Connexion à l'annuaire LDAP de la collectivité

Nous avons déployé une instance de Publik.

Afin de la connecter à votre annuaire nous avons besoin de connaître :

- le nom de votre serveur LDAP, sinon son adresse IP publique
- le « base DN » : chemin de base de votre annuaire — exemple OU=Mairie,DC=ville,DC=fr
- le « bind DN » : login pour un compte en lecture — exemple CN=ldapReadForGRU,OU=System Users,DC=ville,DC=fr ou simplement un login
- le « bind password » : mot de passe du compte en lecture
- un filtre éventuel : typiquement pour réduire la liste des comptes à importer — exemple (&(objectClass=user)(service=voirie))

Pour limiter les comptes importés à un groupe, merci de nous fournir le DN de celui-ci, il sera ajouté au filtre.

Tests

Pour que nous puissions tester le bon fonctionnement de la connexion, il faudra nous fournir un compte de test, voire plusieurs s'il faut tester le bon approvisionnement des groupes.

Sécurisation

Nous devons accéder à l'annuaire de manière sécurisée (c'est à dire chiffrée). Cela s'obtient :

- soit en utilisant l'extension StartTLS sur le port standard 389/tcp
- soit en utilisant la connexion non standard LDAPS (S pour SSL) sur le port 636/tcp

Note : si vous utilisez Active Directory, les deux manières de chiffrer la communication (StartTLS ou LDAPS) sont supportées. Voir https://msdn.microsoft.com/en-us/library/cc223502.aspx et https://www.worteks.com/fr/2020/03/20/signature-ldap-obligatoire-dans-active-directory-ce-qui-change-pour-vos-applications/. Voir aussi https://www.arsouyes.org/blog/2020/35_LDAPs_Active_Directory/ et https://www.arsouyes.org/blog/2020/36_LDAPs_vs_starttls/

L'accès peut être limité aux adresses IP des sites Entr'ouvert :

- production : 5.196.106.224 91.134.171.1 145.239.124.40 et 5.135.221.17
- recette : 193.70.65.200 51.255.136.116 178.32.21.252 et 94.23.114.108

Certificat serveur

L'utilisation d'un certificat auto-signé est impossible.

Si votre certificat serveur est signé par une autorité locale (non reconnue classiquement), il faudra fournir la **chaîne de certification** (l'ensemble des certificats des autorités signatrices, jusqu'à la racine).