_group_filter | CN=Domain Admins,CN=Users,DC=YOUR,dc=DOMAIN,dc=com \| CN=OTHERGROUPS,OU=Groups,OU=Users Groups,DC=YOUR,dc=DOMAIN,dc=com | Les contacts importés depuis la base OpenLDAP "contacts_base" seront filtrés avec ceux présents dans le Groupe d'utilisateur (CN) spécifié. Vous pouvez définir plusieurs groupes en séparant les filtres avec le caractère pipe \| |
| AddFirst_template_(**domain-admins**)_to_contact_matching_[memberOf] | CN=Domain Admins,CN=Users,DC=YOUR,dc=DOMAIN,dc=com | Ajouter le modèle de contact **domain-admins** à tous les contacts ayant la valeur "CN=Domain Admins,CN=Users,DC=YOUR,dc=DOMAIN,dc=com" dans son attribut "**memberOf**" - premier à être appliquer (avant la règle de contacts_tag ). |
| AddLast_template_(**users**)_to_contact_matching_[memberOf] | CN=Users,DC=YOUR,dc=DOMAIN,dc=com | Ajouter le modèle de contact **users** à tous les contacts ayant la valeur "CN=Users,DC=YOUR,dc=DOMAIN,dc=com" dans son attribut "**memberOf**" - dernier à être appliquer (après la règle de contacts_tag ). |
| Force_template_(**specific**)_to_contact_matching_[memberOf] | CN=SpecificUsers,DC=YOUR,dc=DOMAIN,dc=com | Ajouter le modèle de contact "**specific**" à tous les contacts ayant la valeur "CN=SpecificUsers,DC=YOUR,dc=DOMAIN,dc=com" dans son attribut "**memberOf**" - seul à être appliquer (la règle de contacts_tag ne sera pas appliquée). |

Exemple :

**/etc/shinken-user/source-data/source-data-active-directory-sample/_configuration/openldap-rules.json**

```
{
  "hosts_tag": "windows",
  "hosts_tag_citrix": "OU=citrix,OU=serveurs,dc=shinken,dc=local",
  "hosts_tag_database": "OU=database,OU=serveurs,dc=shinken,dc=local",
  "hosts_tag_exchange": "OU=exchange,OU=serveurs,dc=shinken,dc=local",
  "hosts_tag_fileprint": "OU=fileprint,OU=serveurs,dc=shinken,dc=local",
  "hosts_tag_windows": "OU=infra,OU=serveurs,dc=shinken,dc=local",

  "contacts_tag": "generic-contact",
  "contacts_group_filter": "CN=paris_shinken_users,OU=utilisateurs,DC=shinkendom,DC=local |
CN=bordeaux_shinken_users,OU=utilisateurs,DC=shinkendom,DC=local",
  "AddFirst_template_(domain-admins)_to_contact_matching_[memberOf]": "CN=Domain Admins,CN=Users,DC=YOUR,
dc=DOMAIN,dc=com",
  "AddLast_template_(users)_to_contact_matching_[memberOf]": "CN=Users,DC=YOUR,dc=DOMAIN,dc=com",
  "Force_template_(specific)_to_contact_matching_[memberOf]": "CN=SpecificUsers,DC=YOUR,dc=DOMAIN,dc=com"
}
```

Attention, les 4 dernières propriétés **contacts_group_filter**, **AddFirst_template_(domain-admins)_to_contact_matching_[memberOf]**, **AddLast template_(users)_to_contact_matching_[memberOf]** et **Force_template_(specific)_to_contact_matching_[memberOf]** doivent être adaptées à votre Annuaire OpenLDAP. Si vous ne souhaitez pas utiliser ces propriétés, veuillez les mettre à "aucune valeur" avec l'astuce suivante:

Si vous souhaitez ne pas utiliser ce filtre et donc importer tous les objets d'une OU peu importe leurs groupes, configurez le **contacts_group_filter à aucune valeur ("")**

Tous les objets dans **contacts_base** (fichier *active-directory-connection.json*) filtrés via le **contact.filter** (fichier *openldap-mapping.json*) seront importés.

Voici un exemple de fichier cfg du fichier openldap-rules.json simple, sans utilisation de filtre ou d'application automatique de modèle :

```
{
  "hosts_tag": "",

  "contacts_tag": "",
  "contacts_group_filter": "",
  "Force_template_(specific)_to_contact_matching_[memberOf]": ""
}
```

## Import des objets

Pour importer des objets, allez sur la page d'accueil de l'**UI de configuration**, si votre configuration est bonne, vous devriez avoir un message "**OK: Import clean**."

Maintenant, faîtes un "**Force import**" en cliquant sur 

Dans le panneau "**Elements >**" vous verrez les nouveaux éléments apparaître (Hôtes et Contacts).


La prochaine étape sera alors d'importer ces nouveaux éléments dans Shinken.

# HOW TO

## Importer des ordinateurs avec des noms spécifiques

Dans le fichier **openldap-mapping.json**

Modifiez le paramètre **host.filter**

```
  "host.filter": "(&(objectClass=computer)(sAMAccountName=*SERVER_NAME*))",
```

Changez **SERVER_NAME** par le nom de serveur vous voulez importer.

## Importer des utilisateurs issus d'un ou plusieurs groupes

Avec la source OpenLDAP, il est donc possible d'importer des utilisateurs de la base contacts_base spécifiée dans le fichier **openldap-connection.json** mais on peut aussi les filtrer afin de n'importer que ceux qui sont dans un ou plusieurs groupes différents de l'annuaire LDAP.

Dans le fichier **openldap-rules.json**

Dans **contact_group_filters,** ajouter le Distinguished Name (DN) des différents groupes d'utilisateurs séparés par un pipe ("|")

**/etc/shinken-user/source-data/source-data-active-directory-sample/_configuration/active-directory-rules.json**

```
  "contacts_group_filter": "CN=shinken_admins,OU=utilisateurs,DC=shinkendom,DC=local | CN=shinken_users,
OU=utilisateurs,DC=shinkendom,DC=local",
```

## Filtrer et appliquer des modèles

Cette source inclut également d'autres paramètres qui permettent d'appliquer des modèles automatiquement suivant le type d'objets :

- ***hosts_tag***: chaque hôte chargé aura au moins le modèle défini en valeur
- ***contacts_tag***: chaque contact chargé aura au moins le modèle défini en valeur

Il est également possible de tagguer les hôtes sur leur OU (Organization Unit) en utilisant le paramètre ***hosts_tag_**

Par exemple, si vous voulez ajouter le tag **exchange** à tous les serveurs qui sont dans l'OU: OU=Email Collaboration Servers,OU=DataCenter Servers,DC=YOUR,dc=DOMAIN,dc=com

Utilisez le paramètre:

```
"hosts_tag_exchange":  "OU=Email Collaboration Servers,OU=DataCenter Servers,DC=YOUR,dc=DOMAIN,dc=com"
```

Si vous voulez ajouter le tag **enterprise** à tous les objets ldap qui correspondent au string **Enterprise** dans leurs propriétés **operatingSystem,**

Utilisez le paramètre:

```
"hosts_match_operatingSystem_enterprise":        "Enterprise"
```

# 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 champs LDAP suivants sont ajoutés en tant que clés de synchronisation de l'objet dans Shinken:

- name
- dNSHostName
- ip
- fqdn