

Broker - Les logs du module auth-active-directory

Sommaire

- Initialisation du module
 - Lecture des fichiers de mapping
 - Résumé de la configuration chargée
 - Première connexion au serveur LDAP
- Authentification d'un utilisateur
 - Les logs en INFO
 - Les logs de WARNING
 - Les logs en ERROR
 - Les logs en DEBUG

Initialisation du module

Lecture des fichiers de mapping

Cas général où les fichiers ne comportent pas d'erreur et un fichier utilisateur est précisé

```
[YYYY-MM-DD HH:MM:SS] INFO    : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ INITIALISATION ] Read the default mapping file "/etc/shinken/_default/modules/auth-active-directory/mapping.json" to get default values
[YYYY-MM-DD HH:MM:SS] INFO    : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ INITIALISATION ] Read the file "/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json" to override default values
```

En cas d'erreur de lecture d'un fichier (chemin erroné) :

```
[YYYY-MM-DD HH:MM:SS] WARNING: [ WEBUI-NAME      ] [ MODULE_NAME      ] [ INITIALISATION ] The parameter mapping_file is defined on "/etc/shinken-user/modules/auth-open-ldap/mapping.json", but this file doesn't exist. The default values are used.
```

Erreur de syntaxe dans le fichier JSON : virgule en trop, crochets fermants manquants ... :

```
[YYYY-MM-DD HH:MM:SS] ERROR   : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ INITIALISATION ] The file "/etc/shinken-user/modules/auth-active-directory/mapping.json" is malformed. The error is : Expecting property name enclosed in double quotes: line 5 column 1 (char 88)
```

Le fichier comporte un paramètre inconnu ou une erreur de syntaxe dans le nom du paramètre :

```
[YYYY-MM-DD HH:MM:SS] ERROR   : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ INITIALISATION ] The parameter "login_place_holder" set in file "/etc/shinken-user/modules/auth-active-directory/mapping.json" is not an allowed parameter
```

S'il manque un paramètre pour se connecter, le module affiche un log et il ne sera pas utilisé lors de l'authentification des utilisateurs :

```
[YYYY-MM-DD HH:MM:SS] ERROR   : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ INITIALISATION ] For the module defined in the file "/etc/shinken/modules/auth_active_directory.cfg:12", these parameters are missing : ldap_uri. Can't use this module to authenticate users
```

Résumé de la configuration chargée

Ces logs permettent de connaître la configuration utilisée par le module, qu'il y ait des erreurs de lecture de fichier ou pas.

```
[YYYY-MM-DD HH:MM:SS] INFO : [ WEBUI-NAME ] [ MODULE_NAME ] [ INITIALISATION ] EXPLANATION : The property "contact_name" in Shinken will be compared to the LDAP attribute "uid" to authenticate users. In the login page, the placeholder is "votre.compte@shinken.local"
[YYYY-MM-DD HH:MM:SS] INFO : [ WEBUI-NAME ] [ MODULE_NAME ] [ INITIALISATION ] EXPLANATION : The authentication will be done on LDAP server "ldap://ldap-server" on the base "dc=shinken,dc=local" and this server is an Open LDAP
```

Première connexion au serveur LDAP

Au démarrage le module tente de se connecter pour vérifier les login/mot de passe renseignés dans le module. S'ils sont bons, le message indique qu'on peut se connecter et que le module est prêt à authentifier les utilisateurs.

```
[YYYY-MM-DD HH:MM:SS] INFO : [ WEBUI-NAME ] [ MODULE_NAME ] [ INITIALISATION ] The Username and password set in cfg file "/etc/shinken/modules/auth_active_directory.cfg:12" are correct and LDAP server at "ldap://ldap-server" is available to authenticate users
```

Le cas échéant, le module indique les mauvais logins et ne tentera pas de se reconnecter à chaque fois qu'un utilisateur tente de se connecter. L'état du module sera remonté dans le healthcheck et le check Shinken. Il faut corriger les identifiants et relancer l'Arbiter

```
[YYYY-MM-DD HH:MM:SS] ERROR : [ WEBUI-NAME ] [ MODULE_NAME ] [ INITIALISATION ] The username and password set for LDAP server "ldap://ldap-server" in cfg file "/etc/shinken/modules/auth_active_directory.cfg:12" are invalid. Can't use this module to authenticate users.
```

Dans le cas où le serveur LDAP n'est pas disponible au démarrage du module, ces logs indiquent que la tentative de reconnexion sera effectuée quand un utilisateur tentera de se connecter

```
[YYYY-MM-DD HH:MM:SS] ERROR : [ WEBUI-NAME ] [ MODULE_NAME ] [ INITIALISATION ] Can't connect to LDAP server "ldap://ldap-server" => error : Can't contact LDAP server
[YYYY-MM-DD HH:MM:SS] WARNING: [ WEBUI-NAME ] [ MODULE_NAME ] [ INITIALISATION ] The LDAP server "ldap://ldap-server" is unavailable for the moment. The connection will be retried when a user tries to connect
```

Authentification d'un utilisateur

Les logs en INFO

Lorsque le module fonctionne et qu'il n'y a pas d'erreur lors de la recherche d'un utilisateur, le module ne log aucune INFO. Le module retourne l'utilisateur s'il l'a trouvé et False le cas échéant.

C'est la Webui qui logue si le module a authentifié ou non un utilisateur.

Les logs de WARNING

Les logs de warning permettent de diagnostiquer les problèmes en loguant des informations sur les utilisateurs.

- Dans le cas où l'utilisateur n'a pas saisi de mot de passe :

```
[YYYY-MM-DD HH:MM:SS] WARNING: [ WEBUI-NAME ] [ MODULE_NAME ] [ AUTHENTICATION ] [ UI Visualization ] User "user.example" doesn't give the password. It's not allowed ( authentication phase id-98e66a548bad11eb88b4080027cc5994 )
```

- Dans le cas où l'attribut LDAP renseigné dans le fichier de mapping n'a pas été trouvé sur l'objet LDAP correspondant à l'utilisateur :

```
[YYYY-MM-DD HH:MM:SS] WARNING: [ WEBUI-NAME ] [ MODULE_NAME ] [ AUTHENTICATION ] [ UI Visualization ] The LDAP object has not the attribute "uuid". Can't map the attribute with the shinken key. The user value ( user.example ) will be used to find the user ( authentication phase id-98e66a548bad11eb88b4080027cc5994 )
```

Les logs en ERROR

Lors d'une tentative d'authentification, il est possible de rencontrer les erreurs suivantes:

- Pas de connexion au serveur LDAP à cause d'un paramètre manquant

```
[YYYY-MM-DD HH:MM:SS] ERROR : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] Can't connect to the LDAP server. For the module defined in the file "/etc/shinken/modules
/auth_active_directory.cfg:12", these parameters are missing : ldap_uri. Can't use this module to
authenticate users.
```

- Pas de connexion au serveur LDAP à cause d'un identifiant (dans le fichier de configuration) erroné

```
[YYYY-MM-DD HH:MM:SS] ERROR : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] The username and password set for LDAP server "ldap://ldap-server" in cfg file "/etc/shinken
/modules/auth_active_directory.cfg:12" are invalid. Can't use this module to authenticate users (
authentication phase id-a95ff93a8bbd11ebbd80080027cc5994 )
```

- Perte de la connexion au serveur LDAP pendant une authentification (timeout, service qui s'éteint, ...)

```
[YYYY-MM-DD HH:MM:SS] ERROR : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] Error during requesting the LDAP server "ldap://ldap-server" during authentication phase id-
a95ff93a8bbd11ebbd80080027cc5994. Error message is : Can't contact LDAP server
```

Les logs en DEBUG

Les logs en debug sont les plus précis et permettent de tracer un utilisateur.

- Le module reçoit une requête

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] Trying to authenticate username "user.example" on LDAP server "ldap://ldap-server" (
authentication phase id-b947c70a8bc311ebbf8e080027cc5994 )
```

- Si l'utilisateur n'existe pas dans la base Shinken (s'il existe, rien n'est logué)

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] User "user.example" tried to connect but this username doesn't match any user in Shinken
database with the property "contact_name" ( authentication phase id-b947c70a8bc311ebbf8e080027cc5994 )
```

- le module cherche dans la base LDAP un utilisateur correspondant (en se connectant avec les identifiants du module)

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] Search for a user in LDAP server "ldap://ldap-server". The LDAP attribute used is
"samaccountname" with the value "user.example". The LDAP request filter is : "(samaccountname=user.example)"
( authentication phase id-b947c70a8bc311ebbf8e080027cc5994 )
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] Trying to get the connection to LDAP server "ldap://ldap-server" with this user
"SHINKEN\administrator" on base_dn "DC=SHINKEN,DC=local" in mode "ad" ( authentication phase id-
b947c70a8bc311ebbf8e080027cc5994 )
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] Connection to the LDAP server "ldap://ldap-server" is OK ( authentication phase id-
b947c70a8bc311ebbf8e080027cc5994 )
```

- Si l'utilisateur a été trouvé dans LDAP

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI
Visualization ] A user was found in the LDAP server "ldap://ldap-server" in base "DC=SHINKEN,DC=local" with
the attribute "samaccountname=user.example". His name is "user.example@SHINKEN.local" ( authentication phase
id-b947c70a8bc311ebbf8e080027cc5994 )
```

- Si L'utilisateur n'a pas été trouvé dans LDAP (arrêt de la tentative de connexion)

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI  
Visualization ] There is no user in the LDAP server "ldap://ldap-server" in base "dc=shinkendom,dc=local"  
which has the attribute "uid=user.example" ( authentication phase id-0460f2a68bc511eba496080027cc5994 )
```

- On vérifie le mot de passe en se connectant au LDAP avec l'utilisateur trouvé dans le LDAP et le mot de passe donnée par l'utilisateur. En cas de succès (utilisateur authentifié) :

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI  
Visualization ] Credentials for LDAP user "user.example" are OK. Authenticated as shinken user "user.  
example" ( authentication phase id-b947c70a8bc311ebbf8e080027cc5994 )
```

- En cas d'erreur de connexion (arrêt de la tentative de connexion)

```
[YYYY-MM-DD HH:MM:SS] DEBUG : [ WEBUI-NAME      ] [ MODULE_NAME      ] [ AUTHENTICATION ] [ UI  
Visualization ] Credentials for "user.example" ( "user.example" in shinken ) failed. Server "ldap://ldap-  
server" refused the user's password ( authentication phase id-1cca18f48bc511eba72c080027cc5994 )
```