

# Module auth-active-directory pour la WebUI

## Sommaire

- [Description](#)
- [Activation du module](#)
- [Configuration](#)
  - [Exemple de fichier de configuration](#)
  - [Détails des sections composant le fichier de configuration](#)
    - [Identification du module](#)
    - [Connexion au serveur LDAP](#)
    - [Correspondances des attributs LDAP avec les propriétés ou données Shinken](#)
    - [Correspondance des champs entre LDAP et Shinken \( mapping.json \)](#)
      - [Liste des correspondances les plus utilisées](#)
- [Exemple de déclaration de l'utilisation du module dans configuration de l'interface de Visualisation](#)

## Description

Le module d'authentification LDAP permet aux utilisateurs de s'authentifier directement sur un serveur supportant le protocole LDAP ( *Lightweight Directory Access Protocol* ).

Pour pouvoir s'authentifier auprès d'un serveur LDAP, il faut que :

- Chaque utilisateur ait un compte Shinken et un compte sur le serveur LDAP
- Chaque utilisateur ait une correspondance unique entre une propriété ou une donnée Shinken et un attribut LDAP, par exemple l'adresse mail.
- Chaque utilisateur soit présent en base de production dans le Synchronizer

Afin de garantir qu'un utilisateur soit existant et que ses données soient bien renseignées, il est fortement conseillé d'importer les utilisateurs grâce à la source LDAP : [Collecteur de type ldap-import \( pour Active Directory \)](#) ou [Collecteur de type ldap-import \( pour Open LDAP \)](#)

Lors de l'authentification, le module utilise le compte LDAP renseigné lors de la configuration du module ( *voir plus bas* ) pour rechercher si l'utilisateur existe sur le serveur LDAP. Si c'est le cas, Shinken transmet la requête d'authentification au serveur LDAP et c'est celui-ci qui authentifie l'utilisateur.

Le module supporte le protocole LDAP. Il est donc compatible avec :

- Les serveurs Active Directory
- Les serveurs OpenLDAP
- Les serveurs supportant le protocole LDAP ( *Oracle DSEE , ...* )



Les serveurs OpenLDAP et Active Directory ne sont pas sensibles à la casse. Pour se conformer à eux, ce module d'authentification ne prend pas en compte la casse dans les identifiants de connexion lors de l'accès à l'Interface de visualisation.



### Avoir plusieurs modules d'authentifications

Vous pouvez définir et utiliser plusieurs modules d'authentification sur l'interface de Visualisation, ce qui est très pratique si vous avez un serveur LDAP primaire et des secondaires.

Pour chaque essai de connexion, les modules d'authentifications seront interrogés les uns à la suite des autres:

- Ceci permet par exemple de gérer l'indisponibilité du primaire.
- Le module suivant n'est interrogé que si le premier n'a pas répondu ou pas reconnu l'utilisateur.

## Activation du module

Le module `auth-active-directory` est un module qui peut être activé sur le module `webui` et le `Synchronizer`.

- L'activation du module s'effectue en ajoutant le nom de ce module dans le fichier de configuration du module `webui`.
- Pour ce faire, ouvrez le fichier de configuration du module `WebUI` du `Broker` à l'emplacement `/etc/shinken/module/ma_webui.cfg`, et ajoutez le nom de votre module `"auth-active-directory"`.

Exemple: par défaut, nous livrons un module dont le nom est "auth-active-directory":

```
define DEMON-TYPE {  
    [...]  
    module          Module 1, Module 2, Module 3, MODULE-NAME  
    [...]  
}
```

Pour prendre en compte le changement de configuration, redémarrer l'Arbiter:

```
service shinken-arbiter restart
```

## Configuration

La configuration du module se trouve par défaut dans le fichier `/etc/shinken/modules/auth_active_directory.cfg`.

- Vous trouverez aussi systématiquement un exemple dans `/etc/shinken-user-example/configuration/daemons/brokers/modules/webui/authentication_modules/auth_active_directory/auth_active_directory-example.cfg`

## Exemple de fichier de configuration

```

=====
# auth-active-directory
=====
# Daemons that can load this module:
# - synchronizer
# Modules that can load this module:
# - WebUI
# This module allow to authenticate a user with an active directory server
=====

define module {

    #==== Module identity =====
    # Module name. Must be unique
    module_name      auth-active-directory-example

    # Module type (to load module code). Do not edit.
    module_type      ad_webui

    #==== Active Directory connection =====
    # ldap_uri: uri to connect to your Active Directory server
    # with the form:
    # - ldaps://myserver
    # - ldap://myserver
    #ldap_uri         ldaps://myserver

    # username: user to connect to the ldap(s) server
    # On active directory, this will be the userPrincipalName (the form is user@myserver.com)
    # On openldap, this will be the DN (the form is cn=user,dc=myserver,dc=com)
    username          user

    # password: to use to connect to the ldap(s) server
    password          password

    # basedn: DN top level to use for query users
    basedn            DC=google,DC=com

    # Connection mode:
    # - ad: active directory
    # - openldap: openldap. If you switch to this mode, you must configure the mapping (see option below.)
    mode              ad

    # File for additional configuration of the module behavior
    # By default, the module tries to auth a user using its ldap samaccountname and the matching contact (by
    # contact name).
    # To change this behavior, put a working mapping file in your shinken-user directory.
    # You can copy the example at /etc/shinken-user-example/modules/auth-active-directory/mapping.json.
    # NEVER MODIFY OR USE EXAMPLES DIRECTLY as they will be overwritten without notice.
    #
    # mapping_file     /etc/shinken-user/configuration/modules/auth-active-directory/mapping.json

}

```

## Détails des sections composant le fichier de configuration

### Identification du module

Il est possible de définir plusieurs instances de module de type "ad\_webui" dans votre architecture Shinken .

- Chaque instance devra avoir un nom unique.

Nom	Type	Unité	Défaut	Commentaire
-----	------	-------	--------	-------------

module_name	Texte	---	<b>auth-active-directory</b>	<b>Nous vous conseillons de choisir un nom en fonction de l'utilisation du module pour que votre configuration soit simple à maintenir.</b>  Doit être unique.
module_type	Texte	---	<b>ad_webui</b>	Ne peut être modifié.

## Connexion au serveur LDAP

```

...
##### Active Directory connection #####
# ldap_uri: uri to connect to your LDAP server
# with the form:
# - ldaps://myserver
# - ldap://myserver
#ldap_uri ldaps://myserver

# username: user to connect to the LDAP/LDAPS server
# On active directory, this will be the userPrincipalName (the form is user@myserver.com)
# On openldap, this will be the DN (the form is cn=user,dc=myserver,dc=com)
username user

# password: to use to connect to the LDAP/LDAPS server
password password

# basedn: DN top level to use for query users
basedn DC=google,DC=com

# Connection mode:
# - ad: active directory
# - openldap: openldap. If you switch to this mode, you must configure the mapping (see option below.)
mode ad
...

```

Ces paramètres vous permettront de définir la connexion au serveur LDAP.

Nom	Type	Unité	Défaut	Commentaire
ldap_uri	Texte	protocole://adresse	<b>ldaps://myserver</b>	Adresse du serveur LDAP, précédée du protocole utilisé Le protocole peut-être "ldap://" ou "ldaps://" pour les serveurs utilisant le SSL
username	Texte	---	<b>user</b>	Nom d'utilisateur utilisé pour se connecter sur le serveur LDAP afin de rechercher les utilisateurs.  Cet utilisateur doit pouvoir se connecter et rechercher les utilisateurs qui pourront se connecter à travers ce module.  Des droits en lecture seule sont suffisants pour ce module.
password	Texte	---	<b>password</b>	Le mot de passe de l'utilisateur précisé ci-dessus
basedn	Texte	---	<b>DC=google, DC=com</b>	Décrit le chemin dans lequel rechercher les utilisateurs. Il ne peut y avoir qu'un seul chemin. Si deux endroits sont requis, il faut utiliser le chemin en commun.
mode	Texte	---	<b>ad</b>	Permet de spécifier si le serveur LDAP est un Active directory ( mode : ad ) ou un serveur OpenLDAP ( mode : openldap ). Seuls les valeurs "ad" et "openldap" sont acceptées pour ce paramètre

### Utilisation avec un serveur OpenLDAP

Le module est présenté et paramétré par défaut pour être utilisé avec un Active Directory. Pour utiliser avec un serveur OpenLDAP ou un serveur supportant ce protocole ( *Exemple : Oracle DSSE* ), il faudra modifier les deux champs suivants :

- **mode** : il faut le mettre à la valeur "openldap". Cela change la recherche des utilisateurs qui a été optimisée pour fonctionner avec Active Directory ou OpenLDAP
- **username** : Avec Open LDAP, le format de ce champ est l'identifiant unique ( *Distinguished Names* ) sous la forme suivante : "cn=user,dc=mydomain,dc=com".

## Correspondances des attributs LDAP avec les propriétés ou données Shinken

```
...
# File for additional configuration of the module behavior
# By default, the module tries to auth a user using its LDAP samaccountname and the matching contact (by
contact name).
# To change this behavior, put a working mapping file in your shinken-user directory.
# You can copy the example at /etc/shinken-user-example/modules/auth-active-directory/mapping.json
# NEVER MODIFY OR USE EXAMPLES DIRECTLY as they will be overwritten without notice.
#
# mapping_file /etc/shinken-user/configuration/modules/auth-active-directory/mapping.json
...
```

Le fichier de mapping permet de faire correspondre un attribut LDAP avec une propriété Shinken afin d'identifier un utilisateur.

- Par défaut, le module recherche les contacts avec la propriété "contact\_name" dans Shinken et recherche un contact dans LDAP avec l'attribut "samaccountname".
- Il est possible de paramétrer ce comportement à l'aide d'un fichier de correspondances.

Il faut copier le fichier "**/etc/shinken-user-example/configuration/daemons/brokers/modules/webui/authentication\_modules/auth\_active\_directory/mapping.json**" dans "**/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json**" ( *créer l'arborescence si besoin* ).

### Fichiers d'exemple

Les fichiers présents dans "**/etc/shinken-user-example/**" sont en lecture seule. Il faut rajouter les droits en écriture après la copie dans "**/etc/shinken-user/**".

Nom	Type	Unité	Défaut	Commentaire
mapping_file	Texte	---	<b>/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json</b>	Lien vers le fichier de mapping. Ce fichier permet de faire correspondre les propriétés Shinken avec les attributs LDAP pour trouver un utilisateur.  Il est également possible de modifier le placeholder du champs de connexion "Login" affiché lors de la connexion à Shinken

## Correspondance des champs entre LDAP et Shinken ( mapping.json )

Le fichier de mapping permet de faire correspondre un attribut LDAP avec une propriété Shinken afin d'identifier un utilisateur.

Par défaut, le module recherche les contacts avec la propriété "contact\_name" dans Shinken et recherche un contact dans LDAP avec l'attribut "samaccountname".

Il est possible de paramétrer ce comportement à l'aide d'un fichier de correspondances.

Pour cela il faut copier le fichier "**/etc/shinken-user-example/configuration/daemons/brokers/modules/webui/authentication\_modules/auth\_active\_directory/mapping.json**" dans "**/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json**" ( *créer l'arborescence si besoin* ).



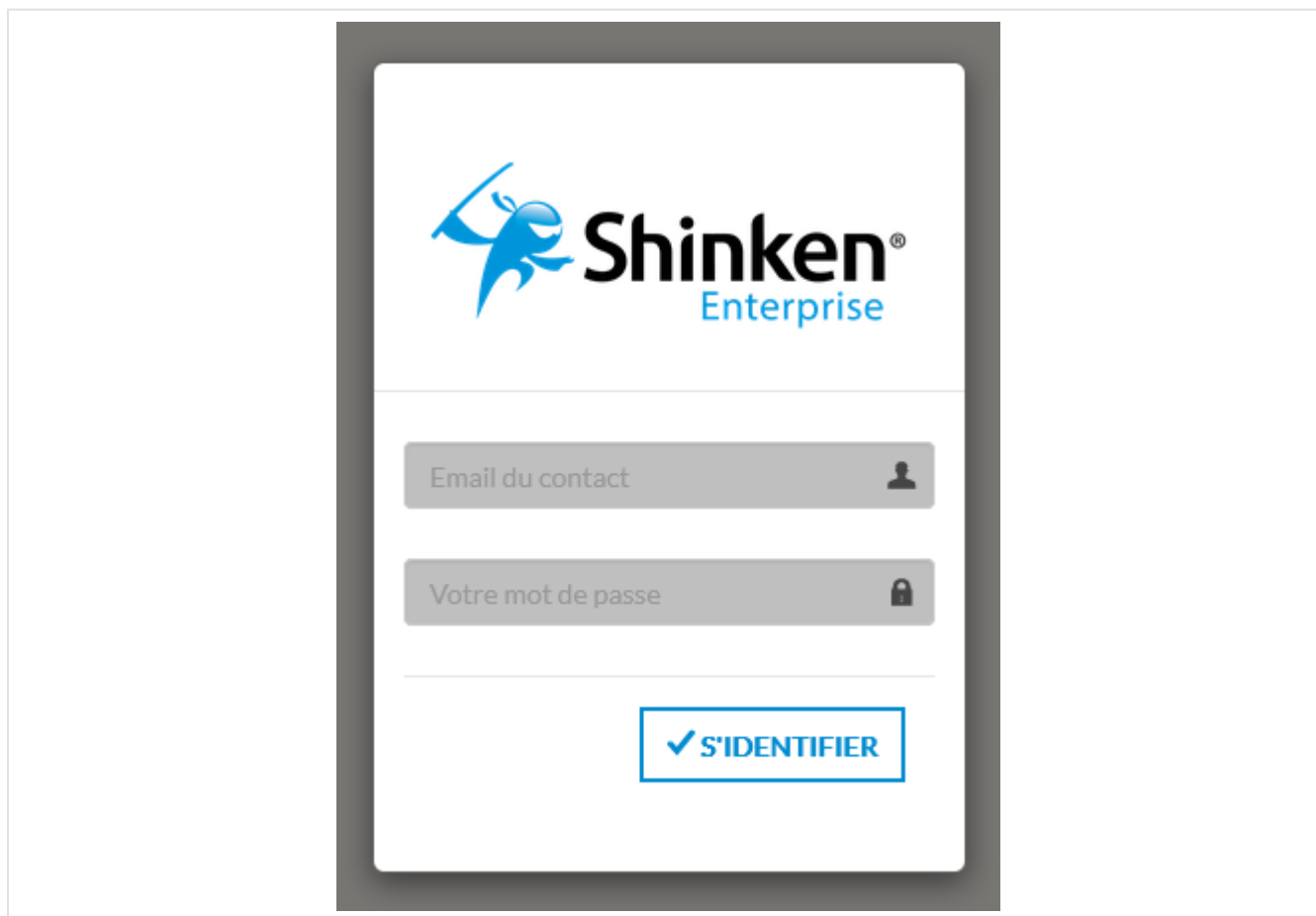
### Fichiers d'exemple

Les fichiers présents dans `/etc/shinken-user-example/` sont en lecture seule. Il faut rajouter les droits en écriture après la copie dans `/etc/shinken-user/`.

Voici les paramètres de ce fichier de configuration :

Nom	Type	Unité	Défaut	Commentaire
ldap_key	Texte	---	samacco untname	L'attribut LDAP qui sera utilisé pour faire la correspondance avec Shinken  N'importe quel attribut présent sur vos utilisateurs peut être utilisé, du moment qu'ils sont renseignés sur vos utilisateurs Shinken
shinken_key	Texte	---	contact_ name	La propriété Shinken qui sera utilisée pour faire la correspondance avec LDAP  N'importe quelle propriété ou donnée peut être utilisée pour identifier vos utilisateurs, du moment qu'un attribut correspondant se trouve sur l'utilisateur LDAP
login_placeholder	Texte	---		Si une valeur est définie dans ce champ, elle sera utilisée dans le formulaire de connexion pour indiquer aux utilisateurs quel identifiant utiliser ( Ex: "Email du contact", voir ci-dessous )

Le paramètre `login_placeholder` permet de configurer le message qui sera affiché sur l'écran de connexion afin de fournir une aide visuelle à l'utilisateur :



Liste des correspondances les plus utilisées

Voici ci-dessous un tableau récapitulatif des propriétés et attributs les plus utilisés pour le fichier de mapping :

Shinken	Active Directory	Open LDAP
contact_name	samAccountName	uid
display_name	displayName	displayName
email	mail	mail
pager	telephoneNumber	telephoneNumber

## Exemple de déclaration de l'utilisation du module dans configuration de l'interface de Visualisation

Afin que le module soit utilisable sur l'interface de visualisation, il faut simplement déclarer le module sur le module WebUI.

Dans cet exemple, le module est nommée "auth-active-directory"

```
/etc/shinken/modules/webui.cfg

define module {
    module_name          WebUI
    #[ ... ]
    modules              auth-active-directory, MongoDB, webui-enterprise, sla
    #[ ... ]
}
```

Redémarrer ensuite l'Arbiter pour prendre en compte les modifications.

```
/etc/init.d/shinken-arbiter restart
```



### Module Cfg\_password

La présence simultanée des modules *Cfg\_password* et *auth-active-directory* peut provoquer un fonctionnement non anticipé. Comme le module *Cfg\_password* vérifie les mots de passe dans la base Shinken et le module *auth-active-directory* dans LDAP, si les 2 modules sont chargés, l'utilisateur pourra se connecter avec les 2 mots de passe ( *Shinken et LDAP* ).

Si ce comportement est souhaité, il est possible d'avoir les 2 modules dans la configuration.

Les modules sont alors utilisés dans l'ordre défini dans le fichier CFG ( *ici d'abord le module auth-active-directory puis le Cfg\_password* ) :

- Si le premier module identifie l'utilisateur, alors le processus d'identification s'arrête.
- Sinon, il essaye avec le suivant.

La présence simultanée des modules *Cfg\_password* et *auth-active-directory* peut provoquer un fonctionnement non anticipé. Comme le module *Cfg\_password* vérifie les mots de passe dans la base Shinken et le module *auth-active-directory* dans LDAP, si les 2 modules sont chargés, l'utilisateur pourra se connecter avec les 2 mots de passe ( *Shinken et LDAP* ).

Si ce comportement est souhaité, il est possible d'avoir les 2 modules dans la configuration. Les modules sont alors utilisés dans l'ordre défini dans le fichier CFG ( *ici d'abord le module auth-active-directory puis le Cfg\_password* ) :

```
modules          auth-active-directory, Cfg_password, autres_modules_eventuels
```

**/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json**

```
# Note: comments can only be preceded by spaces, they should NOT be after a value
# =====
{
  #===== ldap_key =====
  # Describe which ldap attribute will be used for the login. Case
  # insensitive.
  #
  # Possible values include:
  # - samaccountname: Login key on windows systems. This is the
  # default on active directory.
  # - uid: Login key on openldap systems. This is the default on
  # openldap.
  # - mail: The mail address of the user. If used, must be unique.
  # - [...]
  "ldap_key": "mail",
  #===== shinken_key =====
  # Describe which shinken property will be used for the login. The
  # ldap attribute and the shinken contact must match for the
  # authentication to be successful.
  #
  # Possible values include:
  # - contact_name: Shinken login key. This is the default.
  # - display_name: Shinken display name. If used, must be unique.
  # - email: The mail address of the user. If used, must be unique.
  # - [...]
  "shinken_key": "email",
  #===== login_placeholder =====
  # Free text field to help users to know which login he or she should
  # use.
  "login_placeholder": "Email du contact"
}
```