

Mode Opérateur

OCS – LDAP



MENAGE-BIMENET Cyliau / COELHO Tom
15/11/2024

Auteur	MENAGE BIMBENET Cylian
Date de création	15/04/2024
Rédiger par	MENAGE BIMBENET Cylian / COELHO Tom
Réalisé par	MENAGE BIMBENET Cylian / COELHO Tom
Valider par	MENAGE BIMBENET Cylian / COELHO Tom

Objectif de la procédure : Installation et configuration du LDAP sur OCS

Matériels utilisés : Une Debian12 et un Windows 11.

Sommaire

Table des matières

I. Installation du package PHP	4
II. Connexion d'OSC au serveur LDAP.....	5

I. Installation du package PHP

Pour configurer une liaison LDAP avec PHP, vous devez installer l'extension `php-ldap`. Assurez-vous de télécharger la version de l'extension qui correspond à la version de PHP installée sur votre système.

Téléchargez le paquet nécessaire :

```
wget -c https://packages.sury.org/php/pool/main/p/php8.3/php8.3-ldap-  
dbgsym_8.3.14-3%2B0~20241125.49%2Bdebian11~1.gbp1464d7_amd64.deb
```

Installez le paquet :

```
dpkg -i php8.3-ldap-dbgsym_8.3.14-  
3+0~20241125.49+debian11~1.gbp1464d7_amd64.deb
```

Mettez à jour la liste des paquets et corrigez les dépendances manquantes :

```
apt update
```

```
apt --fix-broken install
```

Installez l'extension `php8.3-ldap` depuis les dépôts :

```
apt install php8.3-ldap
```

Redémarrez le service Apache pour appliquer les modifications :

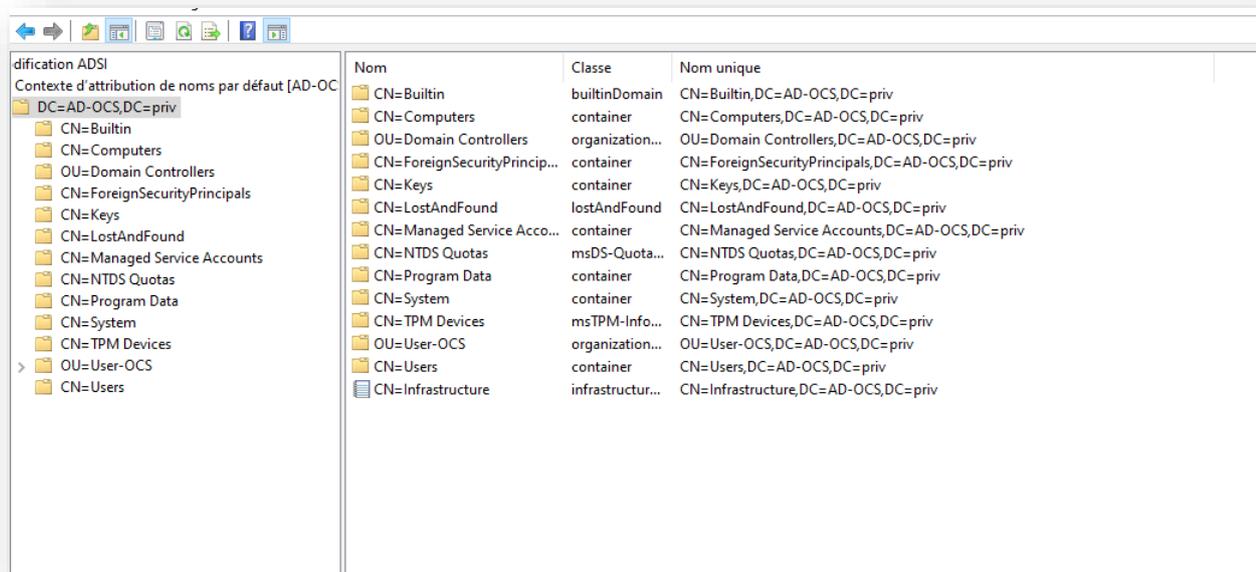
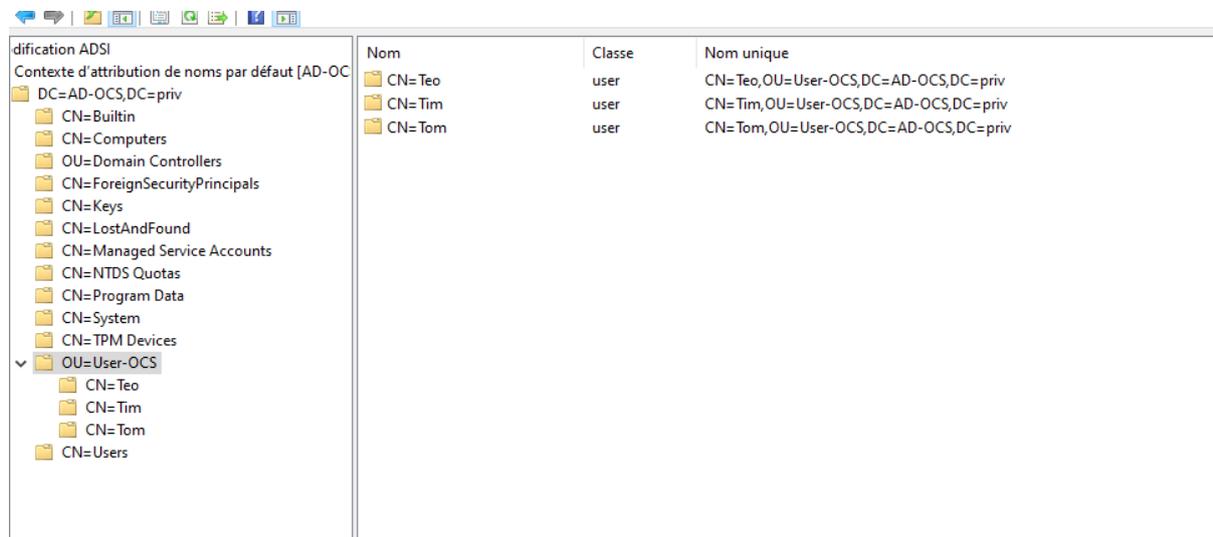
```
systemctl restart apache2
```

Installez également l'outil `ldap-utils` pour tester et administrer les connexions LDAP :

```
apt install ldap-utils
```

II. Connexion d'OSC au serveur LDAP

Accédez à votre serveur Active Directory (AD), puis ouvrez l'outil "**Modification ADSI**". Cet outil vous permet d'afficher l'arborescence complète de votre annuaire Active Directory.



Sur le serveur OCS :

Faite un test de connexion, avec ldapsearch :

Exemple « ldapsearch -x -H ldaps://your-ldap-server -b "dc=example,dc=com" -D "cn=admin,dc=example,dc=com" -W »

Notre test de connexion :

```
ldapsearch -x -H ldap://172.20.133.253 -b "dc=AD-OCS,dc=priv" -D "cn=Tom,ou=User-OCS,dc=AD-OCS,dc=priv" -W
```

Ouvrez le fichier suivant avec un éditeur de texte :

```
nano /usr/share/ocsinventory-reports/ocsreports/var.php
```

Modifiez les paramètres suivants :

```
Auth_type = 2;
```

Cela permet d'autoriser la connexion à la fois en administrateur local et via LDAP.

```
skip = true;
```

Ce paramètre permet de désactiver l'utilisation d'un certificat SSL, autorisant ainsi une connexion sans SSL.

```
//=====
// Authentication Configuration
//=====

/**
 * Define the auth type :
 * - 1 : Local Only
 * - 2 : Local and LDAP
 * - 3 : LDAP Only
 * - 4 : LDAP with SSO
 * - 5 : Always OK, won't ask for user and password
 * - 6 : CAS authentication
 * - 7 : SSO Only (using $_SERVER['REMOTE_USER'] / $_SERVER['HTTP_AUTH_USER'])
 *
 * If LDAP / SSO Basic auth is configured, please configure the LDAP Authentication
 */
define('AUTH_TYPE', 2);

/**
 * For LDAP with SSO auth_type, remove the domain of logins like login@domain
 */
define('SSO_DEL_DOMAIN', false);

/**
 * Auth Insecure LDAP, skip SSL Cert (not recommended)
 * Note : OCS doesn't manage certificate for Ldaps, please edit "/etc/ldap/ldap.conf" to set proper certificate
 */
define('AUTH_LDAP_SKIP_CERT', true);

/**
 * Define password cryptograpy
 * To see all available cryptography, read https://www.php.net/manual/fr/function.hash-algos.php
 */
define('PASSWORD_CRYPT', 'sha256');
```

Sur l'application web :

Activer le paramètre avancé :

[Configuration](#) > [General configuration](#) > [Server](#) > [ADVANCE_CONFIGURATION](#) à **ON**

Configuration LDAP :

[Configuration](#) > [General configuration](#) > [LDAP Configuration](#)

Puis remplir la configuration LDAP :

CONEX_LDAP_SERVEUR

Adresse du serveur Ldap

CONEX_ROOT_DN

Identifiant ROOT

(Laisser à vide pour une connexion anonyme)

CONEX_ROOT_PW

Mot de passe ROOT

(Laisser à vide pour une connexion anonyme)

CONEX_LDAP_PORT

Port du serveur Ldap

CONEX_DN_BASE_LDAP

Nom de la base Ldap + dc

CONEX_LOGIN_FIELD

Nom du champ définissant le login

CONEX_LDAP_PROTOCOL_VERSION

Version LDAP_OPT_PROTOCOL_VERSION

CONEX_LDAP_CHECK_DEFAULT_ROLE

Profil par défaut (vide pour aucun)

CONEX_LDAP_NB_FILTERS

Nombre de filtres LDAP (minimum 1, maximum égal au nombre de profils)

CONEX_LDAP_FILTER1

Premier filtre qui sera utilisé pour évaluer le niveau de sécurité d'un utilisateur LDAP (vide pour aucun)

CONEX_LDAP_FILTER1_ROLE

Administrateur

Si l'utilisateur est trouvé avec le second filtre, réglez ce profil d'utilisateur automatiquement

CONEX_LDAP_SERVEUR Adresse du serveur Ldap	ldap://172.20.133.253
CONEX_ROOT_DN Identifiant ROOT (Laisser à vide pour une connexion anonyme)	cn=Tom,ou=User-OCS,dc=AD-OCS,dc=priv
CONEX_ROOT_PW Mot de passe ROOT (Laisser à vide pour une connexion anonyme)	*****
CONEX_LDAP_PORT Port du serveur Ldap	389
CONEX_DN_BASE_LDAP Nom de la base Ldap + dc	OU=User-OCS,DC=AD-OCS,DC=priv
CONEX_LOGIN_FIELD Nom du champ définissant le login	sAMAccountName
CONEX_LDAP_PROTOCOL_VERSION Version LDAP_OPT_PROTOCOL_VERSION	3
CONEX_LDAP_CHECK_DEFAULT_ROLE Profil par défaut (vide pour aucun)	Administrateurs
CONEX_LDAP_NB_FILTERS Nombre de filtres LDAP (minimum 1, maximum égal au nombre de profils)	1
CONEX_LDAP_FILTER1 Premier filtre qui sera utilisé pour évaluer le niveau de sécurité d'un utilisateur LDAP (vide pour aucun)	&(memberOf=CN=Users,DC=AD-OCS,DC=priv)
CONEX_LDAP_FILTER1_ROLE Si l'utilisateur est trouvé avec le second filtre, réglez ce profil d'utilisateur automatiquement	Administrateurs

Pour des informations qui vous **manqueraient** concernant l'installation de LDAP :

<https://wiki.ocsinventory-ng.org/04.Management-console-and-its-advanced-features/Synchronization-between-OCS-and-LDAP/>