Authentification avec Active Directory/OpenLDAP

Fonctionnement global du module

Le module d'authentification Active Directory permet de lier un compte Shinken et un compte Active Directory pour se connecter sur les différentes interfaces Web de Shinken Entreprise.

Les deux comptes (Shinken et Active Directory) seront liés par une clé commune.

Par exemple, le module d'authentification cherche l'utilisateur avec l'adresse email utilisateur@domaine.com dans la base de données Shinken et fera la correspondance avec le compte Active Directory ayant la même adresse email.

Il est donc impératif qu'un compte Shinken et un compte Active Directory possèdent une donnée commune pour pouvoir être liés et autoriser la connexion.

La procédure pour configurer la donnée à utiliser pour effectuer la correspondance est décrite plus bas dans cette documentation.

Conseil d'utilisation

Pour garder la base de données Shinken et l'annuaire Active Directory synchronisés, il est bien plus pratique d'importer directement les utilisateurs depuis l'annuaire Active Directory grâce à la source Active Directory.

Voir la documentation associée pour plus d'information sur cette fonctionnalité: Active Directory

Procédure de configuration

Ce module permet d'effectuer l'authentification des utilisateurs en allant vérifier le mot de passe du compte dans un annuaire Active Directory plutôt que celui stocké dans la configuration Shinken.

La configuration de cette méthode d'authentification s'effectue en 3 étapes:

- Configuration des identifiants de connexion au serveur Active Directory
- Configuration des correspondances des champs entre Shinken et Active Directory
- Activation du module

Configuration de la connexion Active Directory

Tout d'abord, il faut spécifier au module d'authentification les identifiants de connexion au serveur Active Directory.

Cela se fait par l'intermédiaire du fichier **/etc/shinken/modules/auth_active_directory.cfg**

Décommenter si besoin et renseigner les lignes suivantes:

/etc/shinken/modules/auth_active_directory.cfg

```
ldap_uri                ldap://myserver
username                myuser@mydomain.com
password                password
basedn                        DC=mydomain,DC=com
mapping_file        /etc/shinken-user/configuration/modules/auth-active-directory/mapping.json
```

Le champs présents dans la configuration ci-dessus ont le fonctionnement suivant:

- **ldap_uri**: Adresse du serveur ActiveDirectory. Le protocole utilisé peut être *ldap* ou *ldaps*
- **username**: Nom d'utilisateur utilisé pour se connecter au serveur Active Directory. Il est de la forme "*user@mydomain.com*" ou "*mydomain\user*"
- **password**: Mot de passe utilisé pour se connecter au serveur Active Directory
- **basedn**: DN utilisé comme base pour la recherche des utilisateurs. Le module cherche récursivement dans le DN fourni tous les utilisateurs présents dans ce DN pour effectuer l'authentification.
- **mapping_file**: Ce champ doit pointer vers le fichier de correspondances dont le fonctionnement est détaillé ci-dessous.

Configuration des correspondances entre Shinken et Active Directory

Le module d'authentification Active Directory effectue une correspondances entres les champs dans la base Shinken et les champs dans l'annuaire Active Directory pour identifier les utilisateurs.

Par défaut, le module recherche les contacts avec le champ "*contact_name"* dans Shinken et recherche un contact dans Active Directory avec le champ *"samaccountname"*.

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

Sur une nouvelle installation, il faut copier le fichier *"/etc/shinken-user-example/configuration/modules/auth-active-directory/mapping.json"* dans *"/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json"* (créer l'aborescence si besoin).

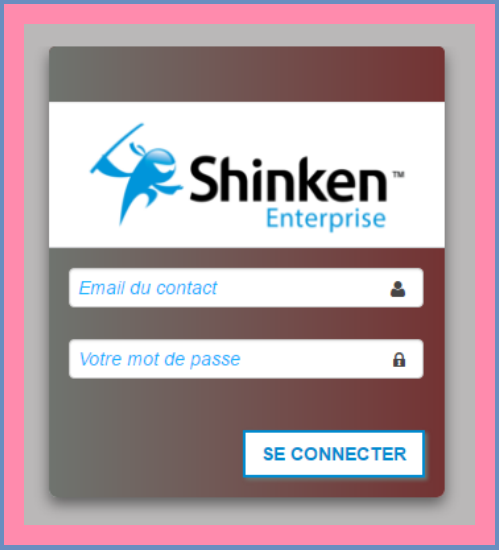
> **Fichiers d'exemple**
>
> Les fichiers présents dans "*/etc/shinken-user-example"* sont en lecture seule. Il faut rajouter les droits en ecriture après la copie dans "*/etc/shinken-user*".

Dans l'exemple suivant, les contacts sont joints par le champ *"mail"* sur Active Directory et le champ *"email"* sur Shinken

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

```
{
        "ldap_key":                         "mail",
        "shinken_key":                        "email",
        "login_placeholder":          "Email du contact"
}
```

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



Activation du module Active Directory

Enfin, il faut activer le module d'authentification dans les différents fichiers de configuration.

UI Configuration

Pour l'activer sur l'interface de Configuration, remplacer *Cfg_password* par *auth-active-directory* dans la configuration du Synchronizer.

/etc/shinken/synchronizers/synchronizer_master.cfg

```
modules                 auth-active-directory
```

Rémarrer ensuite le Synchronizer pour prendre en compte les modifications.

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

UI Visualisation

Pour l'activer sur l'interface de Visualisation, remplacer *Cfg_password* par *auth-active-directory* dans la configuration du Broker (Module WebUI).

/etc/shinken/modules/webui.cfg

```
modules                 auth-active-directory, Mongodb, webui-enterprise, sla
```

Rémarrer ensuite le Broker pour prendre en compte les modifications.

```
/etc/init.d/shinken-broker 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 Active Directory, si les 2 modules sont chargés, l'utilisateur pourra se connecter avec les 2 mots de passe (Shinken et Active Directory).

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

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

Utilisation du module avec OpenLDAP

Le module est initialement prévu pour Active Directory mais fonctionne également avec OpenLDAP.

Cependant, lors de la configuration, quelques étapes diffèrent:

- Dans le fichier de configuration **/etc/shinken/modules/auth_active_directory.cfg**, le paramètre "*mode*" doit être "*openldap*".
- Dans le fichier de configuration **/etc/shinken/modules/auth_active_directory.cfg**, le paramètre "*username*" a un format différent. Avec OpenLDAP, il faut spécifier un CN à utiliser pour la connexion.
  Le champ serait alors de la forme "*cn=user,dc=mydomain,dc=com*".

Le reste de la configuration du module reste identique.

Champs à utiliser pour la correspondance des champs

Dans le fichier de correspondances, il est possible de spécifier plusieurs champs pour lier les comptes Shinken et Active Directory/LDAP.

Voici ci-dessus un tableau récapitulatif des champs les plus utilisés:

Shinken	Active Directory	OpenLDAP
contact_name	sAMAccountName	uid
display_name	displayName	displayName
email	mail	mail
pager	telephoneNumber	telephoneNumber