Module auth-active-directory pour le Synchronizer

Sommaire

Introduction

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.

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 Active Directory ou Collecteur OpenLDAP

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 configuration.

Avoir plusieurs modules d'authentifications

Vous pouvez définir et utiliser plusieurs modules d'authentification sur le Synchronizer, ce qui est très pratique si vous avez un serveur LDAP primaire et des secondaires.
Pour chaque essaie 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.

Configuration du module

La configuration du module se fait en trois étapes :

1. Définir le module et configurer l'accès au serveur LDAP (adresse, utilisateur, mot de passe, ...).
2. La seconde est de configurer la correspondance des propriétés Shinken avec les attribut LDAP grâce au fichier de mapping.
3. Utilisation du module sur l'interface de configuration

Définition du module et configuration

Vous aurez un fichier de définition par instance de module que vous avez besoin

- Par défaut, nous livrons /etc/shinken/modules/auth_active_directory.cfg,
- mais vous pouvez le copier pour définir de nouveau module (pour pointer vers un LDAP secondaire)

Voici les paramètres du module :

Nom du paramètre	Description	Valeur par défaut
module_name	Nom du module que vous aurez choisi.	
module_type ad_webui	auth-active-directory # Module type (to load module code). Do not edit	auth-active-directory, non modifiable
ldap_uri	Adresse du serveur LDAP, précédée du protocole utilisé. Le protocole peut-être "ldap://" ou "ldaps://" pour les serveurs utilisant le SSL.	ldaps://myserver
username	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 suffisant pour ce module.	user
password	Le mot de passe de l'utilisateur précisé ci-dessus.	password
basedn	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.	DC=google,DC=com
mode	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.	ad
mapping_file	Lien vers le fichier de mapping. Ce fichier permet : • de faire correspondre les propriétés Shinken avec les attributs LDAP pour trouver un utilisateur. • Ainsi que de définir le message qui apparait dans la Zone de saisie de l'utilisateur (*ce qui vous permet de donner des indications aux utilisateurs sur comment s'identifier => Ex: "Email de l'utilisateur"*).	/etc/shinken-user/configuration /modules/auth-active-directory /mapping.json

Lorsque vous modifiez les paramètres de ce module, vous devez redémarrer le Synchronizer pour les prendre en compte.

OpenLDAP VS ActiveDirectory

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 optimisé 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*"

Correspondance des Champs entre LDAP et Shinken

Le fichier de maping 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/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 du paramètre	Description	Valeur par défaut
ldap_key	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	samaccountname
shinken_key	La propriété Shinken qui sera utilisée pour faire la correspondance avec LDAP N'importe quelle propriété ou donnée peut être utilisé pour identifier vos utilisateurs, du moment qu'un attribut correspondant se trouve sur l'utilisateur LDAP	contact_name
login_placeholder	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 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:

Correspondance les plus utilisées

Voici ci-dessous un tableau récapitulatif des propriété et attribut 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

Déclaration de l'utilisation du module dans configuration de l'UI de configuration

Afin que le module soit utilisable sur l'interface de configuration, il faut simplement déclarer le module sur le daemon Synchronizer (voir Définition du démon (synchronizer-master.cfg)).

/etc/shinken/synchronizers/synchronizer-master.cfg

```
define synchronizer {

    synchronizer_name   synchronizer-master

    #[ ... ]
    modules             auth-active-dir, Cfg_password, synchronizer-module-database-backup
    #[ ... ]
}
```

Re-démarrer ensuite le Synchronizer pour prendre en compte les modifications.

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

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

Exemple de définition

Dans le répertoire **/etc/shinken/modules/**, voici un exemple de définition qui permet la définition du module auth-active-directory :

⚠ Il est conseillé d'éditer les fichiers .cfg avec l'encodage utf-8

/etc/shinken/modules/auth_active_directory.cfg

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


define module {

# Shinken Enterprise. Lines added by import core. Do not remove it, it's used by Shinken Enterprise to
update your objects if you re-import them.
    _SE_UUID             core-module-26a4fce25adc11e58014080027f08538
    _SE_UUID_HASH        f6daeb0b270c3d80e5649bf000991178
# End of Shinken Enterprise part

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

    # 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://192.168.1.125

    # 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        admin@shinken.local

    # password: to use to connect to the ldap(s) server
    password        azerty123

    # basedn: DN top level to use for query users
    basedn          DC=shinken,DC=local

    # 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

}
```

Voici un exemple de fichier de mapping :

/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
unsensitive.
                                    #
                                    # 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
values in 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"
}
```