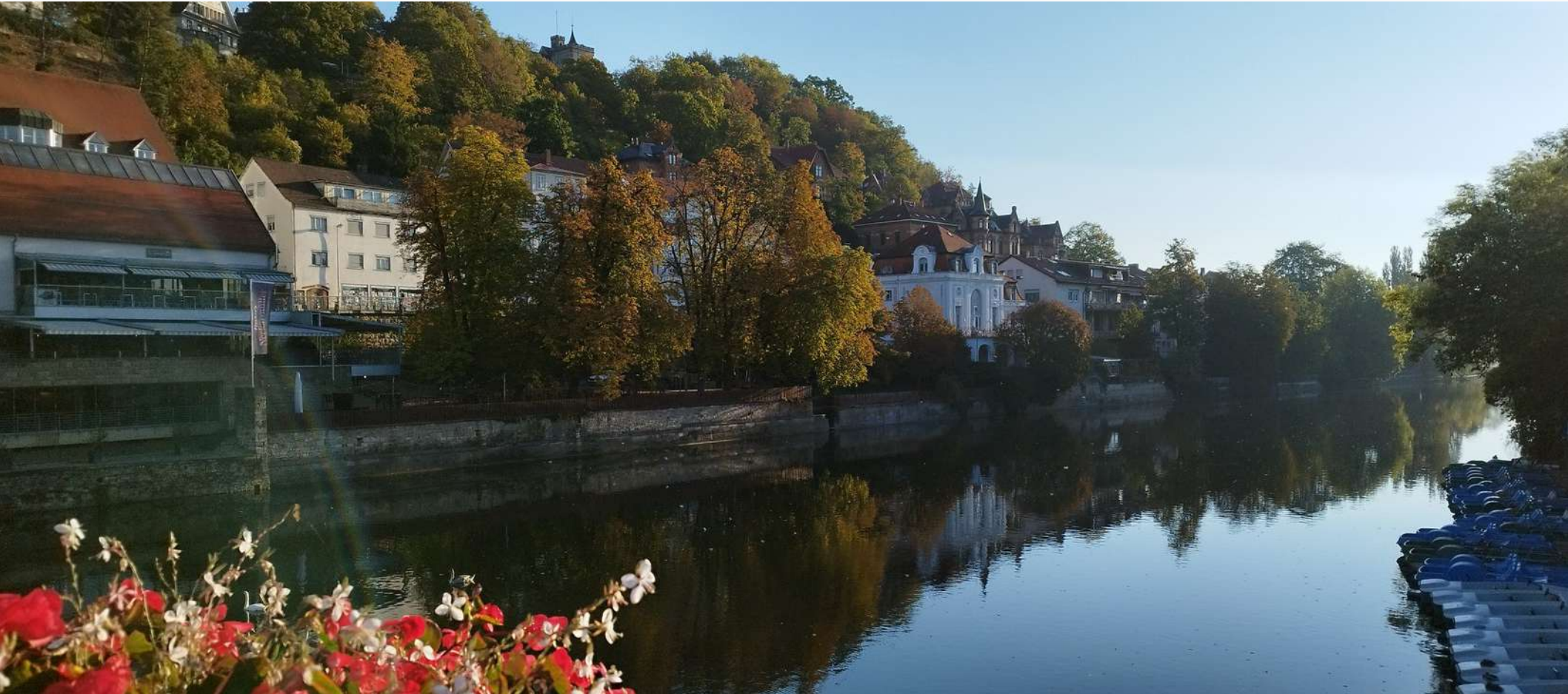


Retour sur la LDAPCon 2026



19 octobre 2026
Paris

Bienvenue à Tübingen





Programme du mercredi

- Quoi de neuf en OpenLDAP 2.7
- Apache Directory, The State of the Union
- LDAP Tool Box, projet open-source pour la gestion d'OpenLDAP et AD
- GOsa² – le vieux chien est toujours en vie !
- Choisir LDAP comme la source de vérité d'Ansible
- slaptain, l'opérateur Kubernetes OpenLDAP multi-site multi-master
- Rendre le LDAP analysable : modernisation jldap et traçage des opérations LDAP avec OpenTelemetry
- Test de charge OpenLDAP avec JMeter



OpenLDAP 2.7

- La version 2.6 est en maintenance seule
- OpenLDAP 2.7 :
 - Overlay ppolicy : attribution dynamique, rehash des mots de passe au moment du bind
 - Suppression de back-perl et back-sql
- LMDB 1.0 : page level encryption, page size configurable, taille des clés plus adaptées à des grands RDN et attributs multi-valués, backup incrémental
- LMDB 1.1 (futur) : Support de recno (nb d'enregistrements dans la table), standalone LDAP data model (comme SQLite pour le SQL)



Apache Directory



- LDAP API 2.1.9 annoncée début Octobre 2026
- Apache Directory Server 2.0.0-AM28 en cours de finalisation
- Apache Directory Studio 2.0.0-RC1 en cours de finalisation
- De gros chantiers en cours:
 - Sécurité (6 CVEs sur LDAP API, d'autres à venir)
 - Corrections (près de 200 anomalies à corriger)
 - Fiabilisation de la base de données

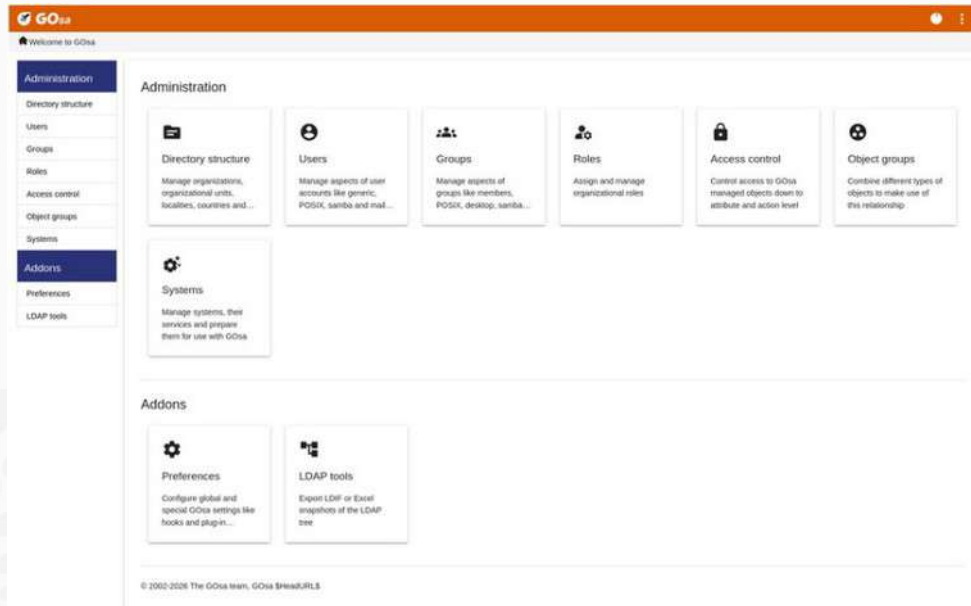


LDAP Tool Box

- Présentation du projet LTB et de ses outils
 - Paquets OpenLDAP
 - Scripts de supervision
 - CLI OpenLDAP
 - Self Service Password
 - White Pages
 - Service Desk



GOSA²



- interface web de gestion d'annuaire
- Projet originel dont est issu FusionDirectory
- démarré dans les années 2000
- à l'arrêt à partir de 2015
- reprise du projet il y a peu, nettoyage du code et remise à jour (PHP 8.1, composer,...)



LDAP comme backend Ansible

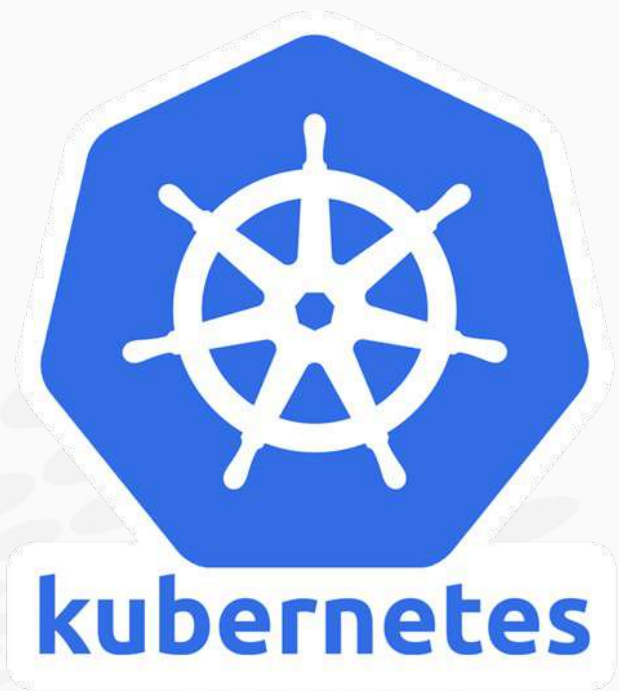
- idée expérimentale : structure stockée dans l'annuaire LDAP pour gérer toutes les variables nécessaires à ansible :
 - inventaire
 - hosts
 - groups
 - variables associées
- une collection spéciale d'ansible récupère ces informations dans le LDAP
- problématiques posées en séance
 - multiples environnements ? (prod, preprod)
 - isolation des secrets dans une autre source de vérité



A N S I B L E



Slaptain



- Kubernetes Operator for Multi-Site Multi-Master OpenLDAP
- 7 types
 - **SlapdMesh** : topologie, définit comment les sites se comportent entre eux
 - **SlapdCluster** : gère les choses qui tournent : pods, volumes, services, TLS, nb de réplica, nb de consumers
 - **SlapdDatabase** : suffixe, ACLs,...
 - **SlapdSchema**
 - + 3 types pour les **backups** et **restore**
- état : tourne en prod chez le concepteur, mais projet jeune

Rendre le LDAP analysable

- modernisation de jldap
- traçage des opérations LDAP avec OpenTelemetry
- Problématique : besoin d'un identifiant commun pour relier les logs d'application, LDAP, et de BDD
- OpenTelemetry définit une en-tête HTTP pour propager cette information : **traceparent**
- En LDAP, il existe un contrôle étendu : **LDAP Session Tracking Control**
- Le conférencier a créé le sien : **LDAPSessionTrackingCarrier**
- Implémentation :
 - Client : injection de la trace
 - Serveur : extraction de la trace



Tests de charge OpenLDAP



- **SLAMD** : framework java mature pour des tests de charge LDAP
 - La version Oracle est morte
 - utiliser la version « ressuscitée » basée sur tomcat : <https://github.com/dirmgr/slamd>
 - gestion multiples machines clientes
 - plusieurs protocoles
- **JMeter** : Application générique de test de charge en Java, initialement conçu pour HTTP
 - out of the box : très bien pour les cas simples
 - Sinon, il faut coder son propre test
 - ldap-load-gen : générateur de charge LDAP basé sur JMeter et Apache Fortress

Programme du jeudi

- LDAP et le paysage Python
- scmid : un framework RUST pour rendre des produits compatibles avec SCIM
- Retour sur l'usage de la politique de MdP OpenLDAP en 2026 et évolutions possibles
- Étude de cas d'entreprise : intégration de 389DS avec PrivacyIdea
- Table ronde – gérer un projet Open Source dans un univers « infesté par l'IA »
- Histoires d'intégration d'OpenLDAP avec le monde moderne
- Présentation courte : « Les lois de la Civilisation, backend LDAP pour un projet ludo-éducatif »



LDAP et le paysage Python

- 3 librairies :
 - **python-ldap**, démarré en 1998
 - Proche de la librairie en C
 - bon support des contrôles
 - asyncio : pas exposé par défaut
 - **ldap3**, démarré en 2013
 - philosophie différente : commencer par définir le serveur, les options TLS,...
 - contraintes pour le support des contrôles
 - pas d'async
 - **bonsai**
 - support partiel des contrôles
 - async supporté en standard



scimd: framework SCIM en REST

- **SCIM** = System for Cross-domain Identity Management
- protocole de (dé)provisionnement d'utilisateurs
 - schéma commun pour les utilisateurs et les groupes
 - protocole REST pour les gérer
 - SCIM 2.0 = RFC 7643 + 7644
- **scimd**
 - projet sidecar pour interconnecter des applications qui ne parlent pas SCIM
 - écrit en RUST
 - statut : à n'utiliser que pour des tests





Feedback on OpenLDAP Password Policy usage in 2026 and possible evolutions



Politique de MdP OpenLDAP

- politique = ensemble de règles autour du MdP
 - robustesse
 - durée
 - verrouillage
- pas de normalisation universelle
 - recommandation NIST
 - brouillon IETF « behera-ldap-password-policy »
- implémentation : overlay **ppolicy**, extension avec **ppm**
- nouveautés en OpenLDAP 2.7
 - **Règles de politiques** de MdP
 - **Rehash** du MdP à l'authentification
- Andrew Findlay : MdP en désuétude, normalisation vers politique de compte plutôt que politique de MdP
- Onrek Kuznik : propagation des attributs internes de la ppolicy grâce à l'overlay chain

Precedence of ppolicy assignment

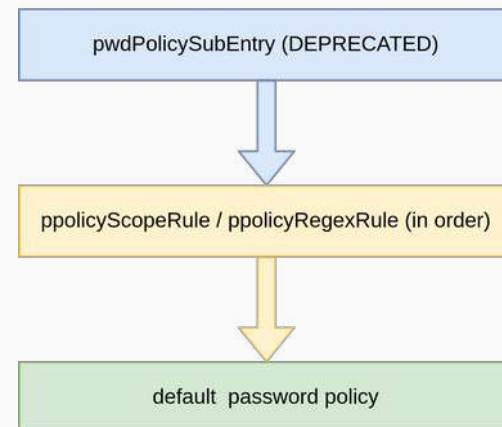
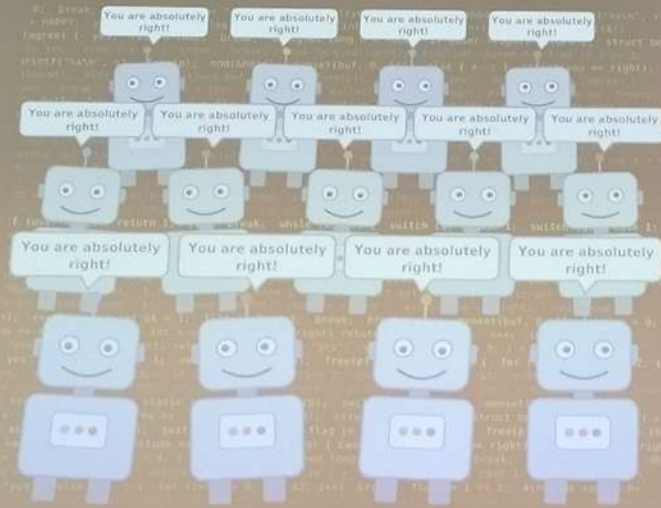


Table ronde « Open Source et IA »

- Dans quelle mesure la qualité des contributions a changé avec l'IA ?
- Est-ce que les contributions sont pertinentes, coûtent-elles cher ?
- Dans quelle mesure les outils IA ont amélioré vos projets ?
- L'impact de l'IA risque-t-il de rendre les contributeurs moins compétents ?
- Comment s'assurer que les nouveaux contributeurs connaissent la base de code ?
- Si vous deviez édicter une règle sur l'utilisation de l'IA dans votre projet, quelle serait-elle ?



Managing an Open Source Project in an AI “infested” universe





MERCI DE VOTRE ATTENTION

