

Zéphir - Scénario #37632

LDAP : mise en place du compte de lecture du LDAP

08/09/2026 14:49 - Laurent Joly

Statut:	Nouveau	Début:	
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	0%
Catégorie:		Temps estimé:	0.00 heure
Version cible:			
Description			
Bonjour,			
Le mode anonyme du LDAP a été supprimé, le zephir a besoin de se connecter avec un compte lecture seule au ldap.			
Proposition de modification :			
Dans le genconfig :			
Création des variables :			
• ldap_reader_password • ldap_reader_anonyme (oui/non)			
<pre><variable name='ldap_reader_anonyme' type='oui/non' description="LDAP en mode anonyme"> <value>non</value> </variable> <variable name='ldap_reader_password' type='password' description='Mot de passe de l'utilisateur de lecture des comptes LDAP'></pre>			
/usr/lib/python3/dist-packages/zephir/config.py			
après la ligne ADRESSE_LDAP (ligne 122), ajout de :			
<pre>LDAP_READER = conf.get_creole("ldap_reader") LDAP_READER_PASSWORD = conf.get_creole("ldap_reader_password") LDAP_READER_ANONYME = conf.get_creole("ldap_reader_anonyme")</pre>			
Service Zephir-web			
fichier : /usr/lib/python3/dist-packages/zephir/web/template/page.py			
Ajout après le result=query.search_s ligne 108			
<pre>if config.LDAP_READER_ANONYME == "oui": query.simple_bind_s(config.LDAP_READER, config.LDAP_READER_PASSWORD)</pre>			
Service Zephir (backend)			
fichier : /usr/lib/python3/dist-packages/zephir/backend/xmlrpcceole.py			
Ajout après le result=query.search_s ligne 106			
<pre>if config.LDAP_READER_ANONYME == "oui": query.simple_bind_s(config.LDAP_READER, config.LDAP_READER_PASSWORD)</pre>			

Des éléments permettant de déclarer un compte reader avaient notamment été ajoutés dans [eole-annuaire](#) dans le cadre d'Envole (cf. [#10498](#)) mais l'utilisation de tels éléments n'a jamais été codée sur Zéphir :

https://eole.ac-dijon.fr/documentations/2.10/completes/HTML/ModuleZephir/co/03-annuaire_1.html#ycN60

L'utilisation d'un fichier pour stocker le mot de passe pose un soucis de droits (les services Zéphir tournent en nobody).

À voir si on peut conserver ce mode de fonctionnement (lecture avant le "su", gain de droits au moment de la lecture, déplacement/copie du fichier avec des droits adaptés...) ou si on utilise une variable "password" comme proposé ou encore une autre solution...

Voir avec les utilisateurs mais, je verrai plutôt Zéphir >= 2.9.0

+ Prévoir une maj de la doc

Pour tester, on peut utiliser un Scribe comme dans le test squash "ZE-T09-001 - Utiliser Zéphir avec un annuaire distant" mais en passant la variable "Utilisateur autorisé à accéder à distance au serveur LDAP" (ldap_restrict_access) à "authentié", cf.

<https://eole.ac-dijon.fr/documentations/2.10/completes/HTML/ModuleScribe/co/23-configurationServeurLDAP.html>

Historique

#1 - 08/09/2026 15:49 - Joël Cuissinat

- Description mis à jour

#2 - 08/09/2026 16:12 - Joël Cuissinat

- Tracker changé de Demande à Scénario

- Description mis à jour

- Début 08/09/2026 supprimé

- Release mis à Carnet de produit Cadolles - MEN

- Points de scénarios mis à 3.0

#3 - 09/09/2026 12:17 - Joël Cuissinat

- Description mis à jour

#4 - 09/09/2026 15:30 - Laurent Joly

Correctif :

- il faut bien sûr que le test sur LDAP_READER_ANONYME soit bien sûr égal à NON