

Rapport Étude IAM

Guillaume Risso

29 Janvier 2025

Table des matières

1	Présentation de l'environnement professionnel	3
1.1	Présentation de l'Université de Strasbourg	3
1.2	Présentation de la DNUM	5
1.2.1	Partenaires	5
1.2.2	Services & départements	6
1.2.3	Missions	6
2	Contexte de l'étude	7
2.1	Contexte générale et historique	7
2.2	Enjeux et complexités spécifiques	7
2.3	Méthodologie adoptée	7
3	Selection des solutions évaluées	8
3.1	Critères de sélection des outils	8
3.2	Solutions retenues pour l'étude	8
3.2.1	LemonLDAP : :NG	8
3.2.2	Keycloak	8
3.2.3	MidPoint	8
4	Analyse des solutions SSO/IAM	8
4.1	LemonLDAP : :NG	8
4.1.1	Présentation générale	8
4.1.2	Histoire & contexte d'utilisation	8
4.1.3	Fonctionnalités clés	8
4.1.4	Prérequis & Installation	11
4.1.5	Administration & configuration	11
4.1.6	Performances & consommation de ressources :	13
4.2	Keycloak (RHBK)	14
4.2.1	Présentation générale	14
4.2.2	Histoire & contexte d'utilisaton	14
4.2.3	Fonctionnalités clés	14
4.2.4	Prérequis et Installation	14
4.2.5	Prérequis & installation	15
4.2.6	Administration & configuration	15
4.2.7	Performances & consommation de ressources	17
4.2.8	OU INTEGRER :	18
4.3	MidPoint	19
4.3.1	Présentation générale	19
4.3.2	Intérêt dans le cadre post-étude	19
4.3.3	Liens possibles avec LLNG :NG ou Keycloak	19
5	Banc d'essais & expérimentation	20
5.1	Architecture technique mise en place	20
5.2	Scénarios de test	20
5.3	Difficultés rencontrées	20
5.4	Résultats et observations	20

6	Comparatif des solutions	22
6.1	Tableau comparatif complet :	22
6.2	Tableau comparatif détaillé	23
7	Conclusion	27
7.1	Synthèse de l'étude et recommandation	27
7.2	Mon avis personnel sur les outils	27
7.3	Retour sur l'année d'alternance	27
7.3.1	Apports techniques	27
7.3.2	Apports professionnels et personnels	27
8	Annexes	27

1 Présentation de l'environnement professionnel

1.1 Présentation de l'Université de Strasbourg

Fondée en 1538 par Jean Sturm également appelé Johannes Sturm sous la forme d'un gymnase humaniste, l'Université de Strasbourg (Unistra) est l'une des plus anciennes institutions d'enseignement supérieur d'Europe. Élevée au rang d'université en 1621, elle a traversé les siècles en s'adaptant aux bouleversements politiques et culturels de l'Alsace, oscillant entre influences françaises et allemandes.



Après avoir été divisée en trois entités distinctes dans les années 1970, l'université a été réunifiée en 2009 pour des raisons de visibilité à l'international et d'interdisciplinarité afin de former une institution pluridisciplinaire.

Aujourd'hui, l'Université de Strasbourg compte environ 55000 étudiants, dont plus de 20% d'internationaux, répartis sur 38 composantes et 77 unités de recherche. Elle est membre de réseaux prestigieux tels que la Ligue européenne des universités de recherche (LERU) et la Confédération européenne des universités du Rhin supérieur (EUCOR).

Située au cœur de l'Europe, Unistra se distingue par son engagement en faveur de l'innovation, de l'interdisciplinarité et de l'ouverture internationale, tout en s'appuyant sur un riche patrimoine architectural et scientifique, notamment le Palais universitaire, la Bibliothèque nationale et universitaire, et le Jardin botanique

L'Unistra actuelle dirigé par la récemment élue Frédérique Berrod s'organise donc de cette façon, la Direction du Numérique appartient à une branche de la partie Services et Direction.

L'organigramme général

de l'  **Université de Strasbourg** 

Président

Michel Deneken

Fondation
Université de Strasbourg

Fondation pour la
recherche en chimie

Vice-présidents

Premier vice-président et vice-président Relations avec le monde socio-économique et valorisation : **Michel de Mathelin**

Vice-présidente Formation et parcours de réussite : **Alexandra Knaebel**

Vice-président Recherche, formation doctorale et sciences ouvertes : **Rémi Barillon**

Vice-présidente Prospective et actions stratégiques : **Catherine Florentz**

Vice-présidente Ressources humaines et dialogue social : **Elisabeth Demont**

Vice-présidente Finances : **Frédérique Berrod**

Vice-président Politique numérique et démarche qualité : **François Gauer**

Vice-présidente Europe et relations internationales : **Irini Tsamadou-Jacoberger**

Vice-président Partenariats académiques et gouvernance : **Jean-Marc Planeix**

Vice-président Patrimoine : **Nicolas Matt**

Vice-président Développement durable et responsabilité sociétale : **Laurent Schmitt**

Vice-présidente Egalité, parité, diversité : **Isabelle Kraus**

Vice-président Culture, science-société et actions solidaires : **Mathieu Schneider**

Vice-présidente Vie universitaire : **Angeline Okombi**

Vice-président Politique hospitalo-universitaire et territoriale en santé : **Jean Sibilia**

Principales instances délibératives et consultatives

Conseil académique (CFVU + CR)

Congrès (CA + CFVU + CR + CTE)

Conseil d'administration (CA)

Commission de la formation et de la vie universitaire (CFVU)

Commission de la recherche (CR)

Comité social d'administration de l'établissement (CSAE)

Commission paritaire d'établissement (CPE)

Commission consultative paritaire compétente à l'égard des personnels non titulaires (CCPANT)

Formation spécialisée en matière de santé, de sécurité et des conditions de travail (F3SCT)

Collégiums

Arts - Langues - Lettres

Droit - Administration - Sociétés

Education et formation

Journalisme et études politiques

Sciences

Sciences économiques et management

Sciences humaines et sociales

Sciences - Ingénierie - Technologie

Vie et santé

FORMATION

35 composantes (facultés, écoles et instituts)
qui couvrent 5 domaines de formation :

- Arts, lettres, langues
- Droit, économie, gestion et sciences politiques et sociales
- Sciences humaines et sociales
- Sciences, technologies
- Santé

SERVICES ET DIRECTIONS

Directrice générale des services

Valérie Gibert

39 services et directions :

Rattachés à la Présidence

et à la Direction générale des services :

- Pôle d'appui aux missions Formation - vie étudiante - relations avec les composantes - documentation - internationalisation
- Pôle d'appui aux missions Recherche - innovation - partenariats - valorisation - développement durable - responsabilité sociétale
- Pôle de gestion des ressources

RECHERCHE

66 unités de recherche

(et 13 autres entités : FR, UAR, UMS)

qui se déclinent au sein de 3 grands domaines de recherche :

- Domaine I : Droit, économie, gestion, sciences humaines et sociales
- Domaine II : Sciences et technologies
- Domaine III : Vie et santé

Mis à jour le 25/03/2024

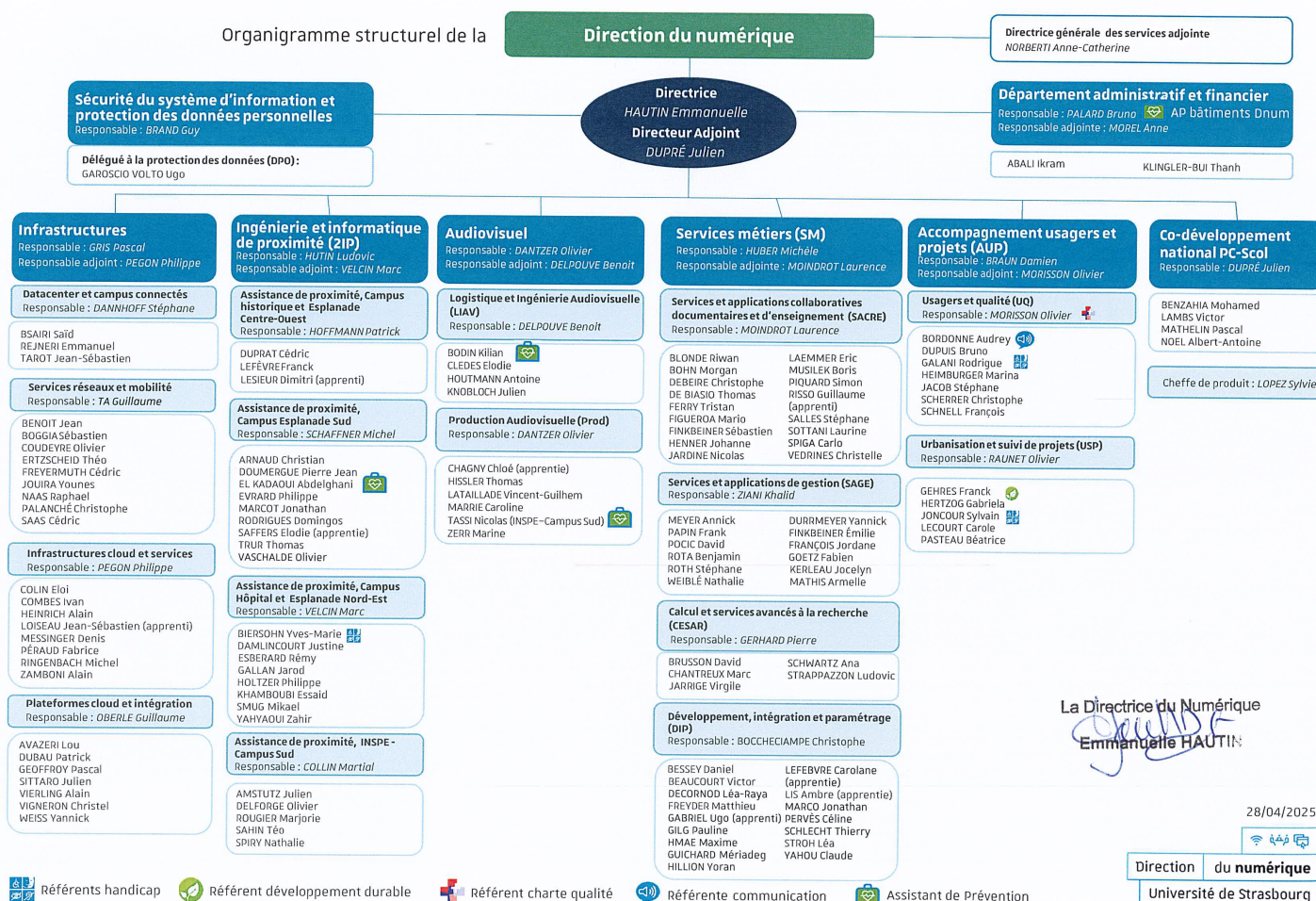
Au sein des services et directions dirigé par Valérie Gibert une branche dénommée "Gestion des ressources" qui a comme directrice Anne-Catherine Norberti apparait et celle ci comprend la Direction du Numérique.



Mise à jour le 24/03/2025

1.2 Présentation de la DNUM

La Direction du Numérique (DNum) dirigé par Emmanuelle Hautin accompagné de Julien Dupré est un service central de l'Université de Strasbourg, contribuant à la définition de la stratégie en matière de système d'information et de développement numérique pour l'université.



Elle initie, organise, met en œuvre puis maintient l'ensemble du système d'information : les infrastructures informatiques et audiovisuelles de l'université mais aussi les sites web, le parc informatique et multimédia de l'établissement et de certains de ces partenaires.

Elle a vocation d'être au plus proche des besoins des usagers et a donc pour mission de rapprocher l'assistance à maîtrise d'ouvrage (AMO) et la maîtrise d'œuvre (MOE). À ce titre, elle assure conseil et expertise auprès des usagers, des directions métiers et des composantes de l'université.

Elle accompagne les usagers à distance par le biais de son support numérique (qui assure une permanence téléphonique 5 jours sur 7 toute l'année), mais aussi à travers le réseau d'informaticiens de proximité, présents dans les composantes et les unités de recherche – réseau qu'elle fédère dans le cadre du projet « Infoprox ».

Elle organise la formation des usagers aux outils numériques et aux applications métiers déployées dans l'établissement, en lien étroit avec l'Institut de Développement et d'Innovation Pédagogiques (Idip) et le Département de Formation Continue de la Direction des ressources humaines (DRH).

1.2.1 Partenaires

La Direction du numérique a aussi depuis longtemps développé des partenariats avec les établissements publics alsaciens et étend sa collaboration vers les partenaires EUCOR et ceux de la Région Grand Est...

Elle est opératrice du réseau OSIRIS pour les 17 établissements partenaires (CNRS, INSA...) depuis maintenant plusieurs décennies.

Elle est opératrice du réseau RAREST (le réseau alsacien pour la recherche et l'enseignement supérieur).

Opératrice aussi de multiples services numériques pour plusieurs établissements d'enseignement supérieur comme la carte Pass Campus, la plateforme pédagogique Moodle, les portails documentaires, les archives ouvertes etc.

Elle contribue au projet DUNE-EOLE, « un engagement pour ouvrir l'éducation » réunissant entre autre les universités de la région Grand-Est.

1.2.2 Services & départements

Parmi ces 8 départements nous y retrouvons le département Services métiers (SM) dirigé par Michèle Hubert ainsi que de Laurence Moindrot.

Ce département comporte de nombreuses équipes, personnellement j'appartient à l'équipe SACRE ou Services et Applications Collaboratives, documentaiRes et d'Enseignement (SACRE) dirigé par Laurence Moindrot et composé de 18 personnes.



1.2.3 Missions

L'équipe SACRE recouvre des domaines tels que la pédagogie, le documentaire, les outils de communications, la gestion des identités et droits d'accès.

Les principales missions menées sont :

- Réalisation du suivi opérationnel des applications transverses en production
- Effectuer une assistance à la maîtrise d'ouvrage pour les projets d'évolution d'applications transverses
- Réalisation / faire réaliser le développement, l'intégration ainsi que le paramétrage des applications transverses
- Mise en oeuvre des solutions retenues (Installation, paramétrages, tests, accompagnement au changement)
- Pilotage des projets (planification et coordination des tâches entre la maîtrise d'ouvrage, les fournisseurs, les autres départements de la DNum)

2 Contexte de l'étude

2.1 Contexte générale et historique

Cette étude a pour objectif de comparer plusieurs solutions d'authentification, dans le but de simplifier et moderniser l'infrastructure actuelle de gestion des identités au sein de l'Université de Strasbourg (Unistra).

Afin de mener cette analyse de manière rigoureuse, différents cas d'usage ont été identifiés, notamment les méthodes de validation d'identité, la prise en charge des protocoles d'authentification (CAS, SAML2, OIDC), la fédération d'identité, ainsi que les possibilités d'évolution de l'infrastructure.

Objectifs de l'étude

Les outils retenus pour cette étude sont les suivants :

CAS v7.2 : version récente du système actuellement utilisé à l'Unistra. Elle propose des fonctionnalités supplémentaires, notamment le support natif de SAML2, renforçant son intérêt en tant que solution évolutive.

Shibboleth IdP 5.1 : également en usage à l'Unistra, principalement pour la gestion du protocole SAML2. Cette version permet désormais d'envisager également l'utilisation des protocoles OIDC et CAS, ce qui étend son champ d'application.

Keycloak : solution moderne, open source, prenant en charge nativement SAML2 et OIDC mais aussi CAS via un plugin. Elle pourrait constituer une alternative complète aux solutions précédentes, tout en offrant des fonctionnalités avancées de gestion des accès.

LemonLDAP : :NG : solution française open source, compatible avec CAS, SAML2 et OIDC. Elle se positionne également comme une alternative crédible et intégrée, avec une approche orientée simplicité.

2.2 Enjeux et complexités spécifiques

Chaque outil a été étudié en fonction de sa compatibilité avec l'existant, de la facilité de déploiement, de la prise en main, de la couverture fonctionnelle, ainsi que de sa capacité à évoluer dans un contexte fédéré (par exemple via Renater).

À l'issue de cette étude, une recommandation sera formulée, mettant en avant la solution jugée la plus adaptée aux besoins actuels et futurs de l'Université.

2.3 Méthodologie adoptée

....

3 Selection des solutions évaluées

3.1 Critères de sélection des outils

3.2 Solutions retenues pour l'étude

3.2.1 LemonLDAP : :NG

3.2.2 Keycloak

3.2.3 MidPoint

4 Analyse des solutions SSO/IAM

4.1 LemonLDAP : :NG

4.1.1 Présentation générale

4.1.2 Histoire & contexte d'utilisation

LemonLDAP : :NG est une solution open source de gestion de l'identité et d'authentification unique SSO, développée en France principalement en Perl, mais aussi en JavaScript par des agents du service public. Elle permet aux utilisateurs de se connecter une seule fois pour accéder à plusieurs applications web. Conçue pour simplifier la gestion des identités et des accès, elle centralise l'authentification pour différents services tout en offrant une sécurité renforcée.

Le projet a été repris en 2004 par la Gendarmerie nationale pour gérer l'authentification de ses agents. Depuis, il a évolué pour devenir un outil largement utilisé dans diverses institutions publiques et entreprises privées. LemonLDAP : :NG continue de se développer, intégrant de nouveaux protocoles de sécurité et répondant aux besoins croissants des organisations en matière de gestion des identités.

Actuellement, les organisations principales contribuant au projet sont la Gendarmerie Nationale ainsi que la société Worteks.

LemonLDAP : :NG est utilisé essentiellement par des francophones, déployé à des fins personnelles, jusqu'à sa mise en place de service d'authentification pour des milliers d'utilisateurs majoritairement dans l'administration publique (Université de Limoges, Police Nationale...).

Concernant les mises à jour, les majeures sont espacées de plusieurs années (2 ans en moyenne), les mineures d'approximativement tous les deux mois et enfin les correctives le plus rapidement en fonction du besoin.

Pour les ressources, il y a très peu d'informations en ligne autre que la documentation qui est très claire ainsi que le Git des développeurs.<https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng>

De nombreux plugins sont déjà intégrés dans LemonLDAP cependant, il nous laisse l'opportunité d'en créer de nouveaux (en Perl) mais, il est possible de contacter un développeur de LemonLDAP afin de mettre en place une fonctionnalité en plus (payant).

4.1.3 Fonctionnalités clés

- LDAPv2/v3 et Active Directory

La partie LDAP est très poussée, permettant par exemple de s'appuyer sur la LDAP Password Policy pour la politique de mot de passe, lecture des groupes de l'utilisateur.

- CAS : LemonLDAP : :NG est compatible avec les versions 1,2 et 3 en partie (échanges d'attributs).

Il est possible de faire du :

- client (service CAS)
- serveur (serveur CAS)

Le mode client va permettre de déléguer l'authentification (avec le protocole CAS) à un serveur tiers via un module Perl.

- SAML : LemonLDAP : :NG ne supporte pas la version 1.0 du protocole SAML cependant, il supporte tout à fait la 2.0.

Il est possible de faire du :

- client (Service Provider)
- serveur (Identity Provider)

Avec la possibilité d'implémenter des fédérations d'identités tel que Renater dans Identity Provider : <https://lemonldap-ng.org/documentation/2.0/renater.html>

- OpenID Connect : LemonLDAP : :NG supporte le protocole OIDC

Il est possible de faire du :

- client (Service Provider)
- serveur (Identity Provider)

- Sociales, protocoles utilisés OAuth/OIDC (Facebook, X, Github)

- RADIUS : FreeRadius...

- Kerberos

- TOTP (Time-Based One-Time Password)

Utilise des applications comme FreeOTP ou Google Authenticator pour générer des codes temporaires basés sur le temps. Ces codes sont synchronisés avec le serveur et changent toutes les 30 secondes.

- WebAuthn

Standard moderne pour l'authentification sans mots de passe. Utilise des dispositifs biométriques ou physiques (comme les capteurs d'empreintes digitales ou clés USB) pour une authentification sécurisée.

- Mail

Envoie un code ou un lien de vérification à l'adresse e-mail de l'utilisateur pour valider son identité.

- Yubico (Yubikey)

Utilise des clés physiques Yubikey, qui génèrent des OTP ou facilitent l'authentification via NFC/USB pour une sécurité renforcée.

- Externe (SMS, OTP, ...)

Permet l'intégration avec des services externes comme l'envoi de codes par SMS ou d'autres méthodes OTP via des fournisseurs tiers.

- REST

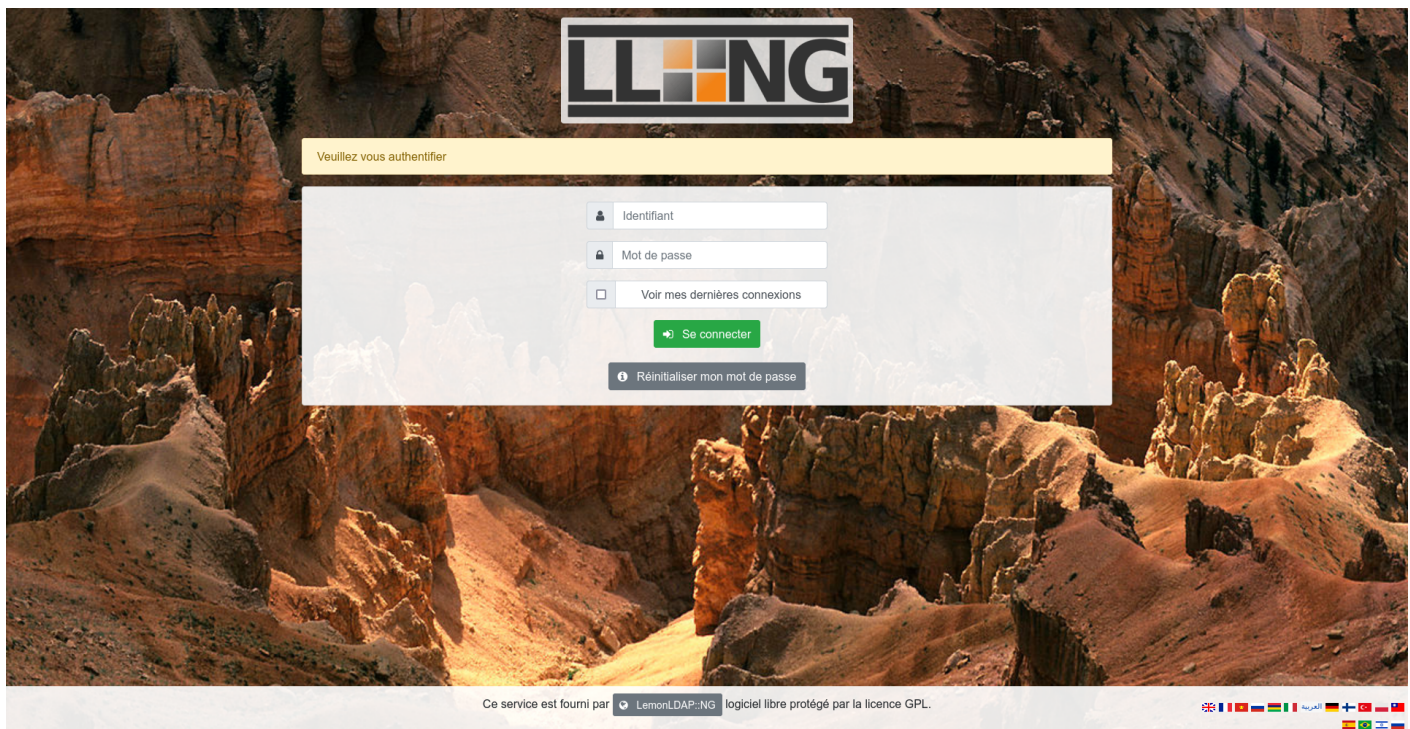
Utilise une API REST pour intégrer la double authentification dans des systèmes personnalisés ou applications externes.

- RADIUS

Protocole utilisé pour gérer l'authentification, autorisation et comptabilité dans les réseaux. Permet d'intégrer 2FA avec des systèmes réseau existants.

L'interface d'authentification de LemonLDAP : :NG se présente de cette façon avec login/password, la possibilité de réinitialiser son mot de passe est proposé à ce niveau.

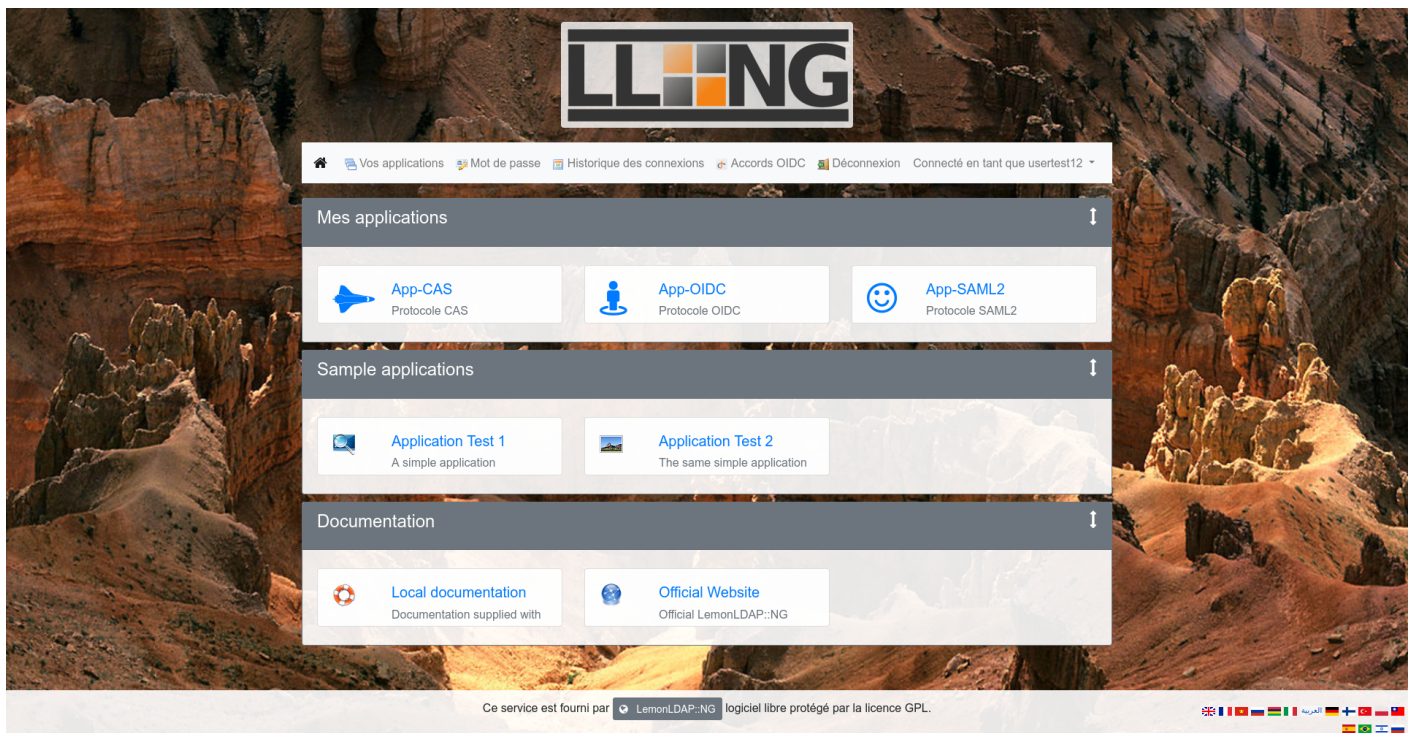
Il existe d'autres fonctionnalités comme la création de compte qui est activable depuis la partie administrateur.



Le portail de LemonLDAP est très intuitif, permettant à l'utilisateur d'accéder facilement aux différentes applications auxquelles il est autorisé (il n'est pas possible pour l'utilisateur de modifier ce portail en catégorisant les différentes applications, cela ne se déroule que du côté administrateur).

Le portail propose également des fonctions de self-service permettant à l'utilisateur de :

- Configurer ses facteurs d'authentification secondaires (second facteur) en ajouter/supprimer
- Réinitialiser son mot de passe par l'envoi d'un mail (Unique méthode présente actuellement).
- Gérer ses accords OIDC, c'est-à-dire supprimer l'accord concernant l'envoi d'attributs établit lors d'une connexion à une application via le protocole OIDC.
- Voir son historique de connexions avec les dernières connexions réussies avec l'heure ainsi que l'adresse IP qui a été utilisé ainsi que les dernières connexions refusées avec les mêmes informations que précédemment avec la raison du refus de cette connexion.



4.1.4 Prérequis & Installation

Au niveau des prérequis, LemonLDAP nécessite :

- Serveur Web (Apache/Nginx, FastCGI ou uWSGI compatible avec un des serveurs web)
- Base de donnée (mySQL, PostgreSQL, MongoDB, Redis...)

L'installation se fait sur un serveur Linux (distributions principales supportées : Debian, Ubuntu, CentOS, Red Hat) De plus, le logiciel est présent dans les dépôts du projet Debian.

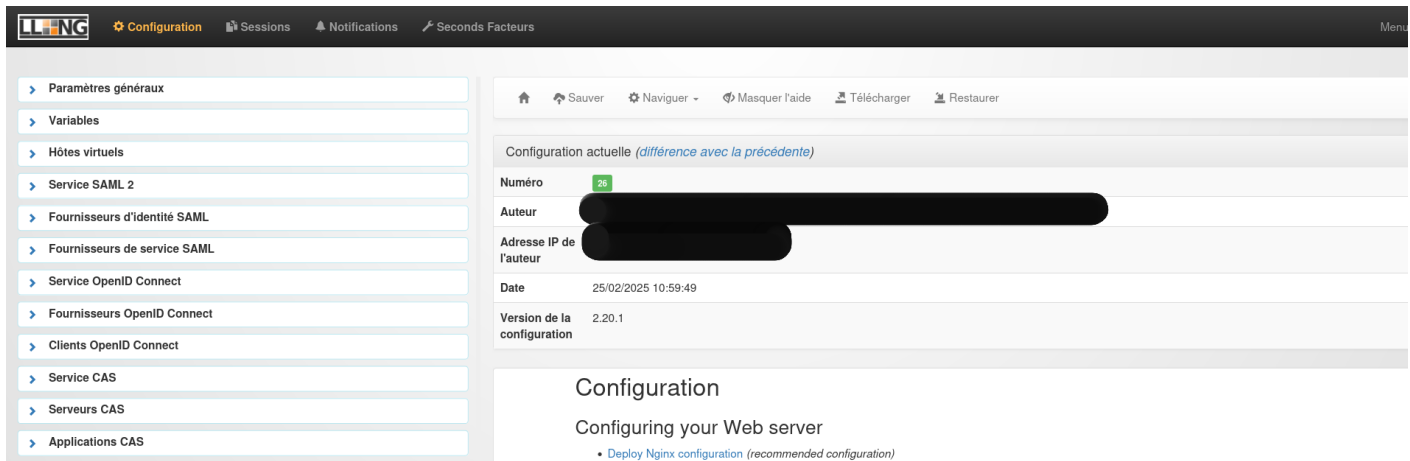
Il existe un Docker Hub contenant des images Docker pour chaque nouvelle version mineure ainsi qu'un Ansible fourni par Worteks.

Son déploiement est très simple :

- Installation des paquets / Utilisation d'une image Docker déjà configuré
- Configuration du serveur Web (Apache ou Nginx)
- Configuration DNS pour accéder aux hôtes virtuelles
- Paramétrage depuis le Manager ou CLI ou importation d'une configuration (.json)

4.1.5 Administration & configuration

La configuration de LemonLDAP est donc possible par une interface Web dénommée Manager :



Permettant de configurer le serveur via une interface graphique, mais aussi de voir les sessions actives ainsi que les anciennes tout cela sous forme de logs (Historique de connexion avec l'IP utilisé, les attributs remontés lors de la connexion...), ainsi que de créer des notifications qui s'afficheront lors de la connexion de l'utilisateur.

Il est aussi possible de l'administrer en ligne de commande (CLI).

```
root@2639407b4cef:/# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli
Usage:
  Usage: lemonldap-ng-cli [options] ACTION [parameters ...]

  Available actions:

  help                : print the full documentation
  info                : get current configuration info
  update-cache        : force configuration cache to be updated
  test-email DESTINATION : send a test email
  get KEY              : get values of parameters
  set KEY VALUE        : set parameter(s) value(s)
  del KEY              : delete parameters
  addKey KEY SUBKEY VALUE : add or set a subkey in a parameter
  delKey KEY SUBKEY     : delete subkey of a parameter
  addPostVars HOST URI KEY VALUE : add post vars for form replay
  delPostVars HOST URI KEY : delete post vars for form replay
  merge FILE [FILE ...] : merge JSON/YAML files with existing configuration
  save                : export configuration to STDOUT
  restore -            : import configuration from STDIN
  restore FILE         : import configuration from file
  rollback             : restore previous configuration
```

Une API est également disponible pour faciliter la gestion des seconds facteurs ainsi que la déclaration des nouvelles applications.

LemonLDAP : :NG intègre un système de versionning, à chaque nouvelle modification le numéro de la configuration est incrémenté permettant de revenir à une configuration précédente en plus de pouvoir comparer les différences entre celle-ci.

Il est possible de personnaliser, l'interface du portail utilisateur en fournissant un logo, une image de fond ainsi qu'un fichier CSS, soit en créant un thème graphique via les fichiers JavaScript, CSS et les modèles HTML.

4.1.6 Performances & consommation de ressources :

Voici un exemple des ressources consommées pour LemonLDAP :NG, ici, nous avons donc notre LLNG qui gère les interactions utilisateurs, interface web et les authentifications ainsi que notre base de donnée (PostgreSQL) pour la configuration de notre SSO ainsi qu'un REDIS qui va s'occuper des sessions.

CONTAINER ID	NAME	CPU %	MEM USAGE / LIMIT	MEM %	NET I/O	BLOCK I/O	PIDS
b212659cc6a3	full-portal-1	0.00%	581.8MiB / 7.754GiB	7.33%	1.98MB / 1.05MB	1.08MB / 987kB	30
5217f1e9d2b7	full-db-1	0.00%	33.66MiB / 7.754GiB	0.42%	198kB / 1.24MB	98.3kB / 905kB	13
81fcb8815dd9	full-redis-1	0.24%	3.469MiB / 7.754GiB	0.04%	61.3kB / 260kB	0B / 0B	6

Cet exemple est peu représentatif étant donné que très peu de comptes sont connectés ou utilisent l'application. Cependant, l'infrastructure actuelle est largement capable de gérer une charge plus importante grâce à ses ressources disponibles, notamment avec Redis pour les sessions et PostgreSQL pour la configuration, qui peuvent facilement évoluer en cas d'augmentation du nombre de connexions simultanées.

VOIR OU/COMMENT INTEGRER

Flexibilité : Possibilité d'ajouter des modules supplémentaires ou d'intégrer des solutions tierces pour répondre à des besoins spécifiques, qu'il s'agisse de nouveaux mécanismes d'authentification ou d'outils de gestion des accès.

Configuration des sources utilisateurs simple à mettre en place, LemonLDAP propose différents modules (Authentification, Utilisateurs, Mot de passe, Auto enregistrement) ou différents backend vont pouvoir être intégré.

METTRE DES LIENS / DOCUMENTATION SUR CERTAINS POINTS

Releases : <https://projects.ow2.org/bin/view/lemonldap-ng/>

4.2 Keycloak (RHBK)

4.2.1 Présentation générale

...

4.2.2 Histoire & contexte d'utilisaton

Keycloak est une solution open-source de gestion d'identité et d'accès (IAM - Identity and Access Management) permettant d'implémenter l'authentification unique (SSO), la gestion des utilisateurs, l'authentification multifactorielle (MFA), et la fédération d'identités. Il est conçu pour sécuriser les applications et services en ligne en centralisant la gestion des utilisateurs et en facilitant l'intégration avec d'autres applications.

Keycloak a été développé par Red Hat, une entreprise américaine spécialisée dans les technologies open-source. Le projet a été lancé en 2014 et est désormais maintenu par la communauté avec l'aide de Red Hat. Il fait partie de la suite d'outils utilisés pour gérer la sécurité des applications dans l'écosystème de Red Hat.

Keycloak est largement utilisée à l'échelle internationale, aussi bien dans des entreprises privées que dans des organismes publics ou des multinationales. Son adoption dépasse largement le cadre des pays francophones.

Les mises à jour majeures de Keycloak sont publiées à un rythme d'environ tous les 3 à 4 mois, apportant de nouvelles fonctionnalités ou des changements structurels importants. Les mises à jour mineures, quant à elles, interviennent généralement tous les 1 à 2 mois, en fonction des besoins, notamment pour corriger des vulnérabilités ou améliorer la stabilité.

La communauté Keycloak est particulièrement active, avec une présence significative sur de nombreux forums et plateformes collaboratives. Cela permet de bénéficier d'un important soutien communautaire et de trouver rapidement des réponses à la plupart des problématiques rencontrées.

4.2.3 Fonctionnalités clés

...

4.2.4 Prérequis et Installation

Keycloak nécessite les éléments suivants pour fonctionner correctement :

- Système d'exploitation : Toute distribution Linux capable d'exécuter Java (tests principalement effectués sur RHEL9).
- Java : OpenJDK 21 ou supérieur.
- Mémoire et stockage : Minimum de 2 Go de RAM et 1 Go d'espace disque disponible.
- Base de données : Une base de données externe partagée, comme PostgreSQL, MySQL, ou Oracle, est requise pour les déploiements en cluster.
- Outils supplémentaires : zip ou gzip et tar pour extraire les fichiers d'installation.

Keycloak dispose d'une image officielle sur Docker Hub et Quay.io, facilitant son déploiement via Docker ou Podman. Pour Kubernetes, un Helm Chart officiel est disponible, permettant une gestion simplifiée des déploiements dans des environnements conteneurisés.

Il existe aussi des rôles Ansible en ligne, mais il en existe déjà un au sein de la DNUM réalisé par ICS. Maintenance (Docker compose up, BDD bien configurée! Montée de version incrémentiel possible si montée de version de Java?) Pas utiliser, exporter/importer données peuvent manquer.

Mises à jour mineures assez fréquentes (40 jours), majeur tous les environs 4 mois avec cependant, moins de tickets (contenus) lors des mises à jour

4.2.5 Prérequis & installation

4.2.6 Administration & configuration

Keycloak dispose d'une interface d'administration accessible via une URL dédiée, par exemple :

- **https ://<url-keycloak>.unistra.fr/admin/<nom-du-royaume>/console**

Cette console permet de gérer tous les aspects des royaumes (realms), des utilisateurs, des groupes, des rôles, et bien plus encore. Voici un aperçu détaillé des fonctionnalités principales :

Gestion des éléments principaux

Royaumes (Realms)

Un royaume est une unité d'administration indépendante dans Keycloak, c'est à dire que différents royaumes ne peuvent pas entrer en contact, disposants de ses propres utilisateurs, clients, rôles et configurations.

L'interface permet :

- La création et la gestion des royaumes.
- La configuration globale du royaume (SSL, paramètres de connexion, durée des sessions, etc.).

Clients

Les clients représentent les applications ou services (SP - Service Providers) qui utilisent Keycloak pour l'authentification, il est possible de :

- Ajouter et configurer des clients.
- Définir les protocoles utilisés (OIDC, SAML, CAS).
- Gérer les client scopes, qui permettent de restreindre ou personnaliser les attributs envoyés dans les jetons en fonction du service.

Rôles (Realm Roles)

Les rôles au niveau du royaume permettent :

- De définir des permissions globales ou spécifiques pour les utilisateurs ou groupes.
- D'accorder des droits d'accès à des applications ou fonctionnalités spécifiques (par exemple, activer un 2FA).
- D'ajouter des attributs supplémentaires non présents dans le LDAP pour répondre à des besoins spécifiques lors de l'authentification.

Importation des utilisateurs

Les utilisateurs peuvent provenir de différentes sources :

Identity Providers (IdP) : Fédération d'identités externes (par exemple, Google, GitLab ainsi que des IDP qui utilisent du SAML2 ou OpenID Connect).

Cependant, Keycloak ne sait lire qu'un seul IDP (exemple avec la fédération Renater qui est fichier metadata qui comprend les nombreux IDP présents dans la fédération).

User Federation : Intégration avec LDAP (Active Directory/OpenLDAP/...) ou Kerberos.

Dans l'interface d'administration, il est possible de :

- Remonté des utilisateurs/groupes avec un filtre
- Faire du mapping d'attributs
- Importation & Synchronisation des utilisateurs/groupes

Groupes

Les groupes permettent de gérer collectivement les utilisateurs :

- Créez des groupes et assignez-leur des rôles ou attributs.
- Ajoutez automatiquement des utilisateurs à un groupe spécifique (y compris ceux provenant du LDAP en cas de synchronisation).
- Utilisez ces groupes pour restreindre l'accès à certaines ressources ou applications.

Sessions

La section "Sessions" permet :

- De visualiser les sessions actives par utilisateur ou par application.
- D'obtenir des informations détaillées comme l'heure de début de session, la dernière activité, l'adresse IP et les applications consultées.
- De révoquer toutes les sessions actives si nécessaire.

Événements (Events)

Keycloak enregistre deux types principaux d'événements :

- Événements utilisateur : Connexions réussies/échouées, modifications de mot de passe, etc.
- Événements administratifs : Actions réalisées par les administrateurs sur le royaume ou sur les utilisateurs.

Configuration avancée

Paramètres du Royaume (Realm Settings)

Général : Configuration SSL et paramètres globaux du royaume.

Login : Activation/désactivation d'options comme l'inscription utilisateur, "se souvenir de moi", récupération de mot de passe.

Email : Configuration du serveur SMTP et personnalisation des emails envoyés (format, expéditeur...).

Themes : Personnalisation des thèmes pour la page de connexion, le compte utilisateur, l'administration et les emails.

Keys : Gestion des certificats et clés cryptographiques utilisés pour signer les jetons.

Localization : Gestion des langues supportées et traduction des messages affichés aux utilisateurs.

Security Defenses : Activation de protections comme XSS Protection, X-Frame Options et gestion contre la force brute.

Sessions / Tokens

Configuration des durées d'inactivité et expiration pour :

- Sessions SSO (standard et "remember me").
- Sessions client.
- Sessions hors ligne (offline sessions).

Paramètres liés aux jetons :

- Algorithmes de signature par défaut.
- Durée de vie des jetons d'accès et de rafraîchissement.

User Profile / Registration

- Définissez les attributs obligatoires pour la création/importation d'un compte utilisateur (nom d'utilisateur, email...).
- Configurez qui peut modifier certains attributs (utilisateur lui-même ou administrateur).

Client Policies

- Permet la configuration avancée pour imposer certaines règles aux clients (par exemple, validation stricte des jetons).

Pour les méthodes d'authentification Keycloak supporte donc :

- LDAPv2/v3 et Active Directory
La partie LDAP est très poussée, permettant par exemple de s'appuyer sur la LDAP Password Policy pour la politique de mot de passe, lecture des groupes de l'utilisateur.
- CAS : Keycloak doit implémenter un plugin communautaire afin de fournir du protocole CAS (1.0/2.0/3.0) et de pouvoir authentifier les utilisateurs.

- SAML2 : Keycloak support le SAML2 (Version 2 du protocole SAML).

Il est possible de faire du :

- client (Service Provider)
- serveur (Identity Provider)

Pour ce qui est des fédérations d'identité, Keycloak ne sait pas lire les metadatas comprenant plusieurs IDP, pour régler cela, il faut passer par un SATOSA

- OpenID Connect : LemonLDAP : :NG supporte le protocole OIDC

Il est possible de faire du :

- client (Service Provider)
- serveur (Identity Provider)

- Sociales, protocoles utilisés OAuth/OIDC (Facebook, X, Github...)

- RADIUS : Plugin communautaire <https://github.com/vzakharchenko/keycloak-radius-plugin>

- Kerberos : Keycloak propose nativement du Kerberos

Les méthodes permettant la double authentification possible par Keycloak sont :

- TOTP (Time-Based One-Time Password)

Utilise des applications comme FreeOTP ou Google Authenticator pour générer des codes temporaires basés sur le temps. Ces codes sont synchronisés avec le serveur et changent toutes les 30 secondes.

- WebAuthn

Standard moderne pour l'authentification sans mots de passe. Utilise des dispositifs biométriques ou physiques (comme les capteurs d'empreintes digitales ou clés USB) pour une authentification sécurisée.

- Mail

Envoie un code ou un lien de vérification à l'adresse e-mail de l'utilisateur pour valider son identité.

- Yubico (Yubikey)

Utilise des clés physiques Yubikey, qui génèrent des OTP ou facilitent l'authentification via NFC/USB pour une sécurité renforcée.

- Externe (SMS, OTP, ...)

Permet l'intégration avec des services externes comme l'envoi de codes par SMS ou d'autres méthodes OTP par l'installation de plugin.

- REST

Utilise une API REST pour intégrer la double authentification dans des systèmes personnalisés ou applications externes.

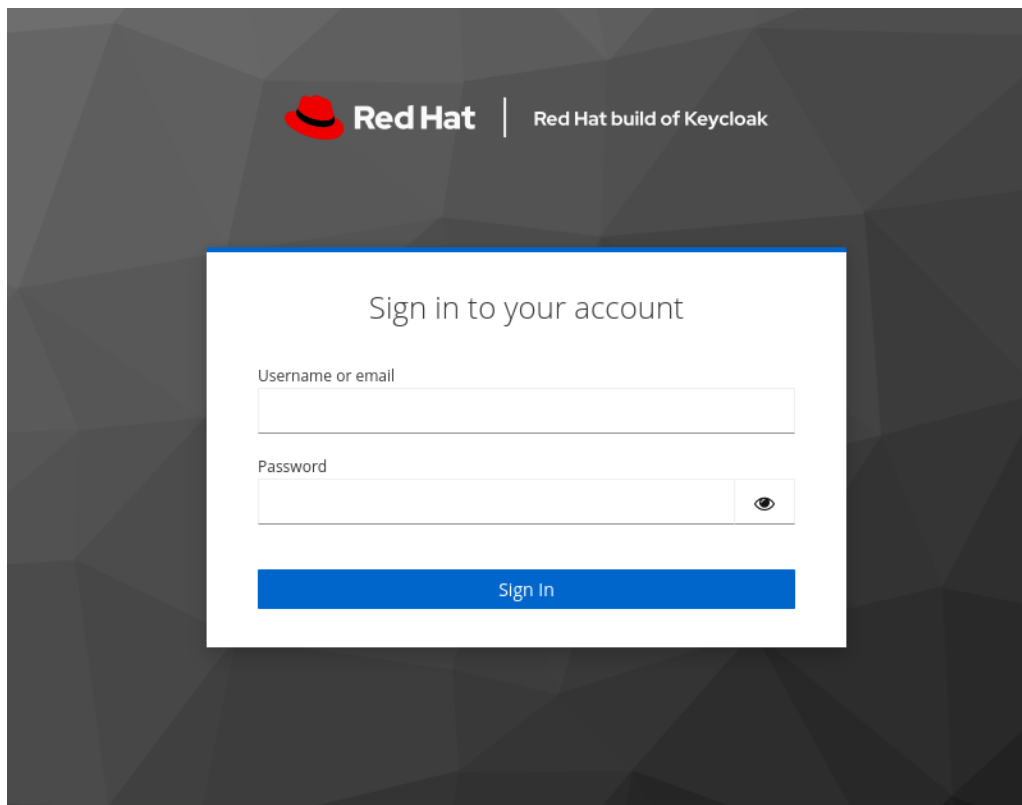
- Autres...

Le fait de pouvoir créer des plugins ou d'utiliser ceux créés par la communauté laisse de nombreuses possibilités d'évolution.

Keycloak permet de personnaliser entièrement l'interface d'authentification grâce à des thèmes modifiables, incluant les pages de connexion, d'inscription, et de réinitialisation de mot de passe. Vous pouvez ajuster les modèles HTML, les styles CSS, et même utiliser des outils comme Keycloakify (basé sur React).

<https://www.keycloakify.dev/>

4.2.7 Performances & consommation de ressources



4.2.8 OU INTEGRER :

Langage de programmation Java

Consommation / Ressources min requises : 512M RAM, 1G disk RAM 557MB CPU 0,18%

ID	NAME	CPU %	MEM USAGE / LIMIT	MEM %	NET IO	BLOCK IO	PIDS	CPU TIME	AVG CPU %
600e1c0e637c	2ea2c2ed03a7-infra	0.00%	49.15kB / 8.057GB	0.00%	344.8MB / 688.8MB	0B / 0B	1	7.986ms	0.00%
7b6d874ab352	postgres	0.00%	6.14MB / 8.057GB	0.08%	344.8MB / 688.8MB	0B / 0B	7	5m10.890893s	0.02%
7aa3e41aa3b0	rhbk	0.13%	557.1MB / 8.057GB	6.91%	344.8MB / 688.8MB	0B / 0B	53	18m26.880385s	0.16%

– Légende –

Possibilité de créer / ajouter des plugins Communauté de Keycloak très présente (25K stars git), beaucoup de tutoriels, conseils... par les utilisateurs.

Plugin France Connect très complet (ajout de AgentConnect, theme intégré, visiblement maintenu à jour) proposé dans la documentation Keycloak mais pas directement intégré

Fédération Renater, Keycloak n'accepte pas les métadonnées des fédérations (il n'arrive pas à interpréter la métadonnée fournit par celle-ci, car elle comprend plusieurs métadonnées de différents IDP), utilisation de SATOSA comme contournement : <https://www.fairkom.eu/en/federated-identities-with-keycloak>

4.3 MidPoint

4.3.1 Présentation générale

MidPoint est une plateforme de gestion de l'identité et de gouvernance développée par Evolveum. Il s'agit d'un système complet, riche en fonctionnalités, développé et maintenu par une équipe professionnelle d'ingénieurs à plein temps. MidPoint est un logiciel open source, disponible sous les termes de la licence Apache et de la licence publique de l'Union européenne.

4.3.2 Intérêt dans le cadre post-étude

...

4.3.3 Liens possibles avec LLNG :NG ou Keycloak

...

5 Banc d'essais & expérimentation

5.1 Architecture technique mise en place

...

5.2 Scénarios de test

...

5.3 Difficultés rencontrées

...

5.4 Résultats et observations

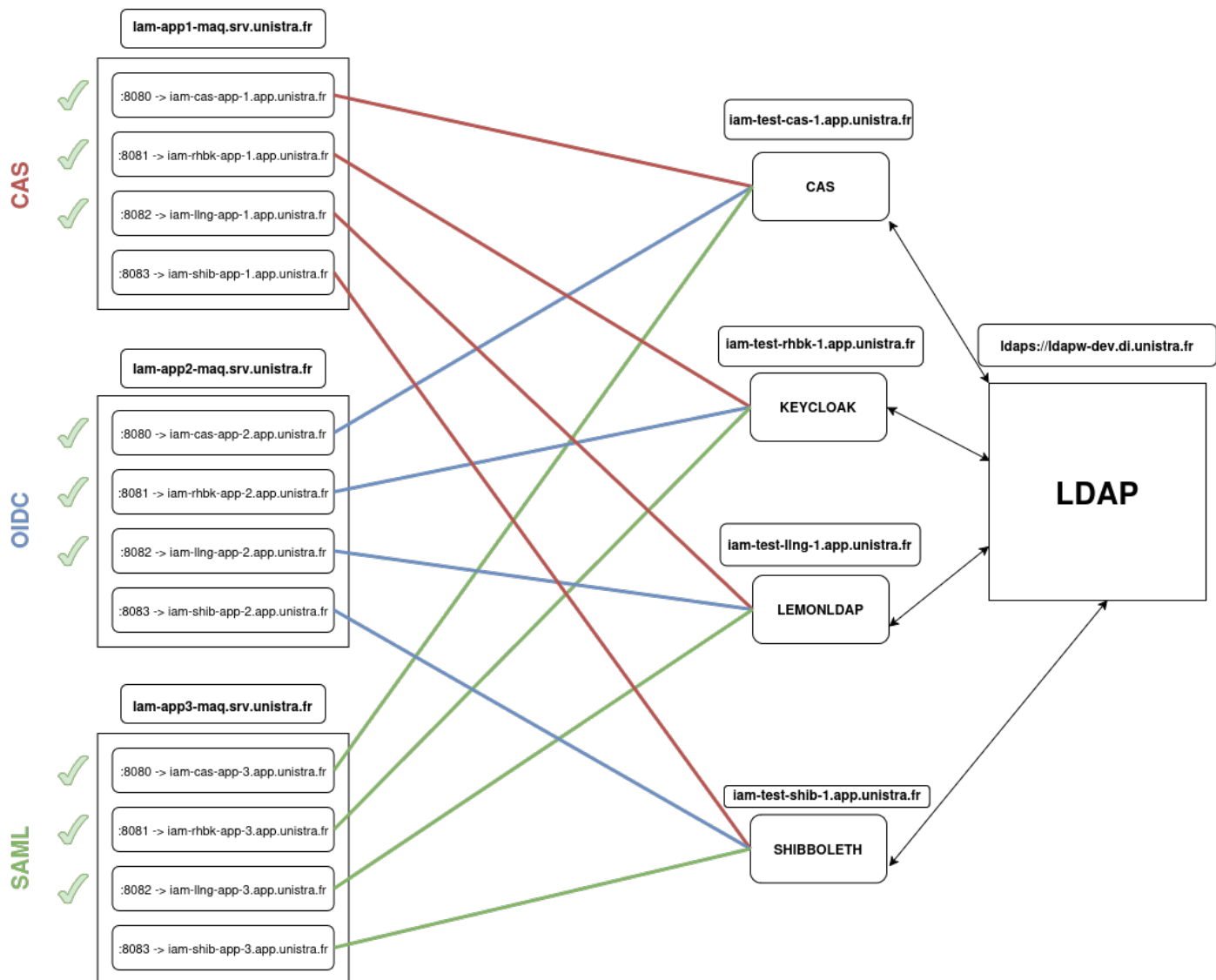
... Pour le bien de cette étude, nous avons dû réaliser des tests concernant les différents protocoles utilisés au sein de l'Unistra et en dehors, tel que CAS, OpenIDConnect et SAML2 sur les différentes applications étudiées qui sont Apereo CAS 7.2, LemonLDAP : :NG, Keycloak (On utilise RHBK ou Red Hat Build of Keycloak qui est une version payante de Keycloak avec des prestations possibles par le support de Red Hat) ainsi que Shibboleth 5.1.

Nous avons aussi testé des appels d'API (REST) pour interagir avec Keycloak et LemonLDAP concernant le changement de mot de passe, récupération d'informations sur un utilisateur, configuration directement dans l'application (Création de SP/RP, modification du Workflow...).

Pour chaque outil IAM nous allons tester chaque protocole d'authentification sur des applications compatibles, nous avons donc déployés des Nextcloud pour la partie OIDC et SAML2 et pour le protocole nous avons utilisé le module d'authentification CAS sur des Apache.

Nous avons donc intégré nos différentes applications au sein des outils pour pouvoir s'authentifier avec notre IDP, nous avons aussi mis en place des règles d'accès sur les différentes applications que ce soit par l'appartenance à un groupe ou un niveau d'authentification trop faible. L'authentification a été activée pour les utilisateurs appartenant à certains groupes (Via Keycloak on peut utiliser des rôles plutôt que les groupes provenant du LDAP).

Les différents outils ont été ajoutés dans la fédération Renater en tant qu'IDP pour permettre aux différents SP inclus dans la fédération de pouvoir s'authentifier avec notre LemonLDAP : :NG ou Keycloak.



6 Comparatif des solutions

Ce comparatif va se baser sur les différentes attentes qui ont été définies pour cette étude sous forme de tableau.

6.1 Tableau comparatif complet :

		LLNG	Keycloak	Midpoint
Protocoles de connexion supportés	CAS	✓	-	X
	SAML2	✓	✓	✓
	OIDC	✓	✓	✓
	RADIUS	✓	✓	X
	KERBEROS	✓	✓	X
	SOCIAL	✓	✓	✓
MFA	TOTP	✓	✓	X
	MAIL	✓	✓	X
	SMS	-	✓	X
	Usage unique	-	✓	X
	WebAuthn	✓	✓	X
	Yubico (Yubikey)	✓	✓	X
	Notifications Push	-	-	X
	Sans contact / NFC	X	-	X
Authentification basé sur des jetons	SSO	✓	✓	X
	Token	✓	✓	✓
Règles de sécurité	ACL	✓	✓	X
	Scripting	✓	✓	✓
Autorisation	Rôles et groupes	-	✓	✓
	Règles	✓	✓	✓
	Accès privilégiés	✓	✓	✓
	Workflow	✓	✓	✓
Annuaire	Référentiel des personnes	X	X	✓
	Référentiel des comptes	X	X	✓
	Référentiel des groupes	X	X	✓
	Fédération d'identité	✓	-	X
	Synchronisation	✓	✓	✓
Services de gestion de utilisateurs	Enrôlement	✓	✓	✓
	Provisioning	X	X	✓
	Deprovisioning	X	X	✓
	Mobilité	X	X	✓
	Changement de mot de passe	✓	✓	✓
	Changement d'attributs	-	✓	✓
	Recherche annuaires	X	X	✓
	Demande d'accès	X	X	✓
	Délégation	✓	✓	✓
	Recertification	-	-	✓
Gouvernance	Audit et traçabilité	✓	✓	✓
	Security policy	✓	✓	✓
	Rapport et alertes	✓	✓	✓

Légende :

✓ : Possible

- : Possible avec contraintes

X : Ne le permet pas

6.2 Tableau comparatif détaillé

Sur ce tableau, sera comparé LemonLDAP : :NG et Keycloak les différentes fonctionnalités qui sont présentes ou non ainsi qu'un niveau de facilité de mise en place accompagné de remarques.

Midpoint n'est pas présent sur ce tableau étant donné que l'étude se concentre sur l'authentification et que ce n'est pas sa fonctionnalité principale.

Authentification

Protocoles de connexion supportés

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
CAS	✓	★★★★	-	★★★★☆
SAML2	✓	★★★★	✓	★★★★☆
OIDC	✓	★★★★	✓	★★★★☆
RADIUS	✓	?	✓	?
Kerberos	✓	?	✓	?
Social	✓	?	✓	?

Remarques :

CAS :

Keycloak : Via un plugin d'extension par la communauté référencé au sein de la documentation officielle de Keycloak), la mise en place de plugin sur Keycloak est très simple.

Problématique : Étant donné que ce plugin est réalisé par la communauté, son maintien lui aussi ne repose que sur la communauté l'utilisant, ce qui pourrait poser un problème, surtout pour un protocole d'authentification...

LemonLDAP : Le module CAS est déjà intégré à l'outils, supportant du CASv1/2/3.

SAML2 :

Keycloak : Le protocole est déjà implémenté dans l'application, son utilisation est assez simple, il reste un problème sur l'envoi de certains attributs.

LemonLDAP : Le protocole est déjà implémenté dans l'application, son utilisation est très claire que ce soit pour l'ajout des SP ou la mise en place de la fédération.

OIDC :

Keycloak : Le protocole est déjà implémenté dans l'application, son utilisation est assez simple, il reste un problème sur l'envoi de certains attributs.

LemonLDAP : Le protocole est déjà implémenté dans l'application, son utilisation est très claire que ce soit pour l'ajout des SP, les différents scopes avec les attributs à récupérer.

Kerberos :

Keycloak : Via un plugin d'extension créé par la communauté

Double authentification supportée

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
TOTP	✓	★★★★	✓	★★★★
MAIL	✓	★★★★	✓	★★★★
SMS	-	?	✓	?
Usage unique	-	?	✓	?
WebAuthn	✓	★★★★	✓	★★★★
Yubico (Yubikey)	✓	★★★★	✓	★★★★
Notifications Push	-	?	-	?
Sans contact / NFC	✓	?	-	?

Remarques :

TOTP :

Keycloak : Fonctionnalité présente nativement dans l'application, possibilité de jouer avec dans la partie Workflow.

LemonLDAP : Fonctionnalité présente nativement dans l'application, possibilité de jouer avec dans la partie Workflow.

MAIL :

Keycloak : Via un plugin d'extension par la communauté, la mise en place de plugin sur Keycloak est très simple.

Problématique : Le plugin va forcer la mise en place de ce 2FA (Aucun choix sûr, si l'on utilise ou pas en fonction d'un compte) si l'utilisateur à un mail de configuré.

LemonLDAP : Fonctionnalité présente nativement dans l'application.

Problématique : L'activation de ce second facteur va forcer la mise en place de cette méthode (Si le mail de l'utilisateur est remonté alors, elle sera activé par défaut, impossible de décider si on souhaite l'activer ou non. Si l'on configure un second facteur, nous aurons le choix entre le mail ou celui configuré).

WebAuthn :

Keycloak : Fonctionnalité présente nativement dans l'application, possibilité de jouer avec dans la partie Workflow

LemonLDAP : Fonctionnalité présente nativement dans l'application, possibilité de jouer avec dans la partie Workflow

SMS :

Keycloak : Via un plugin d'extension par la communauté

PUSH :

Keycloak : Via un plugin d'extension (work in progress)

LemonLDAP : :NG : Plugin "2FA Externe" qui permet d'appeler un système de 2FA extérieur

Yubikey :

LemonLDAP : :NG : Bien installer le module CPAN avant l'activation de la fonctionnalité, sinon "Internal Server Error" + configuration d'une API Yubico.

SSO / Token

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
SSO	✓	★★★★	✓	★★★★
Token	✓	★★★★	✓	★★★★

Remarques :

Single Sign On :

MidPoint : S'intègre à des solutions SSO mais n'est pas un fournisseur SSO natif

Définir des règles de sécurité

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
ACL	✓	★★★★	✓	★★★★☆
Scripting	✓	★★★★	✓	★★★★

Autorisation

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
Rôles & Groupes	-	X	✓	★★★★
Règles	✓	★★★★	✓	★★★★☆
Accès privilèges	✓	★★★★	✓	★★★★☆
Workflow	✓	★★★★☆	✓	★★★★

Remarques :

Rôles et groupes :

LemonLDAP : :NG : Il peut lire les différents groupes du LDAP cependant, il ne pourra en aucun cas les administrer (créer/supprimer/modifier) de plus, il n'y a pas de notion de rôles.

Keycloak : Il peut lier les groupes LDAP au sein de l'outil pour y ajouter de nouveaux membres éventuellement, les changer de groupes ou autre.

Règles :

LemonLDAP : :NG : Permet de mettre en place des règles pour faire de la discrimination (appartenance à un groupe, niveau d'authentification trop faible...) pour accéder à une application.

Keycloak : Mis en place par l'utilisation des royaumes qui vont permettre de séparer les différentes catégories de personnes ainsi que leurs applications autorisées, cependant il existe un plugin qui va permettre d'ajouter un flow d'authentification supplémentaire lors de la connexion (appartenance à un groupe/rôle)

Annuaire

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
Référentiel des personnes	X	X	X	X
Référentiel des comptes	X	X	✓	★★★☆☆
Référentiel des groupes	X	X	X	X
Fédération d'identité	X	X	X	X
Synchronisation	✓	★★★★☆	✓	★★★★

Remarques :

Fédération d'identité :

Keycloak : Via une application tiers

Services de gestion des utilisateurs

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
Enrôlement	✓	★★★★	✓	★★★★
Provisionnement	X	X	X	X
DeProvisionnement	X	X	X	X
Mobilité	X	X	X	X

Remarques :

Enrôlement :

Keycloak : Permet de créer des comptes (manuellement) via un formulaire qui seront répercutés dans le LDAP

LemonLDAP : :NG : Plugin permettant de créer des comptes via un formulaire répercutant cela dans le LDAP.

Self-service

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
Changement de mot de passe	✓	★★★★	✓	★★★★
Changement d'attributs	X	X	✓	★★★★☆
Recherche annuaires	X	X	X	X
Demande d'accès	X	X	X	X

Remarques :

Changement de mot de passe :

Keycloak : Permet de modifier n'importe quel attribut remonté dans l'outil

LemonLDAP : Permet uniquement de changer l'attribut userPassword (cf. Changement de mot de passe)

Délégation/Recertification

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
Délégation	✓	★★★★☆	✓	★★★★
Recertification	-	★★★★	-	★★★★

Gouvernance

	LemonLDAP : :NG		Keycloak	
	Supporté	Facilité	Supporté	Facilité
Audit traçabilité	✓	★★★★	✓	★★★★
Security policy	✓	★★★★	✓	★★★★
Rapport et alertes	✓	★★★★	✓	★★★★

Remarques :

Audit et traçabilité :

Keycloak : Events (Admin/Utilisateurs) donnant le protocole, l'URL de redirection (l'application auquel se connecte l'utilisateur, uid...) + logs console

LemonLDAP : Informations sur les sessions d'utilisateurs telles que son IP, Heure de connexion...
+ logs permettant de voir les connexions aux différentes applications

7 Conclusion

Dans le cadre de la mise en place d'une infrastructure de gestion des identités et des accès (IAM), plusieurs combinaisons sont envisageables, notamment avec Keycloak - MidPoint - Grouper ou LemonLDAP : :NG - Midpoint - Grouper.

L'objectif est de disposer d'une infrastructure légère, simple à déployer et maintenable, tout en répondant aux usages actuels, **LemonLDAP : :NG s'impose comme une solution particulièrement pertinente.**

Avantages de LLNG :

- Compatibilité native avec les protocoles CAS, SAML2 et OpenID Connect, sans recours à des plugins ou composants externes.
- Fonctionnalités de MFA (authentification multifacteur) intégrées.
- Interface d'administration claire, facilitant la gestion des règles d'accès, restrictions, et applications.
- Déploiement rapide : l'installation de LLNG peut être réalisée en quelques heures, avec une configuration initiale simple.

Keycloak est une solution IAM puissante et modulaire, bien adaptée aux environnements complexes et aux besoins d'évolution future. Toutefois, sa mise en œuvre initiale est plus exigeante, notamment dans le contexte universitaire ou fédéré.

Points à considérer pour Keycloak :

Nécessite l'ajout de composants tiers :

- SATOSA pour gérer la fédération d'identité avec des fournisseurs comme Renater.
- Plugin CAS non inclus en natif, maintenu par la communauté.
- Interface riche mais moins intuitive que LLNG pour certains cas d'usage simples.

Compléments possibles avec Grouper et MidPoint

Grouper, déjà en place, peut être couplé à LLNG ou Keycloak pour enrichir la gestion des groupes et des rôles.

MidPoint peut venir compléter l'architecture pour assurer le provisioning des comptes, une fonction non couverte directement ni par LLNG ni par Keycloak.

7.1 Synthèse de l'étude et recommandation

7.2 Mon avis personnel sur les outils

7.3 Retour sur l'année d'alternance

7.3.1 Apports techniques

7.3.2 Apports professionnels et personnels

8 Annexes

...