

HowTo : CamTrace – Support LDAP

Principe d'utilisation de LDAP dans CamTrace.

Gestion de l'authentification

Un nouvel utilisateur déclaré dans CamTrace peut avoir son mot de passe géré au niveau d'un annuaire LDAP. Lors de la création de l'utilisateur, il suffit de préciser que le serveur LDAP déclaré gère l'authentification.

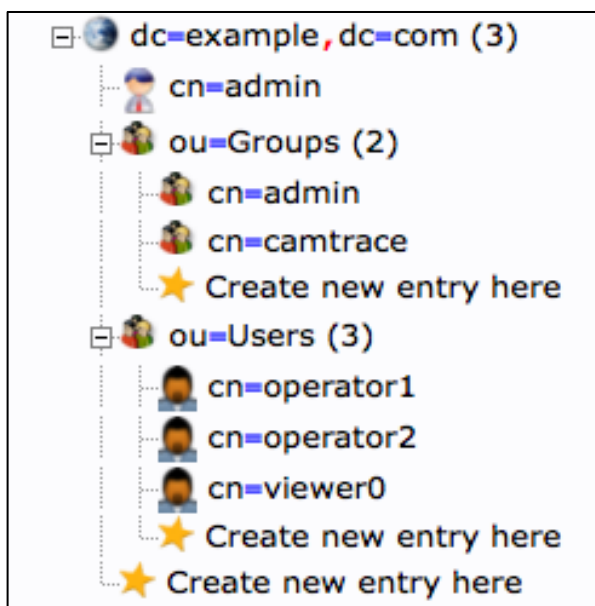
Gestion des groupes d'utilisateurs

Lors de la création d'un profil dans CamTrace, il est possible d'y associer un « groupe LDAP » (un chemin sur un serveur LDAP). Lorsqu'un utilisateur se connecte sur CamTrace et qu'il n'a pas de compte local, alors le serveur LDAP est interrogé pour vérifier si l'utilisateur existe (identification et authentification) et appartient au « groupe LDAP ». Si oui, l'utilisateur est autorisé à se connecter avec les droits de ce profil dans CamTrace.

Configuration LDAP de CamTrace

Annuaire example.com

Voici un exemple de configuration d'un annuaire LDAP :



Le serveur `dc=example,dc=com` est configuré avec deux Organization Units : `ou=Users` et `ou=Groups`.

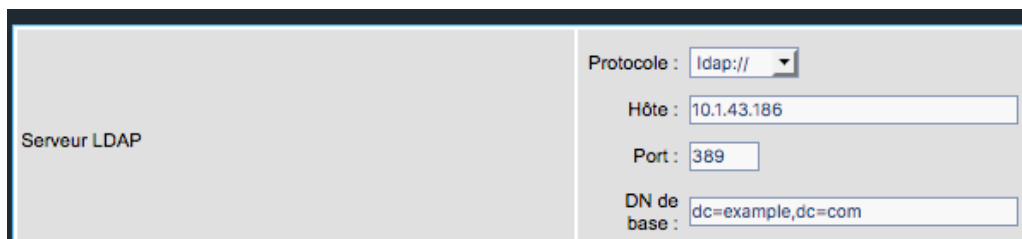
Nous avons 2 groupes de déclarés et 3 utilisateurs.

Seuls `operator1` et `opérateur2` font partis du groupe `camtrace` et nous les voyons dans la section `memberUid` de ce groupe.

cn	camtrace (add value) (rename)
gidNumber	503
memberUid	operator1 operator2

Configuration CamTrace

Pour déclarer l'annuaire LDAP dans CamTrace, en tant qu'administrateur, il faut se rendre dans la section Administration/Configuration, puis sélectionner « Modifier » afin d'éditer la section « Paramètres de l'interface ».



The screenshot shows the 'Serveur LDAP' configuration window. It contains the following fields:

- Protocole : ldap://
- Hôte : 10.1.43.186
- Port : 389
- DN de base : dc=example,dc=com

Après avoir choisi le type de connexion (LDAP ou LDAPS), il faut renseigner l'IP et le port et enfin la Base du serveur LDAP (celle qui servira de base aux requêtes sur l'annuaire), ici : *dc=example,dc=com*.

Utilisateurs - Authentification

Pour le premier exemple, nous allons permettre à l'utilisateur *viewer0* de se connecter au serveur CamTrace avec son mot de passe LDAP.



The screenshot shows the CamTrace login screen with the following fields:

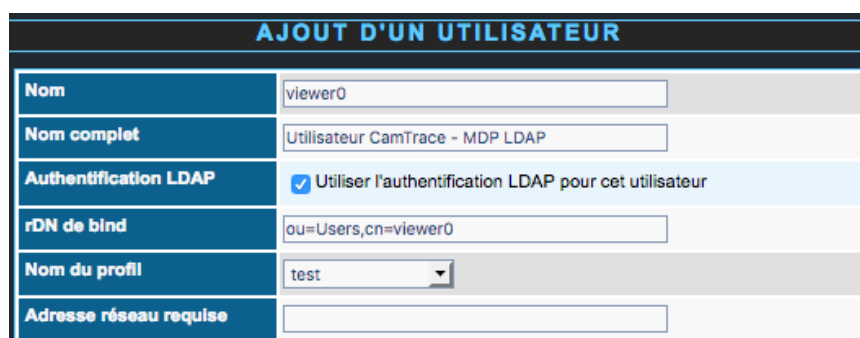
- Nom d'utilisateur : viewer0
- Mot de passe : *****
- Langue : Français

Buttons: Entrer, Annuler, Fermer

Pour cela, dans Administration/Utilisateur, il faut sélectionner « Ajouter un compte ... ».

Le nom d'utilisateur est donc *viewer0* et en cochant la case « Utiliser l'authentification LDAP », nous pouvons renseigner le champ « rDN de bind ». Ce champ correspond au chemin relatif LDAP qu'il faut suivre (à partir de la base entrée dans la configuration) sur le serveur LDAP pour vérifier que l'utilisateur *viewer0* existe et que son mot de passe est bien celui qui sera entré par l'utilisateur.

Nous ajoutons donc le chemin vers le user *viewer0*, soit : *ou=Users,cn=viewer0*.



The screenshot shows the 'AJOUT D'UN UTILISATEUR' form with the following fields:

- Nom : viewer0
- Nom complet : Utilisateur CamTrace - MDP LDAP
- Authentification LDAP : Utiliser l'authentification LDAP pour cet utilisateur
- rDN de bind : ou=Users,cn=viewer0
- Nom du profil : test
- Adresse réseau requise : (empty)

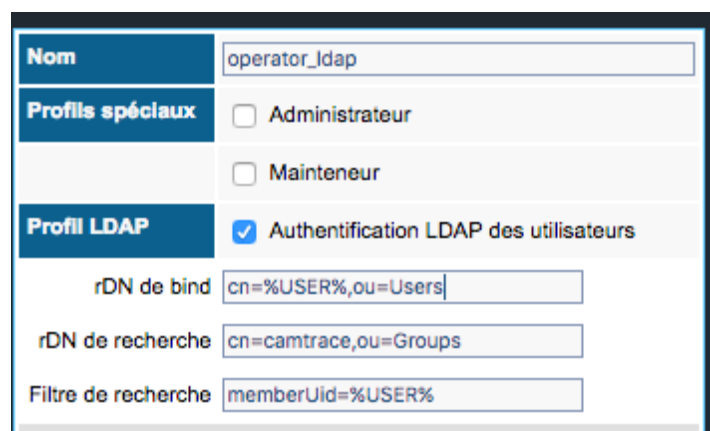
A noter qu'il est aussi possible d'utiliser le mot clé *%USER%* qui est remplacé par CamTrace par le nom d'utilisateur courant lors de la requête sur l'annuaire :

Ou=Users,cn=%USER%

Profils - Identification & Authentification

Le second exemple consiste à permettre aux utilisateurs *operator1* et *operator2* de se connecter à CamTrace avec le profil *operator_ldap*.

Dans Administration/Profils, il faut sélectionner « Ajouter un profil d'utilisateurs ». Tous les champs se configurent comme un profil CamTrace classique, sauf la section « Profil LDAP » qu'il faut cocher et remplir comme suit :



Nom	operator_ldap
Profils spéciaux	<input type="checkbox"/> Administrateur
	<input type="checkbox"/> Mainteneur
Profil LDAP	<input checked="" type="checkbox"/> Authentification LDAP des utilisateurs
rDN de bind	cn=%USER%,ou=Users
rDN de recherche	cn=camtrace,ou=Groups
Filtre de recherche	memberUid=%USER%

Comme précédemment, le champ « rDN de bind » correspond au chemin relatif permettant de valider l'identifiant d'utilisateur, soit *ou=Users,cn=%USER%*, dans lequel on notera l'utilisation du mot clé de substitution *%USER%*.

Le champ « rDN de recherche » correspond au chemin qui permet de sélectionner l'entité (par exemple le groupe) auquel doit appartenir l'utilisateur, ici, *ou=Groups,cn=camtrace*. L'appartenance à cette entité est vérifié par le « filtre de recherche », ici, *memberUid=%USER%*.

Ces deux champs (rDN & filtre de recherche) sont les seuls qui déclarent l'appartenance pour un utilisateur qui se connecte à CamTrace au profil *operator_ldap* et il n'est pas nécessaire de déclarer *operator1* et *operator2* dans les utilisateurs CamTrace, ils seront ajoutés automatiquement lors de leur première connexion.

Filtre de recherche

L'exemple donné est un filtre simple. Dans le détail, sur ce serveur LDAP, *memberUid* est un ObjectClass de type *PosixGroup*. Nous aurions pu utiliser un filtre plus fin qui ressemblerait à ceci :

(&(objectclass=posixGroup)(memberUid=%USER%))

LdapSearch / RFC4515

De manière générale, les filtres des requêtes LDAP de CamTrace suivent le format des requêtes de type [ldapsearch](#), qui respectent la [RFC4515](#). Il y a de nombreuses ressources sur Internet qui permettent de trouver des exemples correspondants à différents cas de figure en utilisant des mot clés comme : ldapsearch ldap group active directory.

Remarques

Suppression d'un compte

Si un utilisateur est supprimé dans l'annuaire LDAP, il ne pourra plus se connecter sur le serveur CamTrace. Toutefois, son compte n'est pas supprimé dans CamTrace et il est alors possible de soit :

- supprimer le compte dans CamTrace ;
- transformer le compte en un compte local.

Pour cela, il suffit de décocher les cases LDAP dans les profils LDAP ou dans les comptes utilisateurs LDAP.

Cache d'authentification

Afin d'éviter de faire de trop nombreuses requêtes sur l'annuaire LDAP, CamTrace cache pendant une heure l'authentification de l'utilisateur. Ceci signifie que la propagation d'un changement de mot de passe ou la suppression d'un compte dans l'annuaire peut prendre jusqu'à une heure avant d'être prise en compte par CamTrace.