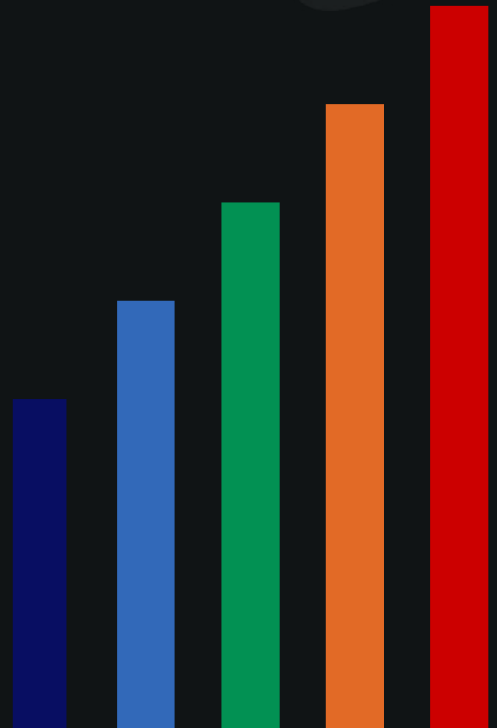
Gestion Identités, Authentification et Permissions (IAM) : Où en est-on ?

OPEN SOURCE EXPERIENCE

10 décembre 2025
Paris

Sommaire



Annuaires

Gestion d’identité

Authentification

Permissions

Annuaires

Les annuaires propriétaires

- En dehors d’Active Directory (qui n’est pas 100% compatible LDAP), il existe des alternatives payantes :
  - Oracle DSEE/OID/OUD
  - IBM Tivoly DS
  - RedHat IDM
  - ForgeRock DS
  - Ping Directory

Les annuaires Open Source

- L’offre Open Source est importante :
  - OpenLDAP (BSD style)
  - RedHat 389DS (GPL3)
  - OpenDJ (CDDL)
  - ApacheDS (AL 2.0)
  - Et quelques autres (Æ-DIR, Meerkat DSA, et quelques forks)

Projet OpenLDAP

- La version 2.6 est la dernière version LTS
  - Les logs peuvent être déportées dans un fichier distinct
  - Ajout de mécanismes de load balancing (lloadd)
  - Back-NDB est déprécié
- La version 2.5 entre en maintenance
- La version 2.4 n’est plus maintenue

En tout état de cause, un projet solide, maintenu, performant, et largement utilisé.

Apache Directory

- Un ensemble de projets d’identité :
  - Apache Directory Studio: Une GUI LDAP
  - Apache Directory Server: Un serveur LDAP en Java
  - Apache Directory LDAP API: Une API LDAP en Java
  - Apache Directory Kerby: Un serveur Kerberos en Java
  - Apache Directory SCIMple: Un serveur SCIM en Java
  - Apache Directory Fortress: Une API RBAC/ABAC en Java
  - Apache Directory Mavibot: Une base de données MVCC

Apache Directory Server

- Un serveur LDAP en Java

- Projet initié en 2002, 41 releases en 23 ans
- Denière release en Octobre 2023
- 22 000 download/mois
- Une release est attendue
- Non utilisable en production (en attendant le remplacement de la base de données par Mavibot)
- Mais idéal pour des tests unitaires

- **Utilisé dans LSC 2.2**

Apache Directory Studio

- Une GUI LDAP multi-plateforme

- Projet initié en 2005, 34 releases en 20 ans
- Denière release en Juillet 2021
- Une release est attendue

Apache Directory LDAP API

- Une API LDAP en Java, en remplacement de JNDI

- Projet initié en 2010, 54 releases en 15 ans
- Denière release en Août 2024
- Une release est attendue

- **Utilisé dans LSC 2.2**

Apache Directory Scimple

- Implémentation de la spécification SCIM 2.0

- Projet initié en 2018, 1ère release en Janvier 2024
- Une release est en préparation

Apache Directory Fortress

- Une API RBAC en Java

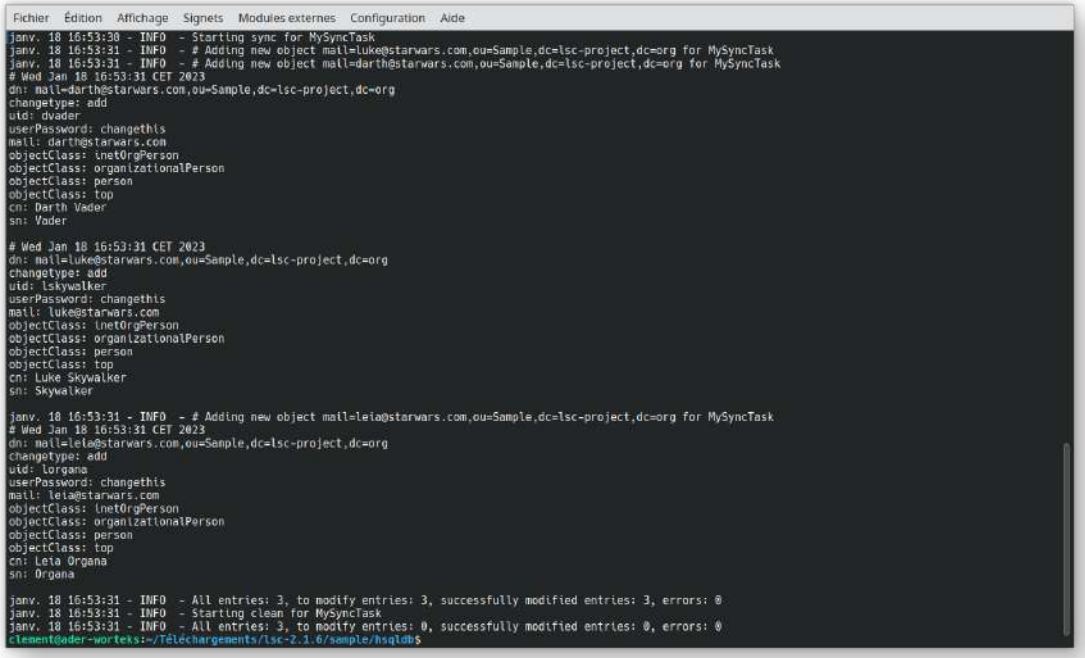
- Projet initié en 2009, 1ère release en Avril 2015
- 17 releases en 10 ans
- Dernière release en Juillet 2025

Gestion d’identité

LSC

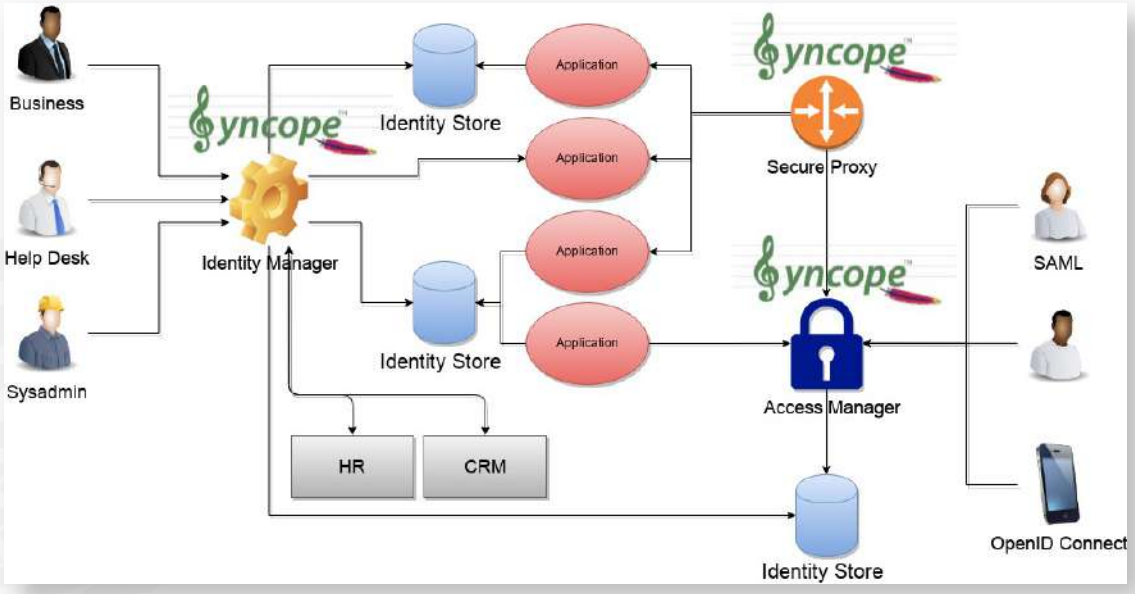
LDAP Synchronization Connector

- Synchronisation des identités et des groupes
- Pas d’interface graphique
- Version 2.2 sortie en 2025
- Système de plugins



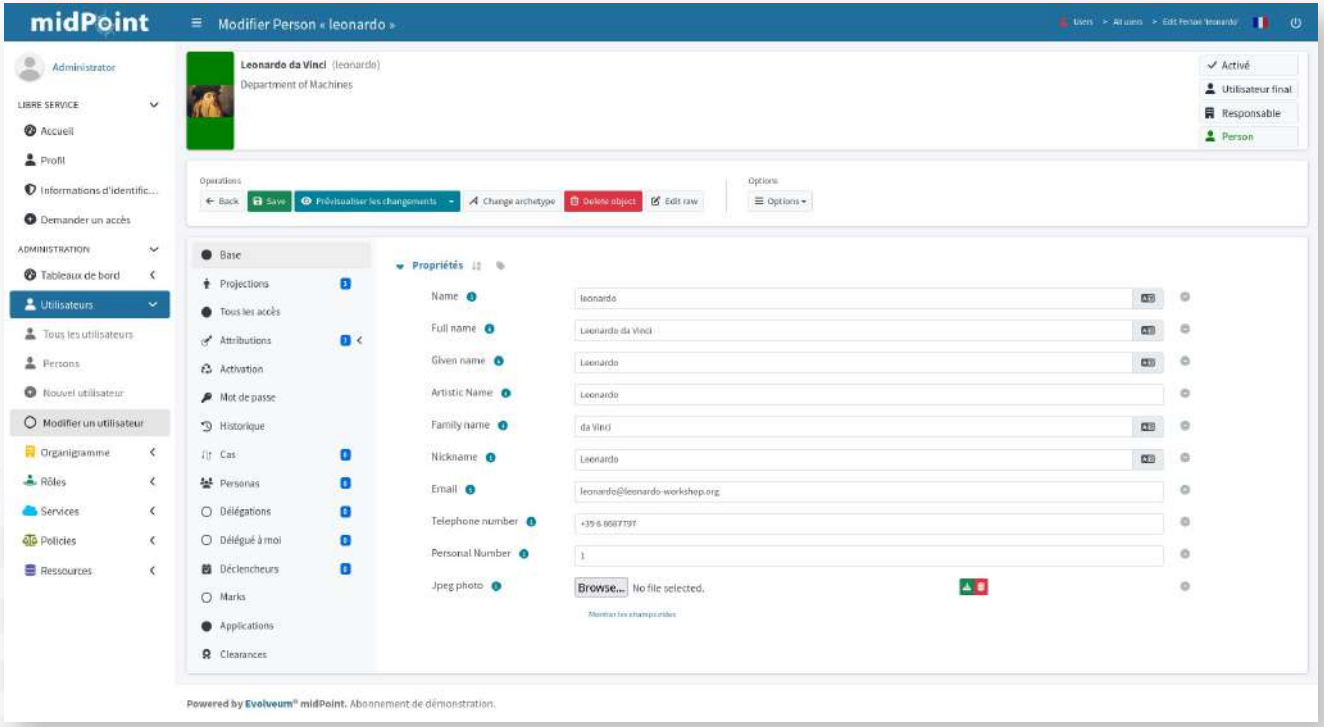
Apache Syncope

- Gestion des identités
- Gestion des accès



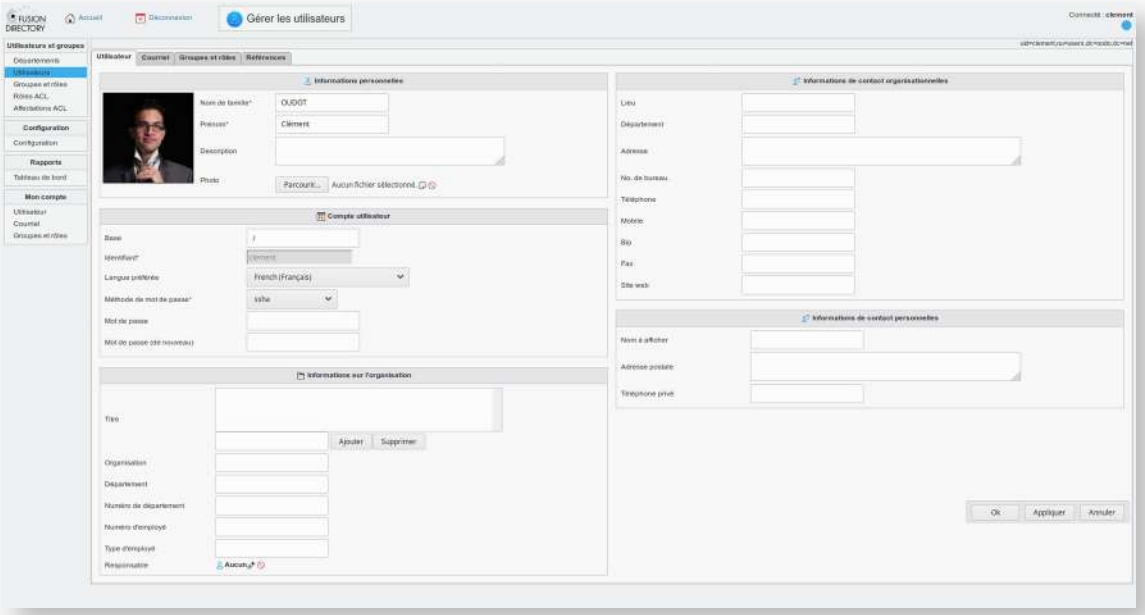
MidPoint

- Interface de gestion des données
- Synchronisation des identités
- Workflows
- Version 4.9.4 publiée en août 2025



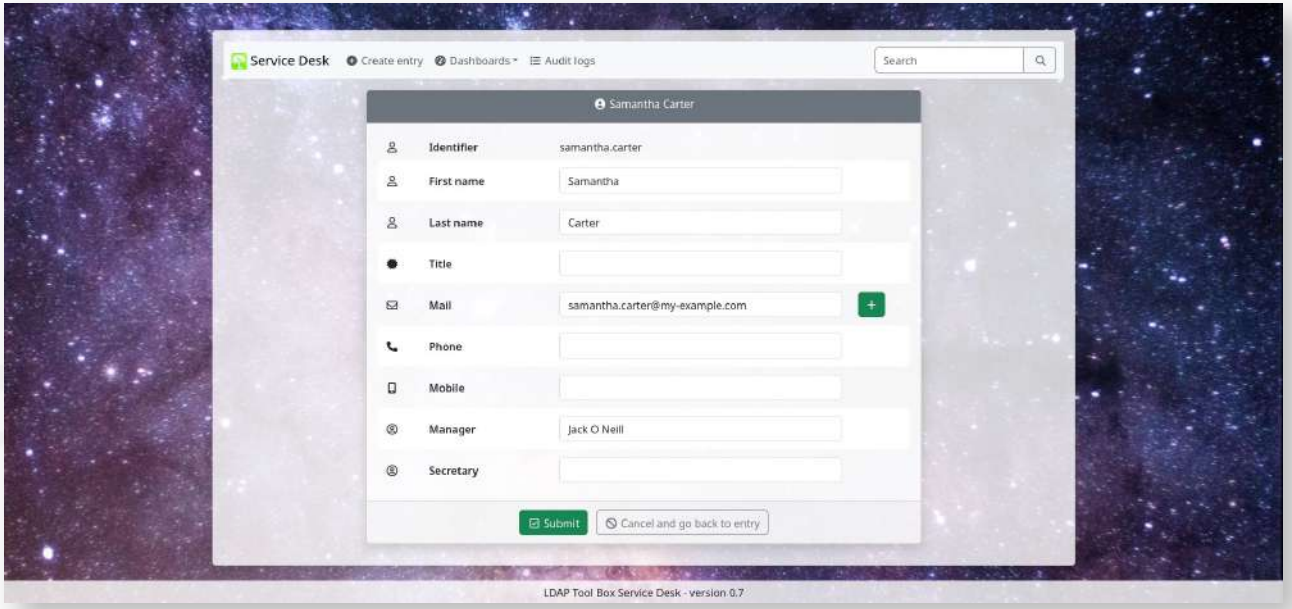
Fusion Directory

- Interface de gestion des identités
- Utilise LSC pour les synchronisations
- Wortkflows
- Délégation de gestion
- Compatible SupAnn



LTB Service Desk

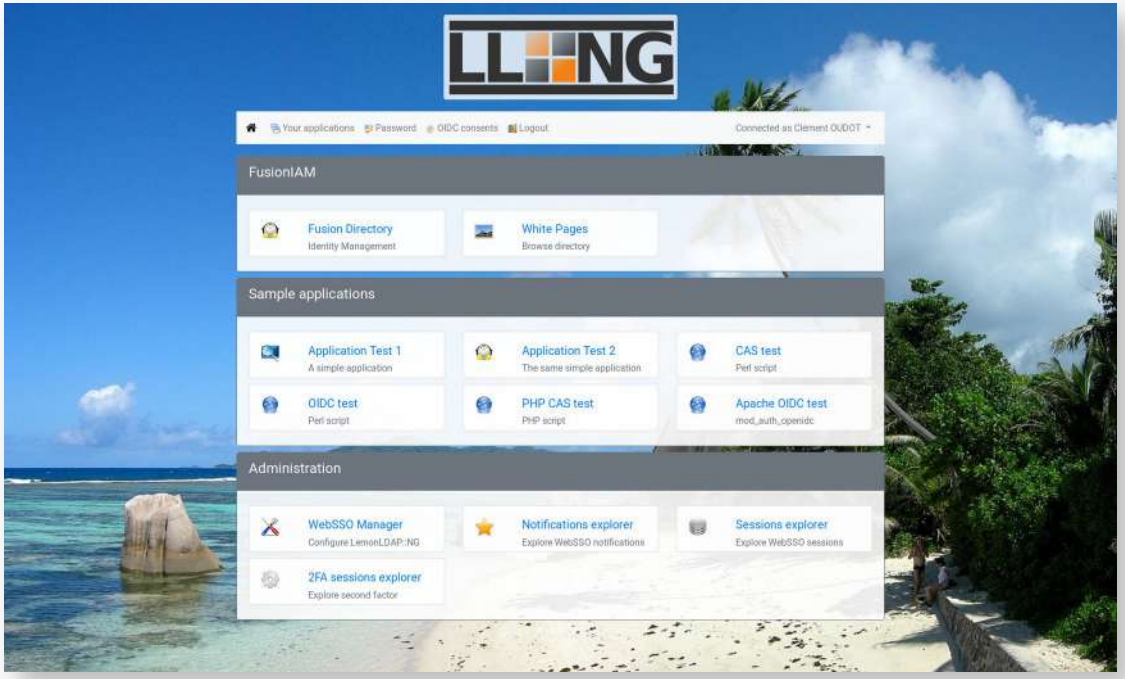
- Gestion simple des identités
- Statut du compte
- Tableaux de bord
- Audit



Authentification

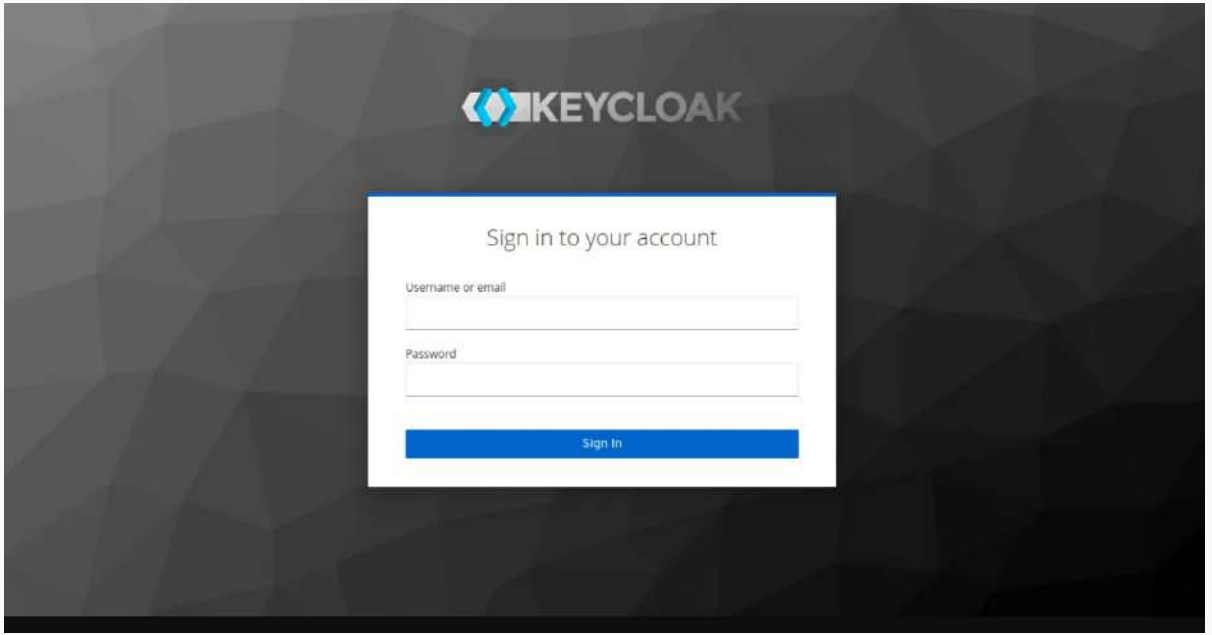
LemonLDAP::NG

- Authentification SSO
- Protocoles CAS, SAML et OpenID Connect
- 2FA
- Version 2.22 en octobre 2025



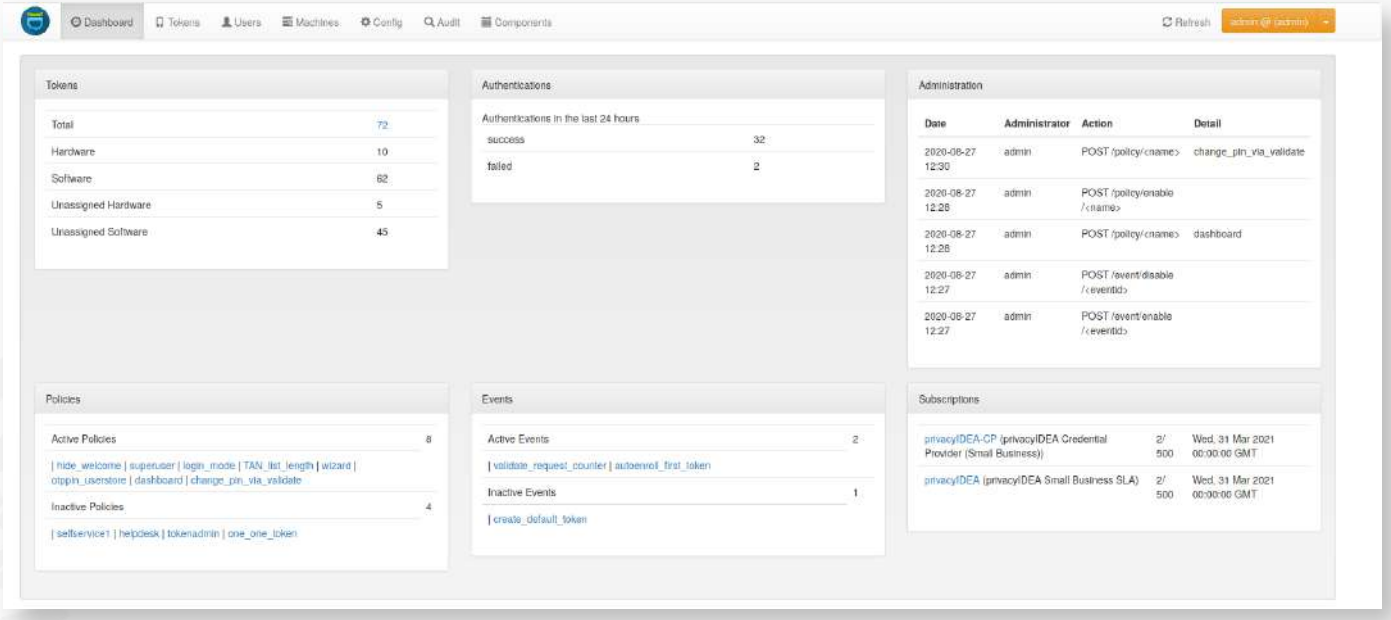
Keycloak

- Authentification SSO
- Protocoles SAML et OpenID Connect
- 2FA
- Version 26.4.7 en Décembre 2025



Privacy ID3A

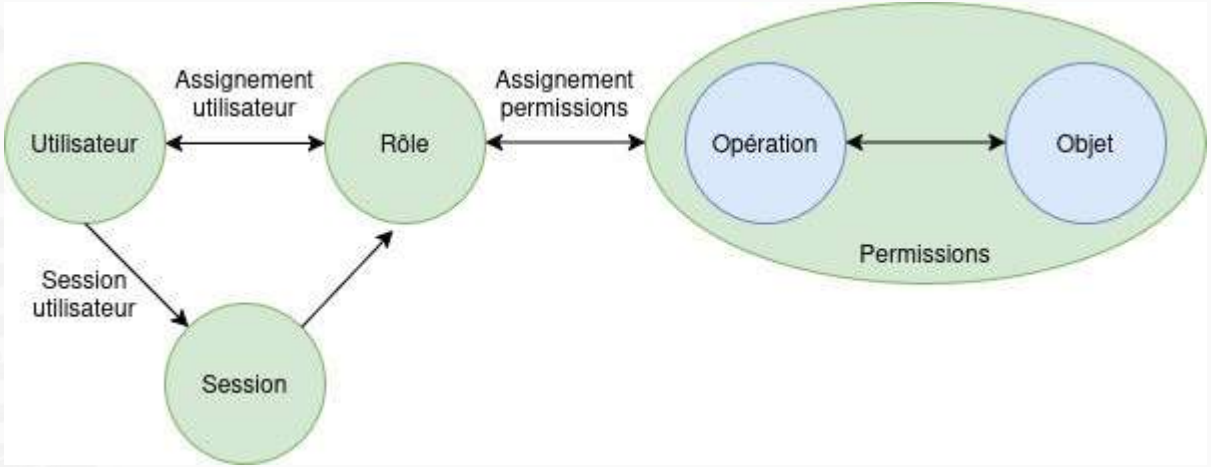
- Authentification mutli-facteur
- Application mobile
- Gestion de jetons
- Version 3.12 en septembre 2025



Permissions

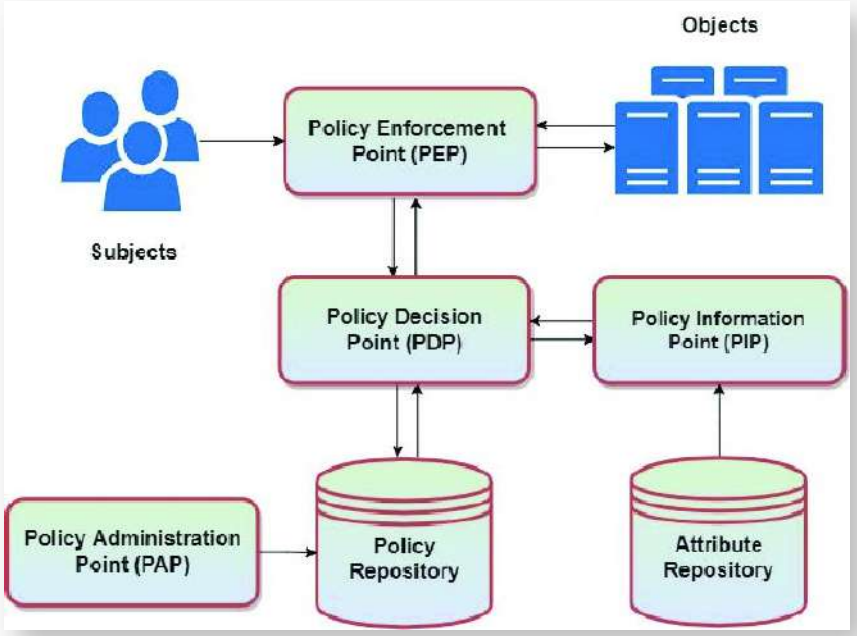
RBAC (2004)

- RBAC (Role-Based Access Control) est un modèle de contrôle d’accès basé sur les rôles
- NIST/ANSI/INCITS RBAC standard (2004)
- Début des travaux en 1992 (David Ferraiolo et Rick Kuhn)



ABAC (2016)

- ABAC (Attribute-Based Access Control) est un modèle de contrôle d'accès basé sur les attributs
- Également David Ferraiolo et Rick Kuhn
- https://csrc.nist.gov/files/pubs/sp/800/162/upd2/final/docs/sp800_162_draft.pdf



NGAC (2020)

- NGAC (Next-Generation Access Control) est un modèle de contrôle d’accès basé sur une modélisation par graphe
- Toujours David Ferraiolo...
- https://standards.globalspec.com/std/14649620/incits-565

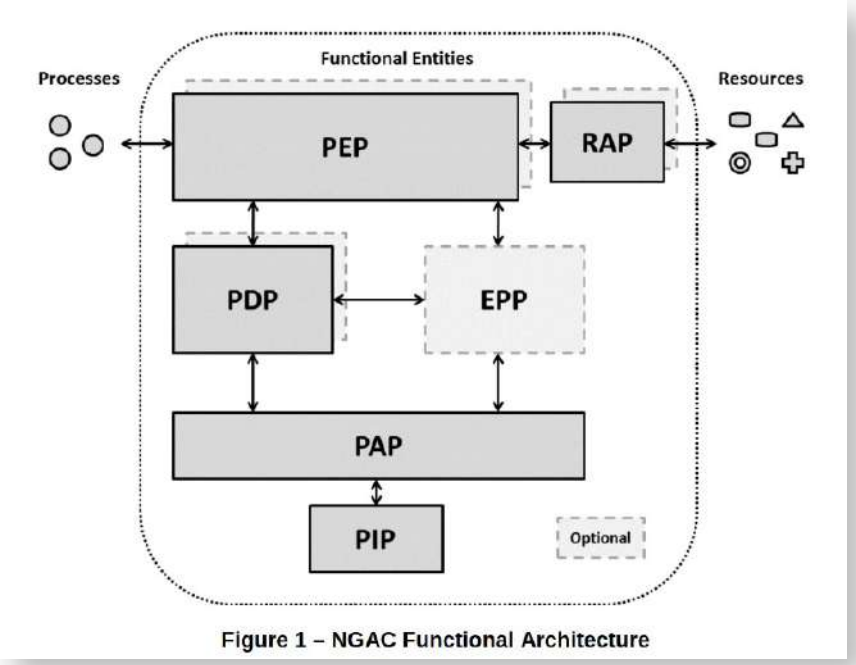


Figure 1 – NGAC Functional Architecture

NGAC exemple

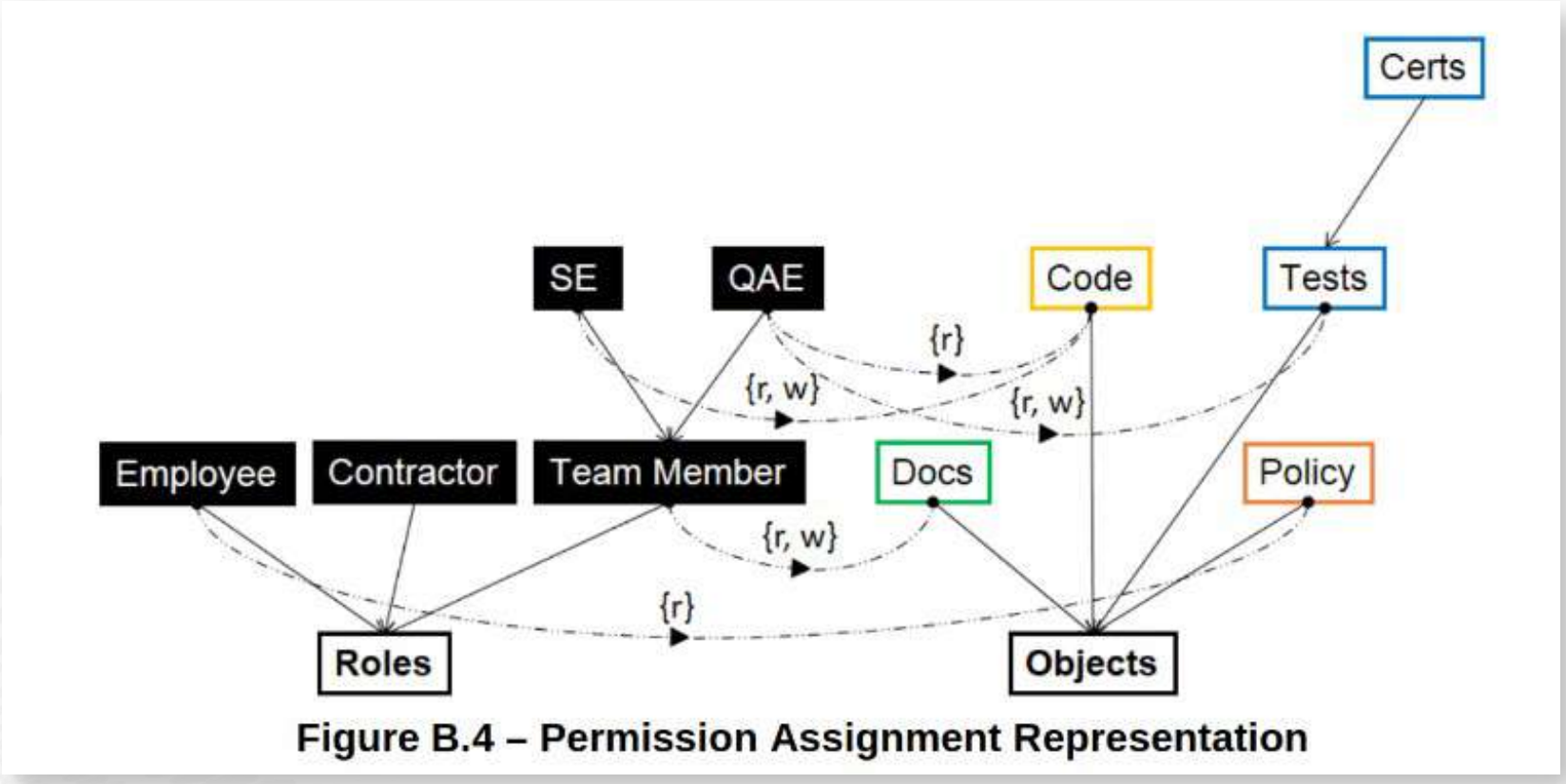


Figure B.4 – Permission Assignment Representation

Implementations OSS

- **RBAC** : Apache Directory Fortress
- **ABAC** :
  - Apache Directory Fortress
  - XACML (https://authzforce.ow2.org/)
  - OpenAZ (https://github.com/apache/incubator-retired-openaz)
- **NGAC** :
  - Policy Machine Core (https://github.com/usnistgov/policy-machine-core)

www.worteks.com

info@worteks.com
+33 1 84 20 86 47
worteks_com
worteks