IDENTITY DAYS

24 octobre 2023 - PARIS

IDENTITY DAYS

24 octobre 2023 - PARIS

@IdentityDays #identitydays2022

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

BeyondTrust

ermetic

Exakis Nelite
MagellanPartners

FUSION DIRECTORY

jumpcloud

KERBEROS CONSULTING

Kleverware

METSYS

okta

ONE IDENTITY by Quest

ManageEngine

SailPoint

semperis

SILVERFORT

Systancia

IDENTITY DAYS

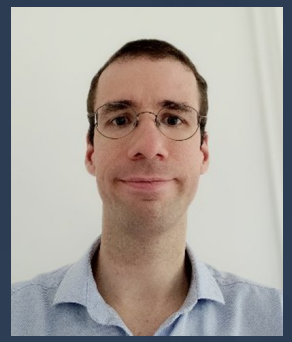
24 octobre 2023 - PARIS

SSO et fédération d'identités avec le logiciel libre LemonLDAP::NG, retour d'expérience d'un client

David Coutadeur

Vorteks
make IT work, make IT free

David Coutadeur
Architecte en gestion d'identité



Ordre du jour

1. Présentation
2. Présentation de LemonLDAP::NG
3. Mise en place chez [client]
4. Nouveautés de LemonLDAP::NG

Présentation

Intervenants

David COUTADEUR

architecte en gestion d'identité

~10 ans d'expérience dans le domaine

passionné d'open-source

david.coutadeur@worteks.com

@dcoutadeur@toot.aquilenet.fr

www.linkedin.com/in/david-coutadeur-06571a1a4

Worteks (\vɔʁ.tɛks\)

Service

Infrastructures complexes, cloud, mail, authentification, sécurité,...

- Études, audit & consulting
- Expertise technique
- Support
- Formation
- R&D et innovation

Édition

V'Sweet — Portail collaboratif

V'Opla — Plateforme de développement commune

V'IDaaS — Gestion des identités et des accès

Partenaires

Red Hat Advanced Business Partner Reseller

BlueMind

ONLYOFFICE

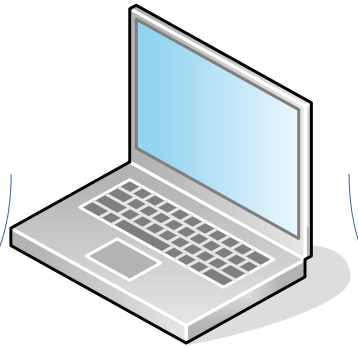
Collabora Online

All we need is you!

https://www.worteks.com/rejoindre/

Présentation de LemonLDAP::NG

SSO Workflow



2. Authentification

1. Premier accès

3. Envoi du jeton SSO

4. Validation du jeton SSO

Portail d'authentification

Lien de confiance

Application

Historique

Création du projet

2003

Fork – version NG

2006

Protocoles CAS, SAML et OpenID version 1.0

2010

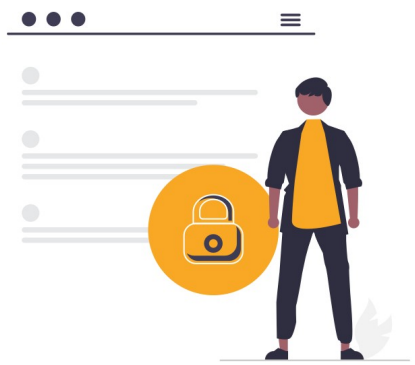
Protocole OpenID Connect

2016

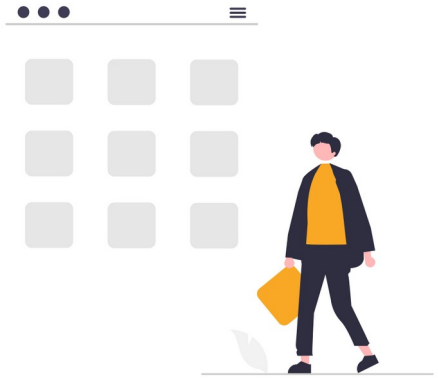
Second facteurs (2FA) version 2.0

2018

Principales fonctionnalités



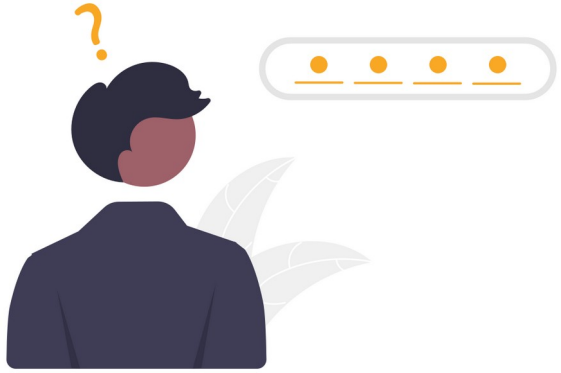
SSO & Contrôle d'accès



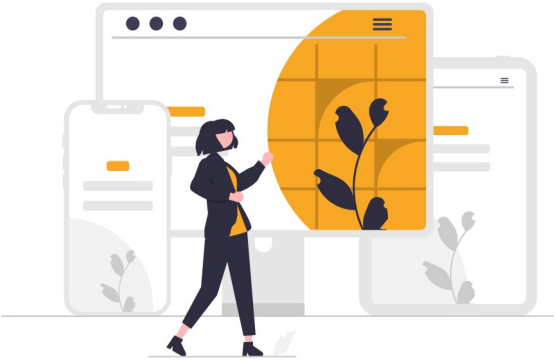
Menu des applications

CAS / SAML / OIDC

Second facteurs (2FA)



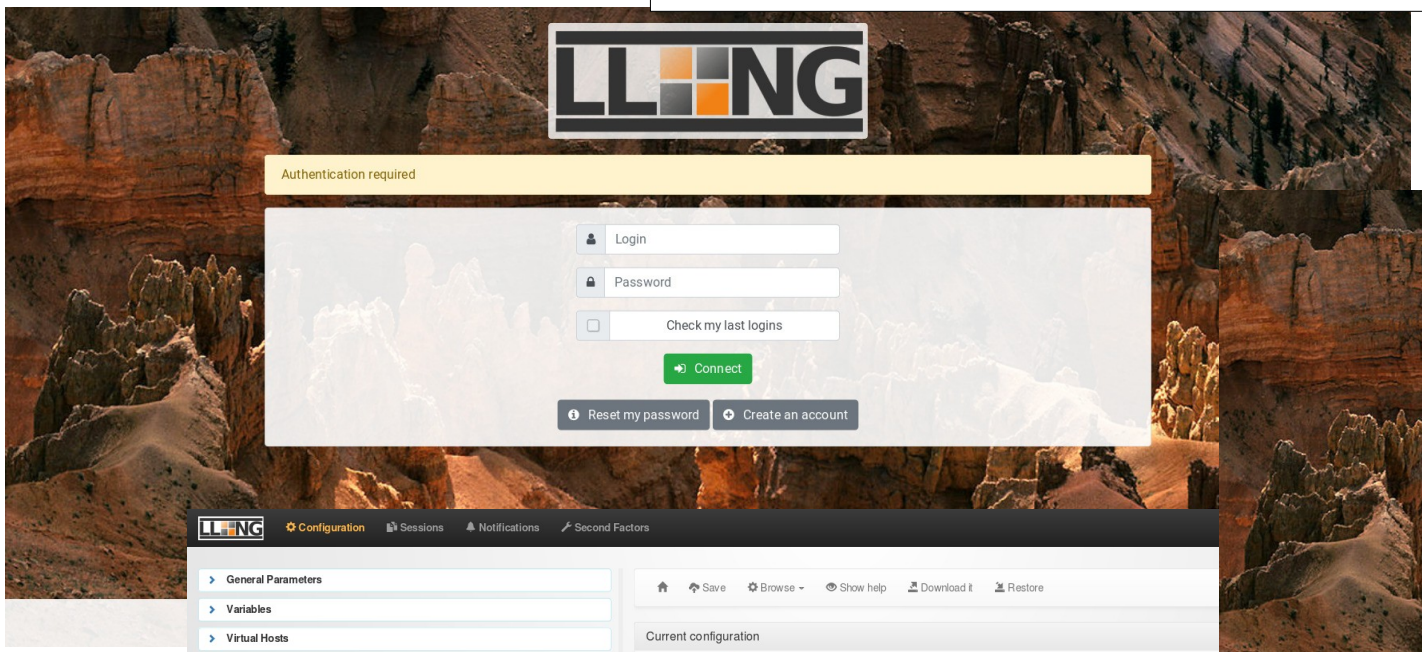
Gestion du mot de passe



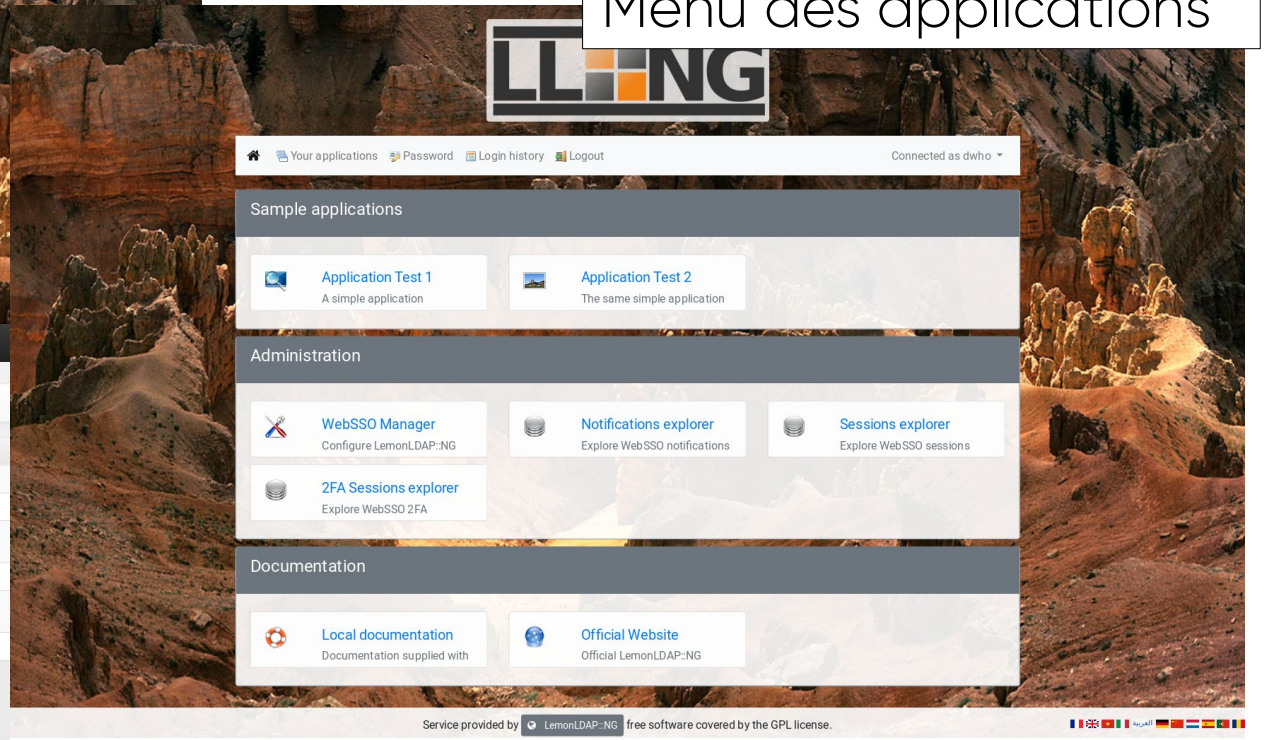
Personnalisation graphique

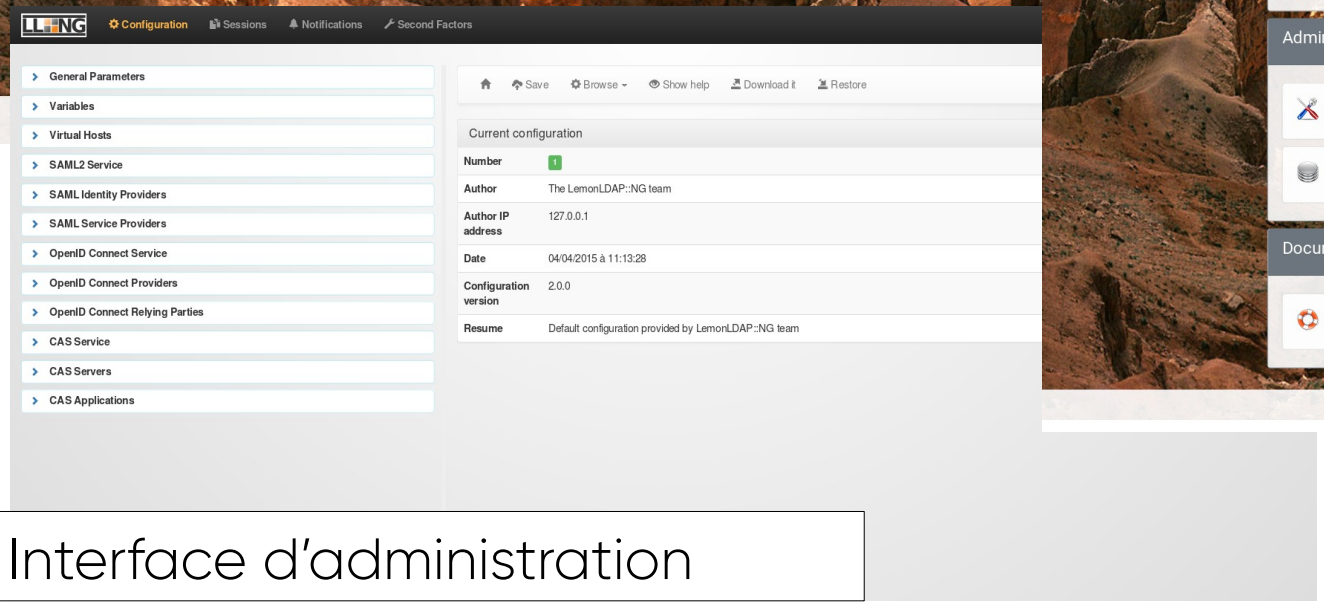
Interfaces

Formulaire d'authentification



Menu des applications





Interface d'administration

Interface CLI

```
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli info

Num      : 88
Author   : clement
Author IP: localhost
Date     : Tue Dec 18 09:57:58 2018
Log      : Edited by lmConfigEditor
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli help
Usage: /usr/share/lemonldap-ng/bin/lemonldap-ng-cli <options> action <parameters>

Available actions:
 - help                          : print this
 - info                          : get currentconfiguration info
 - update-cache                  : force configuration cache to be updated
 - get    <keys>                 : get values of parameters
 - set    <key> <value>          : set parameter(s) value(s)
 - addKey <key> <subkey> <value> : add or set a subkey in a parameter
 - delKey <key> <subkey>         : delete subkey of a parameter

See Lemonldap::NG::Common::Cli(3) or Lemonldap::NG::Manager::CLi(3) for more
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli set ldapServer 'ldap://ldap.example.com'
```

Logiciel libre

- Licence GPL
- Projet OW2
- Forge: https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng
- Site: https://lemonldap-ng.org
- « OW2 Community Award in 2014 »
- Composant SSO du projet FusionIAM : https://fusioniam.org/

Rôles des composants

Portail

Menu des applications

CAS
SAML
OpenID Connect

Self Services

Serveur SOAP/REST

Gestion des sessions

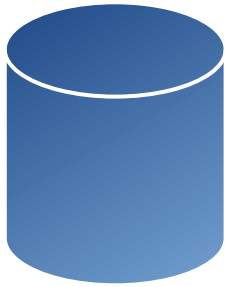
Manager

Configurations

Sessions

Notifications

Second facteurs



Configurations

Sessions

Handler

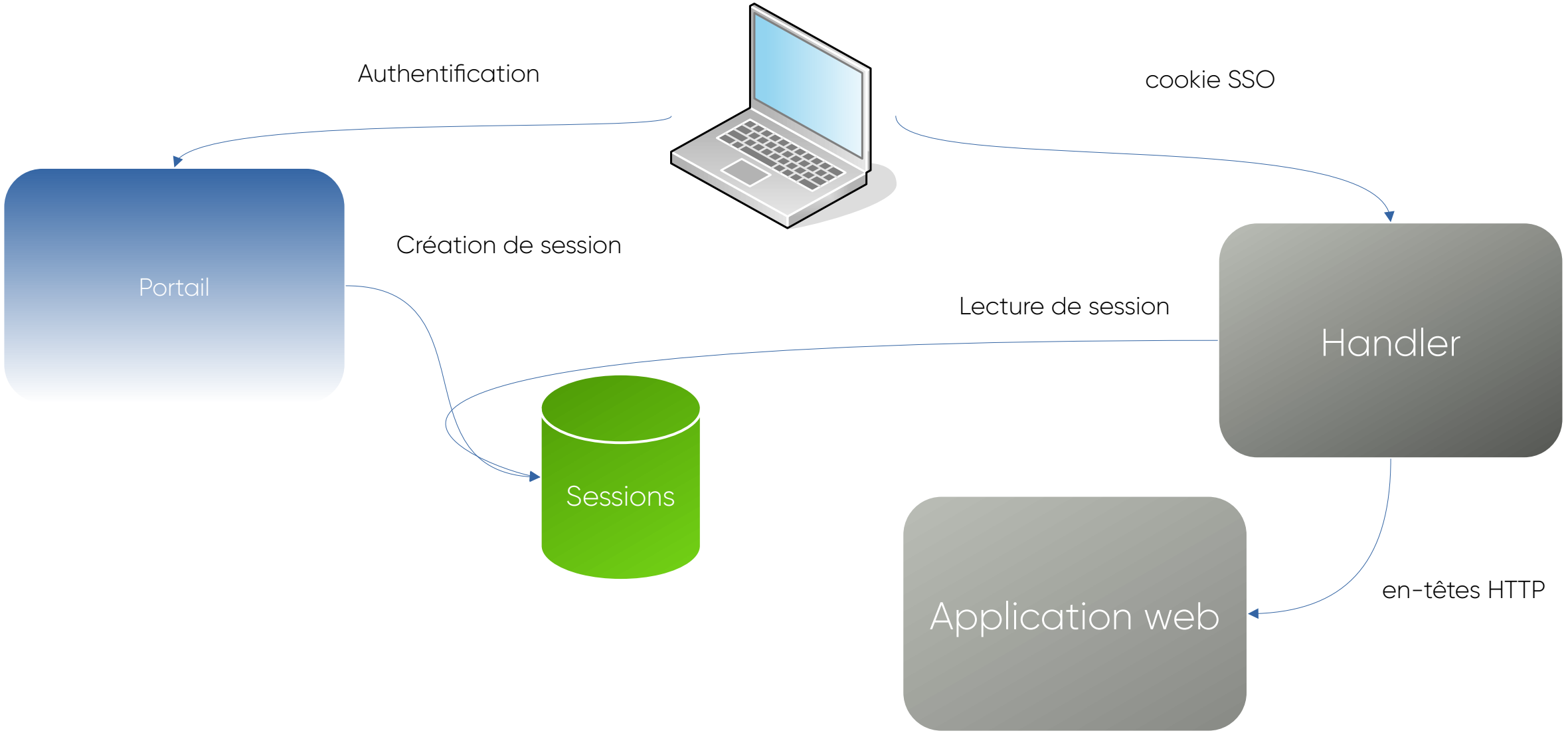
Contrôle d'accès

SSOaaS

Web Service Token

Personnalisé

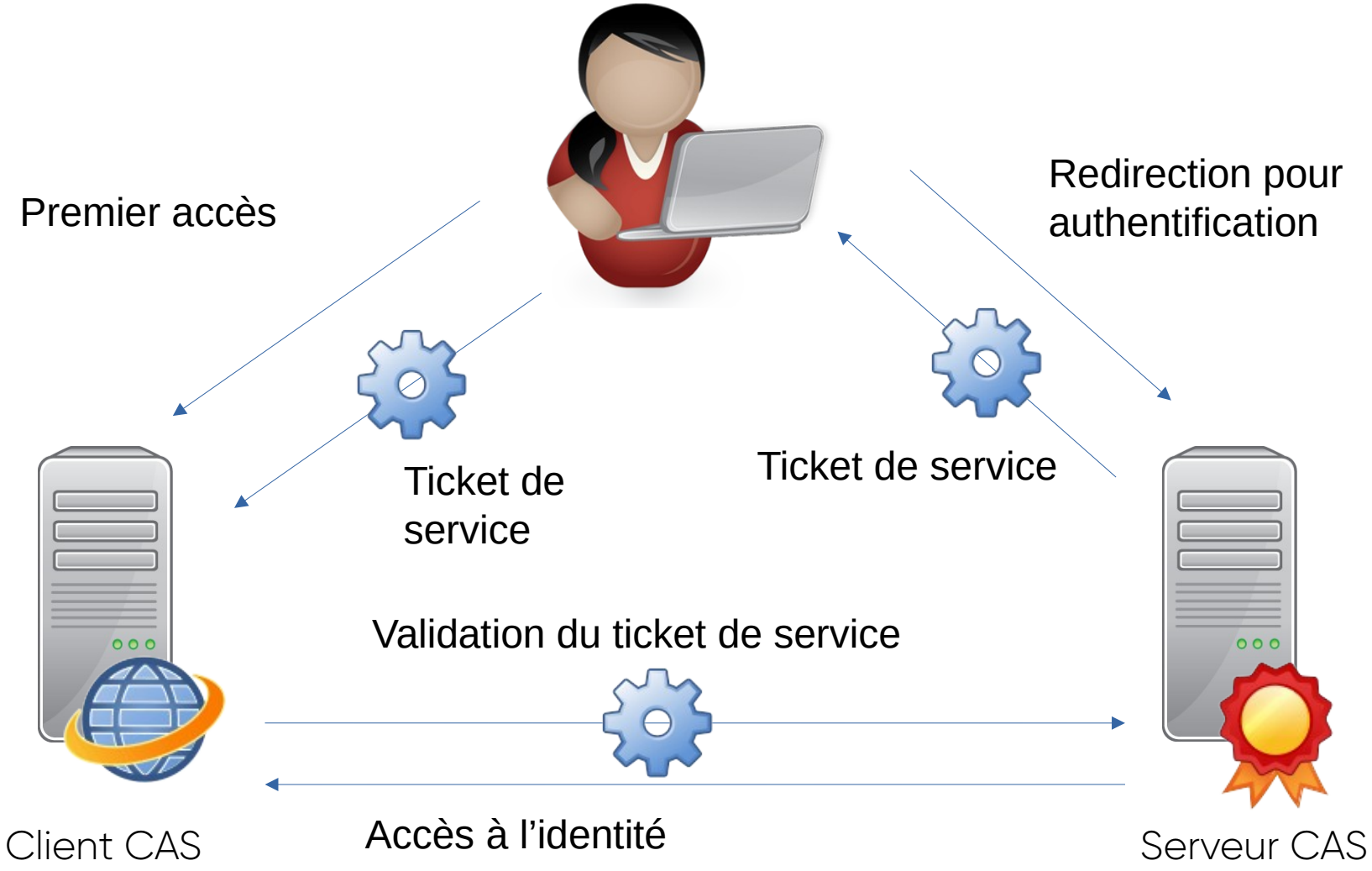
Application web protégée par handler



CAS

- Créé par l'université de Yale
- « Central Authentication Service »
- Mode proxy depuis la v2.0
- Partage d'attributs depuis la v3.0
- https://www.apereo.org/projects/cas

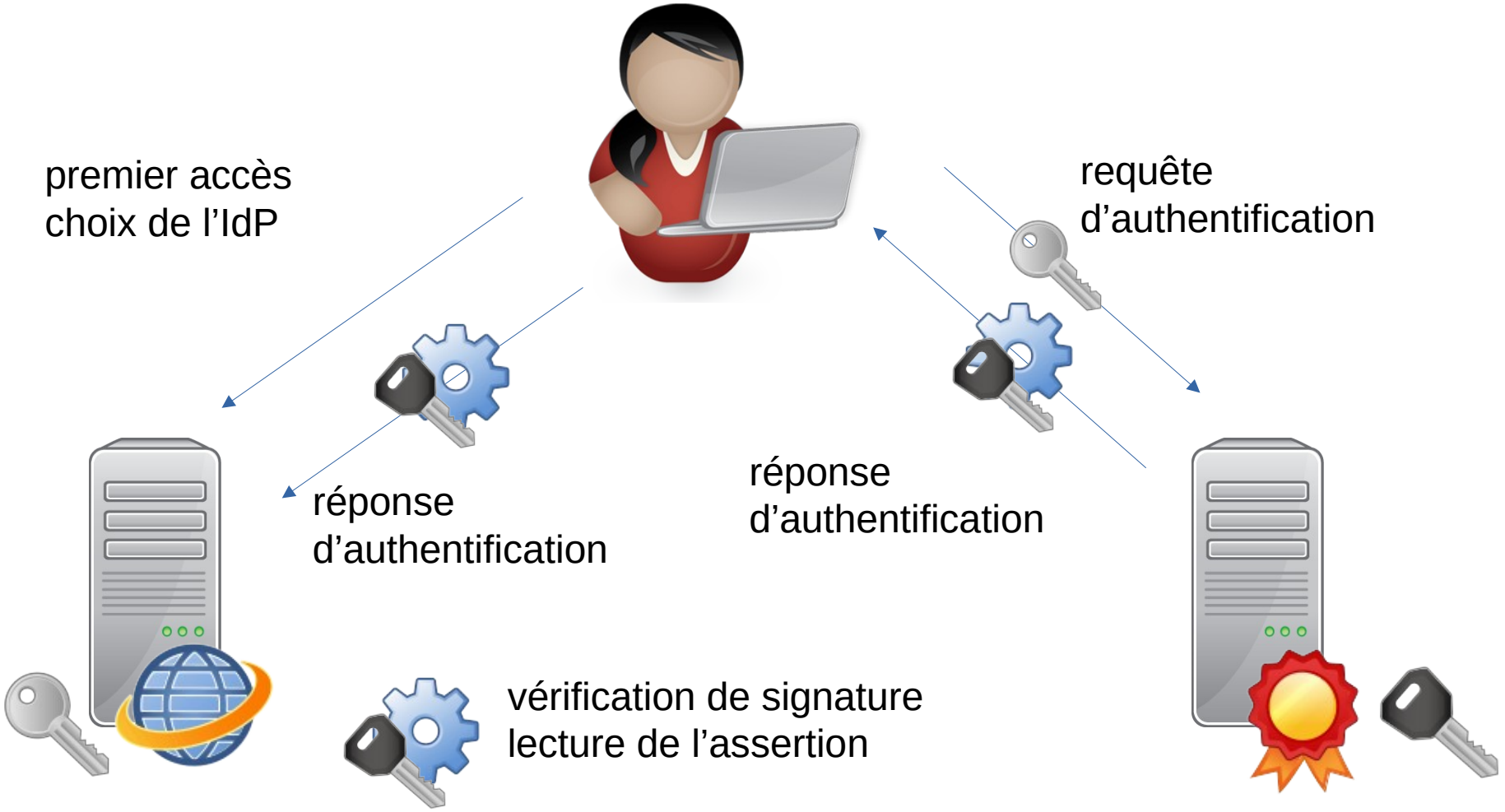
CAS


Premier accès
Redirection pour authentification
Ticket de service
Ticket de service
Validation du ticket de service
Accès à l'identité
Client CAS
Serveur CAS

SAML

- Créé par l'organisation OASIS
- « Security Assertion Markup Language »
- Version 1.0 en 2002
- Version 1.1 en 2003
- Version 2.0 en 2005, fusionnant SAML, Shibboleth et ID-FF (Liberty Alliance)

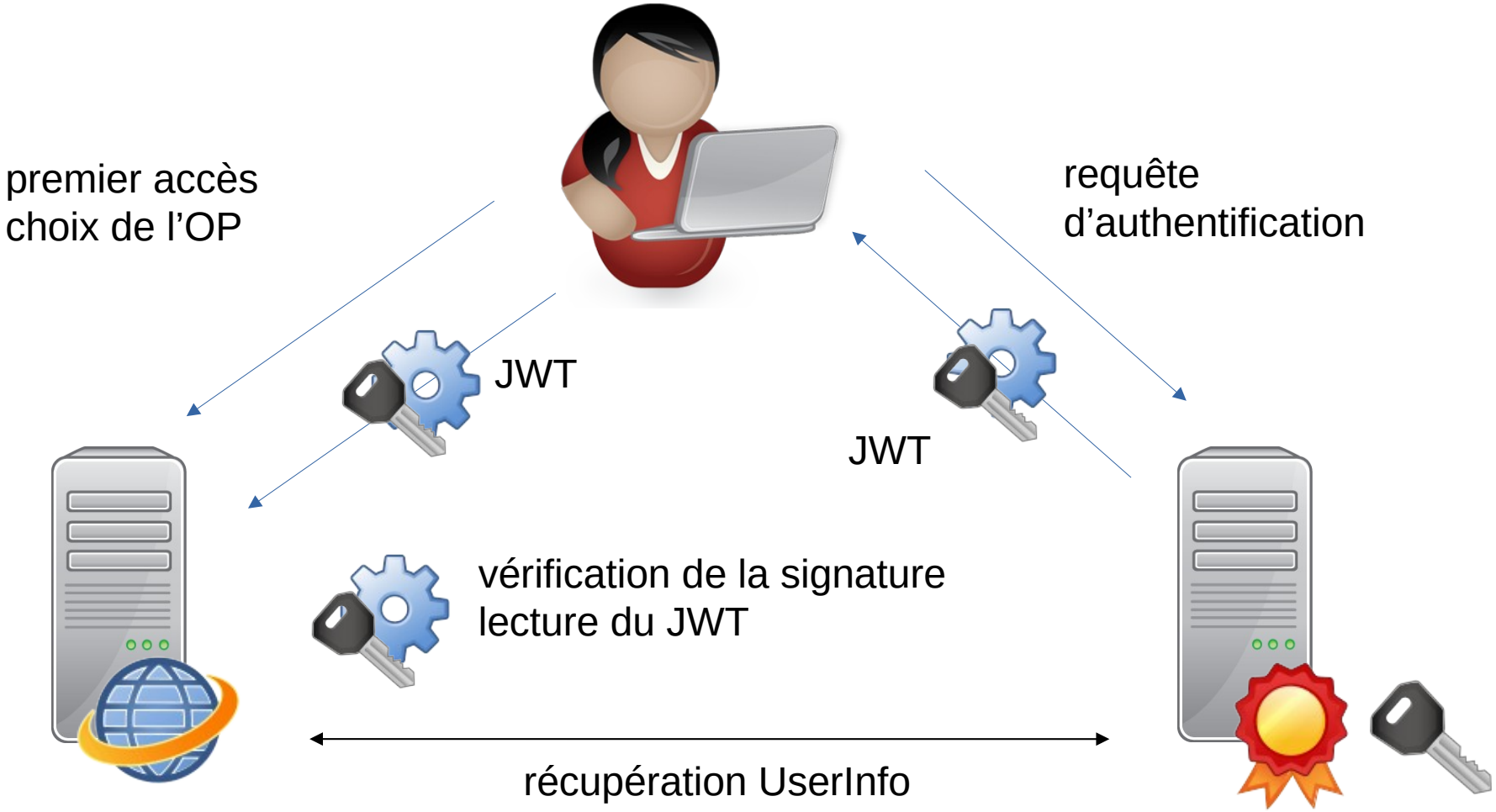
SAML


premier accès
choix de l'IdP
requête
d'authentification
réponse
d'authentification
réponse
d'authentification
vérification de signature
lecture de l'assertion
Fournisseur de Service (SP)
Fournisseur d'Identité (IdP)

OpenID Connect

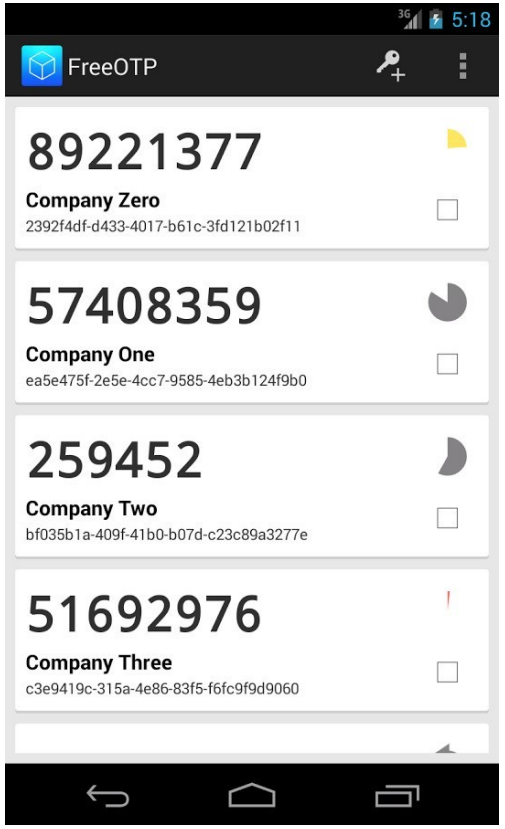
- Créé en 2014
- Présenté aux RMLL en 2015
- Basé sur OAuth 2.0, REST, JSON, JWT, JOSE
- Adapté aux navigateurs web et aux applications mobiles natives
- Partage d’attributs via le point d’entrée UserInfo

OpenID Connect



Second Facteur d'Authentification (2FA)

- LemonLDAP::NG peut utiliser les 2FA suivants :
  - TOTP
  - WebAuthn
  - Mail
  - External (SMS)
  - REST
  - Yubikey
  - Radius



fido ALLIANCE

RENATER / eduGAIN

- Support de RENATER / eduGAIN via SAML2 :

  Fournisseur de Service

  Fournisseur d’Identité

- Appel à la page de sélection du Fournisseur d’Identité (WAYF) via « SAML Discovery Protocol »
- Script d’import en masse des métadonnées

Moteur de plugins

- Le portail a été complètement réécrit, et il permet maintenant le développement de plugins
- Exemples de plugins fournis par défaut :

  Auto Signin : authentification directe pour certaines IP

  Brute Force : protection contre les attaques par force brute

  Stay Connected : bouton « se souvenir de moi »

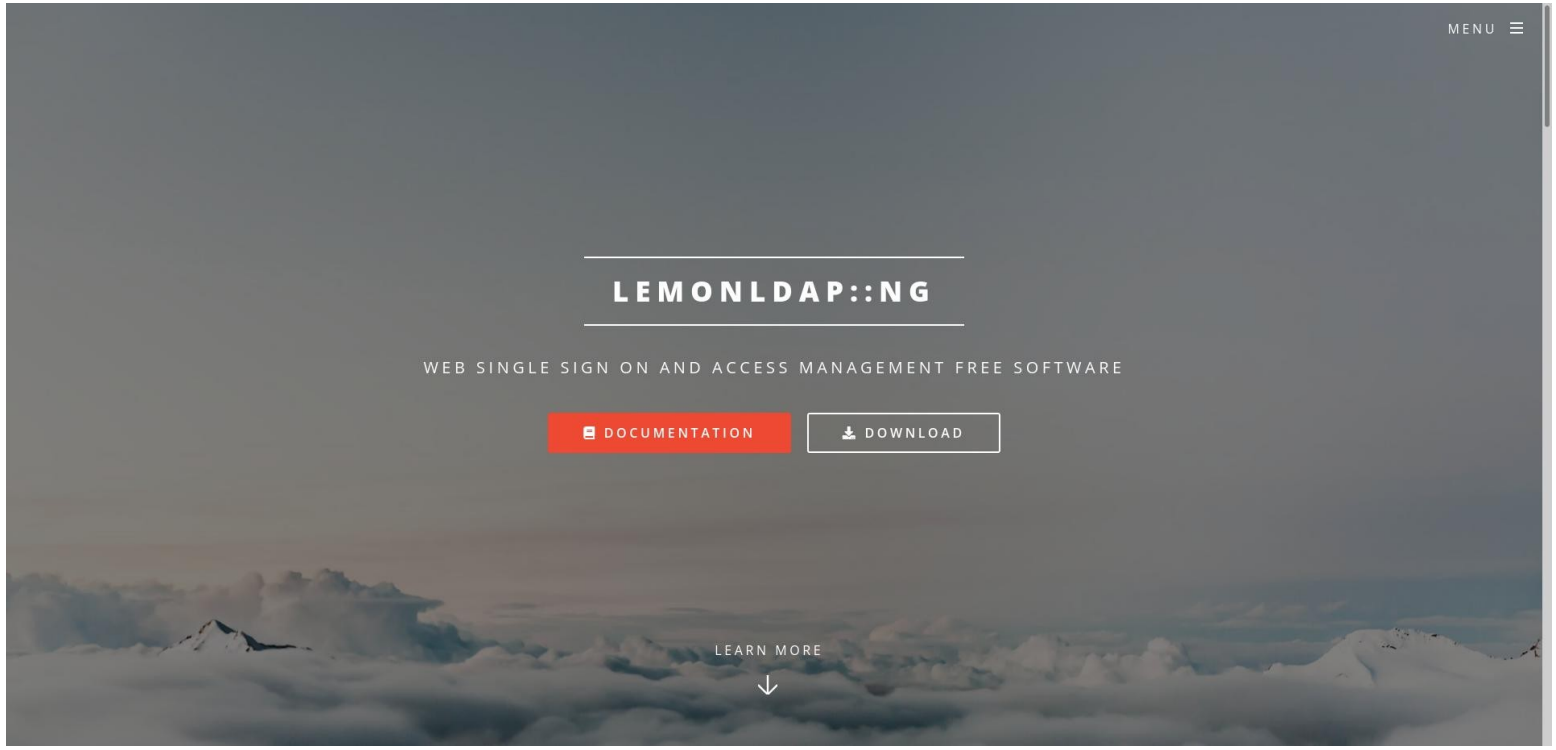
  Public Pages : créer des pages statiques utilisant le thème du portail
- Comment écrire son plugin ?
  https://lemonldap-ng.org/documentation/latest/plugincustom

Politique de mots de passe

- LemonLDAP peut s'appuyer sur la politique de mot de passe de l'annuaire
- Une politique de mots de passe locale peut maintenant être configurée (taille minimale, type de caractères,...)
- Un formulaire graphique montre quel critère est rempli

Documentation et site web

- La documentation a été réécrite en Sphinx (reStructuredText)
- Le site web a été reconstruit en pages statiques avec Templer



Se tenir informé sur LL::NG

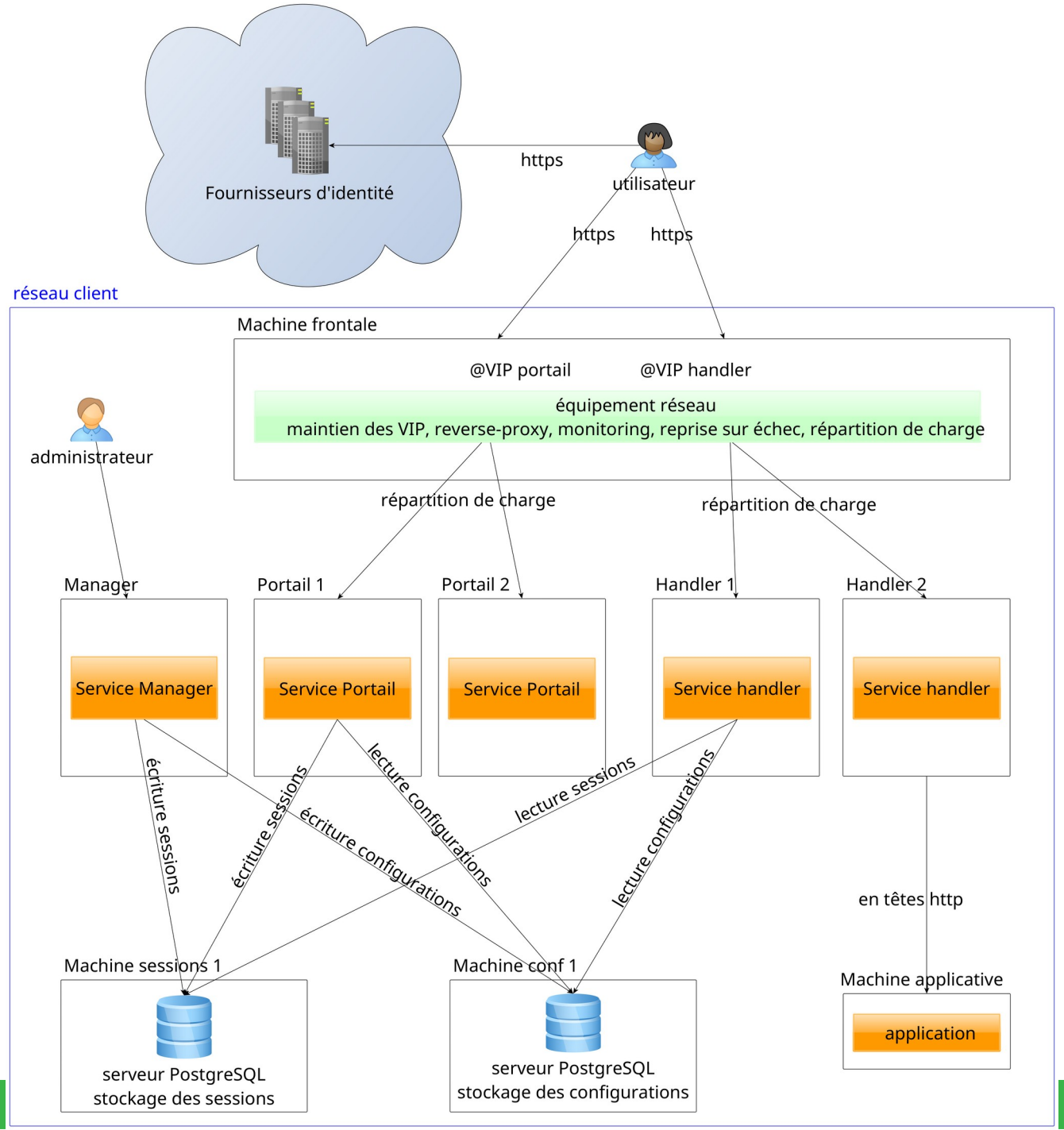
- Inscription sur la mailing-list lemonldap-ng-announces : https://mail.ow2.org/wws/subscribe/lemonldap-ng-announces
- Suivre les mises à jour du projet : https://projects.ow2.org/bin/view/lemonldap-ng/
- Notes de mise à jour : https://lemonldap-ng.org/documentation/latest/upgrade.html
- Réseaux sociaux :

  Twitter: https://twitter.com/lemonldapng/

  Facebook: https://www.facebook.com/lemonldapng/

Mise en place chez [client]

Architecture



Démarche

- Étude comparative Keycloak vs LemonLDAP::NG
  - sélection de LemonLDAP::NG. Critères déterminants :
    - gestion intégrée des applications protégées par en-têtes HTTP
    - pas de stockage des données utilisateurs dans un contexte de pure fédération (respect de la RGPD)
    - support du produit
    - logiciel souverain
- Mise en place de l'environnement de qualification
- Mise en place de l'environnement de préproduction
- Mise en place de l'environnement de production

État des lieux

- Cas d'usage : utilisateurs issus des différents « Fournisseurs d'identité » accèdent à 2-3 applications fournies par le client
- Le portail LemonLDAP::NG joue le rôle de passerelle protocolaire :
  - interconnexion aux fournisseurs d'identité en SAML
  - interconnexion aux applications par Reverse-proxy (en-têtes HTTP)
- Données personnelles issues des fournisseurs transférées aux applications au cas par cas, suivant ce dont elles ont besoin
- État des lieux :
  - Interconnexion avec le fournisseur d'identité « principal » terminée
  - Interconnexion avec un second fournisseur prévu dans l'année

Difficultés rencontrées

- Mobilisation des acteurs : fournisseurs d'identité, responsables applicatifs, infrastructure, service de certificats
- Fourniture de documents « Contrat de service » aux applicatifs pour normaliser l'interconnexion au SSO
- Organisation d'ateliers pour aider les applications à la « SSOisation »

Bilan

- Projet très positif :

pour l'utilisateur :

  - ouverture de nouveaux services applicatifs
  - amélioration du parcours (pas de ré-authentification)

pour les développeurs applicatifs :

  - externalisation complète de la fonction d'authentification (plus de problématique de changement de mot de passe,…)

pour le client :

  - ouverture de nouveaux services sécurisés (via l'interconnexion SAML) sans stockage de données personnelles
  - logiciel LemonLDAP::NG open-source, facile à maintenir et faire évoluer

Nouveautés de LemonLDAP::NG

Nouveautés de la version 2.16.1 (mars 2023)

- Meilleure gestion du versioning : passage à Semantic Versioning

  2.0.16 → 2.16.1

  Majeur.Mineur.Patch

- CVE-2023-28862 : faille de sécurité sur le handler AuthBasic avec des 2nd facteurs
- BUG : le captcha sur la page de login n'est pas affiché en cas d'erreur de backend d'authentification
- Ajout du flag « Secure » au cookie llnglanguage
- BUG : prise en compte du paramètre d'URL pour les plugins d'enregistrement de compte et de mise à jour du certificat

Nouveautés de la version 2.16.2 (mai 2023)

- Mise à jour de la librairie Jquery-UI
- Autoriser un choix d'authentification SSL avec différents backends userDB
- BUG : aucune application visible dans le menu pour tous les utilisateurs quand un utilisateur n'a le droit d'en voir aucune
- BUG : erreur SAML quand le nameID n'est pas dans la requête
- BUG : problème d'affichage dans le plugin checkUser

Nouveautés de la version 2.17 (août 2023)

- Ajout des icônes Font awesome pour personnaliser les applications du menu

- OIDC : implémentation de la déconnexion back-channel et front-channel
- OIDC : configuration de l'attribut utilisé comme pivot
- CAS : amélioration du logout
- Amélioration du logging des 2nd facteurs
- SAML : la vérification de la signature échoue sur RHEL9 + Lasso 2.8.0

Nouveautés de la version 2.17 (août 2023)

- Ajout d'une fonction « inNetwork » pour vérifier les IP
- Sécurité : redirection autorisée à cause d'une gestion incorrecte de l'échappement sur le point d'entrée userinfo
- BUG : le portail ne répond plus lorsqu'un des backends d'authentification est en timeout
- divers problèmes d'encodage
- Correction d'un BUG dans le cas d'une combinaison Kerberos + SSL
- Acceptation des URLs « mobile » comme URLs de callback OIDC (par exemple: teammail.mobile://oidc/callback)
- Ajout d'évènements jquery pour webauthn, SSL et Kerberos

Nouveautés de la version 2.17 (août 2023)

- Ajout du support Cassandra pour les configurations et les sessions
- Possibilité de définir plusieurs classes d'objet pour chercher les groupes LDAP
- BUG : erreur lors d'un changement de mot de passe lorsque l'annuaire renvoie PE_PP_CHANGE_AFTER_RESET et que le captcha est activé

Merci de votre attention

IDENTITY DAYS

24 octobre 2023 - PARIS

IDENTITY DAYS

24 octobre 2023 - PARIS

@IdentityDays #identitydays2022

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

BeyondTrust

ermetic

Exakis Nelite
MagellanPartners

FUSION DIRECTORY

jumpcloud

KERBEROS CONSULTING

Kleverware

METSYS

okta

ONE IDENTITY by Quest

ManageEngine

SailPoint

semperis

SILVERFORT

Systancia