LemonLDAP::NG dans un contexte Education Recherche

"Retour d'expérience sur la mise en place de LemonLDAP::NG dans un contexte de l'enseignement superieur et de Recherche"

Antoine Gallavardin

INRAE > DSI > AM

20 Octobre 2025 - Club utilisateur WORTEKS"

Tables des matières

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

L'institut INRAE

- Institut national de recherche pour l'agriculture, l'alimentation et l'environnement
- 18 centres régionaux
- Environ 12000 employés

L'auteur

- Administrateur système dans l'Enseignement Supérieur et la Recherche
- Architecte "Annuaire et authentification" à INRAE
- Responsable technique de l'environnement "Access Management"
- contact : antoine.gallavardin@inrae.fr

Plan

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Une fusion et des impacts

Contexte

En 2020, L'INRA et l'IRSTEA fusionnent pour donner INRAE

- coté INRA : un projet IAM en cours depuis quelques années
- La fusion devient une opportunité pour accélérer le projet

Les impacts

- Changement de domaine institutionnel : ***inrae.fr*** et donc d'identifiant
- Convergence des identités et des méthodes d'authentification des applications
- Refonte en profondeur de la gestion des identités avec 2 projets distincts
  - IDM : Modernisation du référentiel des identités et leur diffusion
  - **AM** : Mise en place des services d'authentification pour les utilisateurs

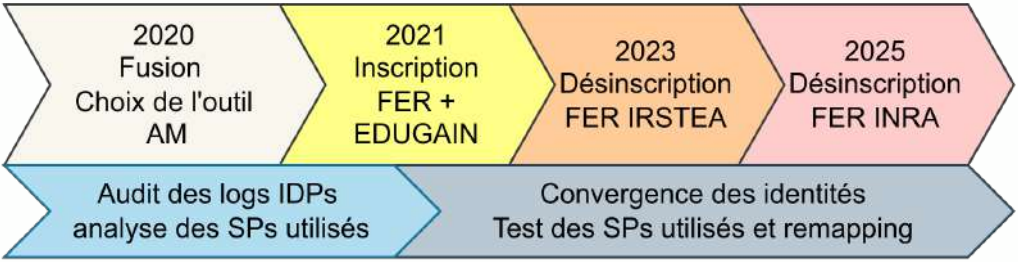
RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Stratégie et calendrier

La stratégie AM

- Raccorder **toutes** les applications (institutionnelles et scientifiques) sur le portail d'authentification
- Promouvoir l'authentification ET l'identification (diffusion d'attributs)
- Support d'OpenIDConnect
- L'authentification LDAP devient l'exception.

Calendrier



L'offre de service de départ

Fournisseur d'identité local

- Fourniture de l'authentification ET identification (via attribut)
- Support OpenIDConnect en vue d'intégrer ProConnect
- Transmission du token d'authentification entre les différents protocoles (Fonctionnalité Single Sign On)
- Déclaration obligatoire des applications

Fournisseur d'identité pour les fédérations

- Inscription dans les différentes fédérations SAML : FER + EDUGAIN
- Usage des standards :
  - d'échange : SAML en mode fédéré
  - de codification de l'information : Schémas EduOrg / Schac / Supann
- Suivre au plus près les recommandations RENATER (opérateur de service et réseaux de l'enseignement supérieur)

Plan

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Pourquoi LemonLDAP::NG ?

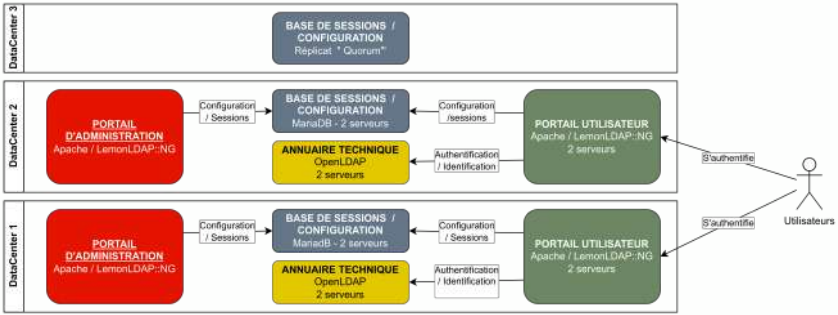
Rapide description

- Fork de LemonLDAP par la gendarmerie nationale en 2004
- Écrit en Perl
- Logiciel Libre hébergé sur la forge du consortium OW2 https://gitlab.ow2.org/lemonldap-ng
- Version en 2.21.1 en juin 2025

Pourquoi LemonLDAP::NG ?

- Déjà utilisé par IRSTEA à l'époque
- Support natif des différents protocoles de SSO : CAS / OIDC / SAML
- Interconnexion possible avec la FER
- Support disponible via une société de service
- modulable (source de donnée, pile logicielle)

Schéma rapide



Résilience

- Load Balancing sur les portails et interface d'administration
- Cluster MariaDB / Galera pour les bases de données
- Réplicat classique d'annuaire LDAP OpenLDAP

Retour d'expérience sur 4 ans - Infrastructure

Les portails de connexion

- 4 noeuds en frontal : c'est très confortable
- Fonctionnalité sous utilisées (possibilité d'augmenter l'expérience utilisateur)
- Des logs multilignes compliqués à parser

Le cluster de base de données

- Le point "faible" en parti du à notre implémentation
- Toujours solliciter le même serveur pour assurer un bon suivi des accès
- Des sessions SAML parfois incomplètes remplissant la base
- Des tailles de champs de table à augmenter

Le portail d'administration

- Très complet et complexe
- Très long à charger avec un nombre de configurations croissants
- Des purges régulières à prévoir

Retour d'expérience sur 4 ans - Administration

Méthode d'administration

- Par interface web : pour des petites opérations simples
- Par import de fichier yaml : pour des configurations en masse en local
- Par API : pour des configurations en masse à distance

Les mises à jours

1. Lecture des releases notes
2. *apt-get update && apt-get upgrade*
3. Redémarrage des services

Quelques difficultés

- Traduire des configurations Shibboleth-idp => LemonLDAP::NG
- Gérer des différences d'implémentation (différences de gestion pour les attributs obligatoires)
- Rendre les configurations génériques pour faciliter la gestion

Retour d'expérience sur 4 ans - Évolutions Logicielles

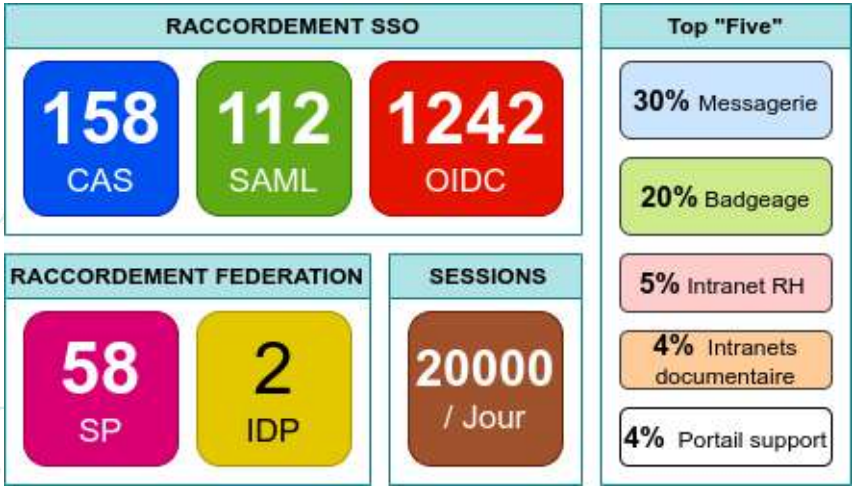
Évolutions Logicielles

- "Lazy Loading" : chargement à la volée des métadonnées des SP et non au démarrage (permet d'alléger la configuration stockée)
- Demande du support du protocole MDQ (Meta Data Queueing)
- Gestion totale du cycle de vie du double facteur via des APIs
- Le support OIDC pour sharepoint
- Quelques corrections de bugs

Évolutions Techniques

- Activation du MFA
- Activation du mode "combinaison" : Interrogation séquentielle de plusieurs annuaires LDAP

Quelques Chiffres



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Plan

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

LemonLDAP::NG et au-delà

LemonLDAP::NG une brique essentielle

LemonLDAP::NG devient une brique essentielle de l'offre d'authentification et d'identification.

Le principal défi est de le rendre encore plus :

- Transparent: Être obligatoire avec le minimum d'interférences avec le SI
- Incontournable: Toute application doit s'appuyer sur lui pour authentification

Transparence vers l'externe

L'écosystème des fédérations

- Ensemble de SP et IDP constitue une fédération SAML
- 1 fédération peut être contenue dans une autre
- Dans le cadre d'INRAE
  - Fédération Éducation Recherche : 360 IDP et 1250 SPs
  - Fédération EduGain : 6155 IDP et 3862 SPs
  - Fédération Locale : 5 IDP et 3 SPs
- Cadre technique (logiciel supporté shibboleth-idp / guichet d'enregistrement)

Beaucoup de partenaires et autant de choses à éclaircir

- Authorization Context (4 par défaut) et leur interprétation
- Différence de traitement sur l'attribut demandé (attribut inexistant => attribut refusé)
- Autres "traductions" de configuration à venir (shibboleth <=>LL:NG) ...

Transparence vers l'interne

Transparence interne

La transparence LEMONLDAP::NG en interne n'est plus à démontrer

- Macro pour la construction de champs à la volée
- Support avancé des protocoles
- Paramétrage fin par application

MAIS

Des défis à venir

- Organiser le suivi des configurations (Ajout / suppression)
- Éviter les configurations trop spécifiques
- Développer des outils annexes pour piloter en masse des configurations

Encore plus incontournable ?

Comment pousser l'authentification unique ?

Le besoin

Faciliter l'onboarding d'applications

- Création de modèle de configuration
- Déléguer la création à d'autres acteurs (via interface ou API)

Les problématiques

- Pas de granularité de droits de l'interface d'admin
- Pas de modèle possible
- Pas d'extension native du modèle de données

Un début de solution

- LemonLDAP::NG : Richesse de l'API
- Création d'une application dédiée qui push sur l'API LemonLDAP : le guichet

le guichet local

Pour les administrateurs : Établir des référentiels

- d'attributs pilotés et diffusés pour des applications tierces
- d'applications inscrites dans le SSO
- de configurations d'applications pour diffusion via API
- des responsables d'applications

Pour les responsables d'application : Être autonome

- Délégation de création et modification de configuration.
- Usage de modèle de configuration par protocole ou type d'application
- Complétion des référentiels (Description / gestionnaire)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Plan

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Remerciements et Questions

Remerciements

- à Worteks pour avoir accepté cette intervention

Des questions ?

Si je peux y répondre

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

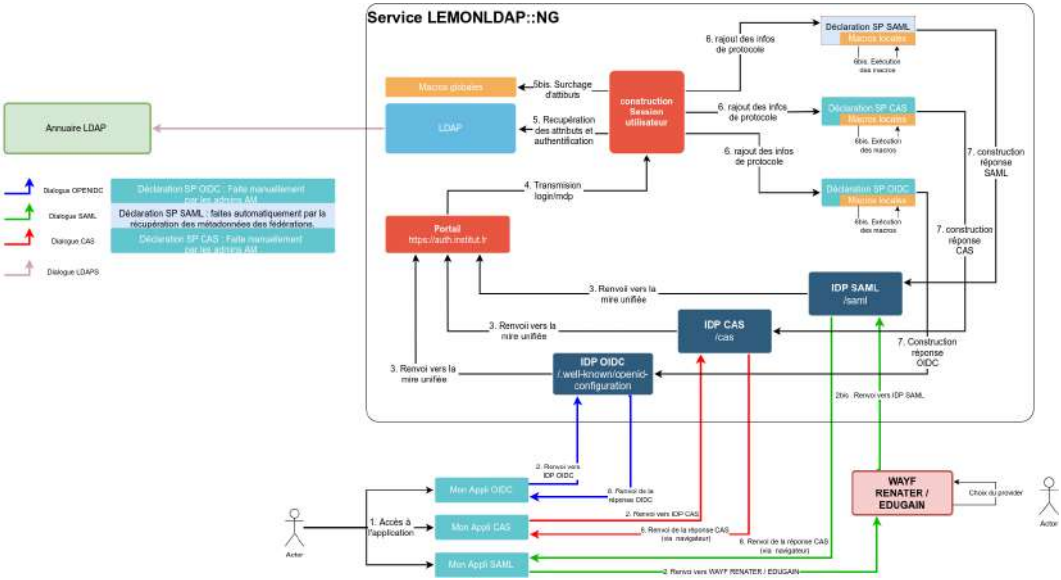
Plan

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Bibliographie

- LemonLDAP::NG : https://lemonldap-ng.org
- Le plugin de gestion LemonLDAP::NG pour le guichet https://github.com/gallak/fusiondirectory-plugins-access

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité


Service LEMONLDAP::NG
Annuaire LDAP
LDAP
Macros globales
5bis. Surchage d'attibuts
5. Recupération des attributs et authentification
construction Session utilisateur
8. rajout des infos de protocole
6. rajout des infos de protocole
6. rajout des infos de protocole
Déclaration SP SAML
Macros locales
6bis. Exécution des macros
Déclaration SP CAS
Macros locales
6bis. Exécution des macros
Déclaration SP OIDC
Macros locales
6bis. Exécution des macros
7. construction réponse SAML
7. construction réponse CAS
7. Construction réponse OIDC
4. Transmission login/mdp
Portail
https://auth.institut.fr
3. Renvoi vers la mire unifiée
3. Renvoi vers la mire unifiée
3. Renvoi vers la mire unifiée
IDP SAML
/saml
IDP CAS
/cas
IDP OIDC
/.well-known/openid-configuration
2bis. Renvoi vers IDP SAML
Dialogue OPENIDC
Dialogue SAML
Dialogue CAS
Dialogue LDAPS
Déclaration SP OIDC : Faite manuellement par les admins AM
Déclaration SP SAML : faites automatiquement par la récupération des métadonnées des fédérations.
Déclaration SP CAS : Faite manuellement par les admins AM
Acteur
1. Accès à l'application
Mon Appli OIDC
Mon Appli CAS
Mon Appli SAML
2. Renvoi vers IDP OIDC
6. Renvoi de la réponse OIDC
2. Renvoi vers IDP CAS
6. Renvoi de la réponse CAS (via navigateur)
6. Renvoi de la réponse CAS (via navigateur)
2. Renvoi vers WAYF RENATER / EDUGAIN
WAYF RENATER / EDUGAIN
Choix du provider
Acteur