# Erreur d'authentification à un serveur LDAP ou Active directory

**Sommaire**



## Contexte

Shinken permet d'utiliser un serveur LDAP ou Active Directory de deux manières :

- Comme méthode d'authentification, via un module de type "`ad_webui`" :
  - Webui - Authentification avec LDAP
  - Synchronizer - Authentification avec LDAP
- Comme source de données pour les éléments dans Shinken, via un collecteur de type "`ldap-import`" :
  - Collecteur de type ldap-import ( pour Open LDAP )
  - Collecteur de type ldap-import ( pour Active Directory )

Dans la configuration, il est nécessaire de spécifier un utilisateur pour se connecter au serveur.

Les erreurs de configuration étant fréquentes et parfois longues à diagnostiquer, cette page regroupe les commandes utiles pour investiguer efficacement.

## Exemples d'erreurs

Les erreurs fréquemment rencontrées lors de l'authentification :

- **Mauvais mot de passe ou utilisateur incorrect :**

Si les identifiants fonctionnent avec la commande **`ldapwhoami`** mais pas dans Shinken, le problème peut provenir d'un caractère mal interprété. Pour échapper un caractère dans la configuration de Shinken, il faut le précéder d'un antislash ( "\" ).

- **Certificat incorrect :**

Dans le cas d'une connexion **LDAPS**, Shinken peut refuser le certificat. Quand celui-ci est incorrect, par exemple si le nom **SN** du certificat ne correspond pas à l'adresse IP ou au nom du serveur, ou s'il est absent dans la chaîne de confiance des certificats de la machine.

- **Fichier json non copié sur la machine avec le module.**

Sur les machines avec le Broker qui utilise le module d'authentification LDAP, il faut que le fichier de mapping soit présent et avec les bonnes informations.
Ces informations ne sont pas envoyées par l'Arbiter mais lues localement dans le fichier de mapping.

La position du fichier est configurée avec la clé "mapping_file" dans le fichier de configuration du module.
Par défaut, la position du fichier est `/etc/shinken-user/configuration/daemons/brokers/modules/webui/authentication_modules/webui-module-authentication-LDAP/mapping.json`

### Module de type "ad_webui"

Les problèmes de connexion aux serveurs LDAP pour un module de type "`ad_webui`" sont détectés à la fois par le shinken-healthcheck et par les checks de supervision Synchronizer - $KEY$ - Alive ou  Broker - $KEY$ - Alive.

Exemple d'erreur :

- Dans le shinken-healthcheck :

```
[ synchronizers ]
   [synchronizer: synchronizer-master]
      OK:      Connect to MongoDB with address : [172.16.0.180]
      OK:      Auth_secret is a custom variable
      OK:      Connection to daemon is OK at port 7765
      OK:      Connection to Synchronizer UI is OK at port 7766
      OK:      Configuration seems valid
      OK:      Daemon version is: VC_Charlie-006.1-B04
      [Encryption status]
         OK:      Encryption DISABLED
      Modules:
         ERROR:   Name: synchronizer-module-authentication-LDAP  Type: ad_webui => The username and password set for LDAP s
ver "ldap://149.56.109.186" in cfg file "/etc/shinken/modules/synchronizer-module-authentication-LDAP.cfg:10" are invalid.
         OK:      Name: synchronizer-module-database-backup      Type: synchronizer_module_database_backup
         OK:      Name: Cfg_password                             Type: cfg_password_webui
      Sources:
         OK:      Name: ip-tag-dmz                               Type: sync-ip-tag
         OK:      Name: sync-regexp-tag                          Type: sync-regexp-tag
```

- Dans l'Interface de Visualisation :

Module info :

| Name | Type | Status | Restart in the last 2h | Last restart date | Submodules |
|---|---|---|---|---|---|
| Cfg_password | cfg_password_webui | OK | 0 | | - |
| synchronizer-module-authentication-LDAP | ad_webui | CRITICAL | 0 | | - |

### Collecteur de type "ldap-import"

L'erreur de connexion sera affichée dans l'interface du Synchronizer lors de l'import de la source.

Exemple d'erreur :

05/12/2025 13:44 Erreur L'import LDAP a échoué à cause d'erreurs critiques

Erreurs avant le MÉLANGE des sources :

- {'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [], 'info': '80090308: LdapErr: DSID-0C0904AE, comment: AcceptSecurityContext error, data 52e, v3839'}

## Tester la connexion au serveur LDAP/AD

Le client OpenLDAP est utilisé pour tester la connexion au serveur LDAP/Active Directory.

Installer le client :

```
yum install openldap-clients
```

Commande pour tester l'authentification :

```
ldapwhoami -x -H URI -D "USER" -w 'PASSWORD'
```

Exemple :

```
ldapwhoami -x -H ldap://192.168.1.98 -D "SHINKEN\Administrator" -w "admin"
```

Pour éviter que le mot de passe apparaisse dans l'historique du shell, on peut remplacer l'option **-w** par l'une des options suivantes :

- **-W** : le mot de passe est demandé de manière interactive dans un prompt ;
- **-y <fichier>** : le mot de passe est lu depuis le fichier spécifié.

## Mode debug

L'option **-d** permet d'exécuter la commande en mode débogage, afin d'obtenir davantage d'informations en cas d'erreur de connexion.

```
ldapwhoami -x -H URI -D "USER" -w 'PASSWORD'  -d 1
```