



Gestion Identités, Authentification et Permissions



20 octobre 2025
Paris

Sommaire

Annuaire

Gestion d'identité

Authentification

Permissions





Annuaire

Les annuaires propriétaires

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



Les annuaires Open Source

- L'offre Open Source est importante :
 - OpenLDAP
 - RedHat 389DS
 - OpenDJ
 - ApacheDS



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 (lload)
 - Back-NDB est déprécié
- La version 2.4 n'est plus maintenue
- La version 2.5 entre en maintenance

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
- Dernière release en Octobre 2023
- 22 000 download/mois
- Une release est attendue, mais dépend d'une release de Apache LDAP API, qui dépend d'une release de Apache MINA (dernière release datant de décembre 2024)
- 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
- Dernière release en Juillet 2021
- Une release est attendue, mais dépend d'une release de Apache Directory Server, de Apache LDAP API, qui dépend d'une release de Apache MINA (dernière release datant de décembre 2024)



Apache Directory LDAP API



- Une API LDAP en Java, en remplacement de JNDI
- Projet initié en 2010, 54 releases en 15 ans
- Dernière release en Août 2024
- Une release est attendue, mais dépend d'une release de Apache MINA (dernière release datant de décembre 2024)
- **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 Juin 2025





Gestion d'identité

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

```
Fichier  Edition  Affichage  Signets  Modules externes  Configuration  Aide
janv. 18 16:53:30 - INFO - Starting sync for MySyncTask
janv. 18 16:53:31 - INFO - # Adding new object mail=luke@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
janv. 18 16:53:31 - INFO - # Adding new object mail=darth@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=darth@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: dvader
userPassword: changethis
mail: darth@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Darth Vader
sn: Vader

# Wed Jan 18 16:53:31 CET 2023
dn: mail=luke@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lskywalker
userPassword: changethis
mail: luke@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Luke Skywalker
sn: Skywalker

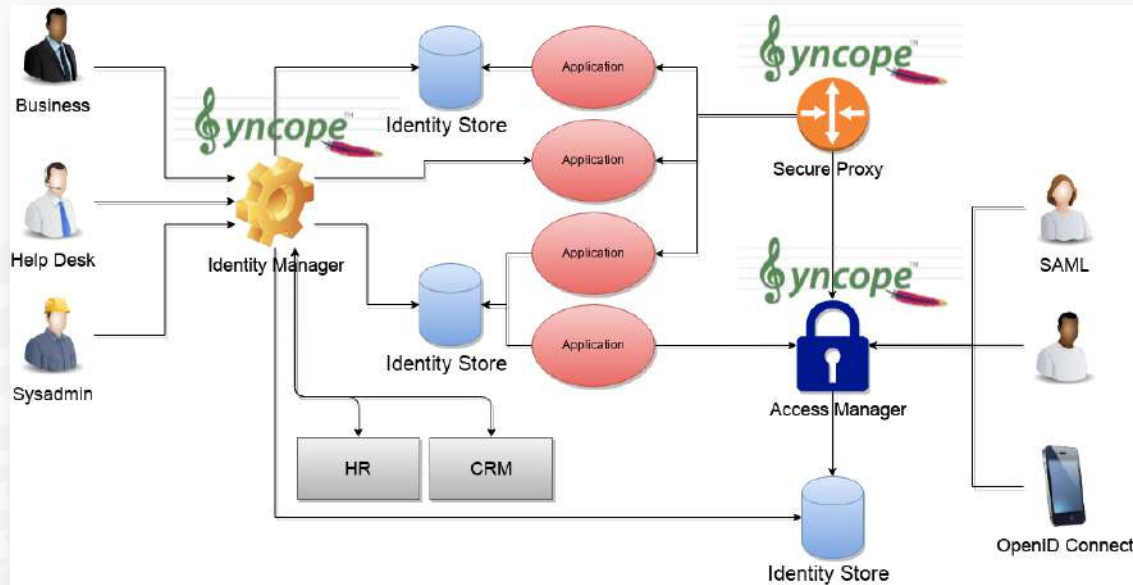
janv. 18 16:53:31 - INFO - # Adding new object mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lorgana
userPassword: changethis
mail: leia@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Leia Organa
sn: Organa

janv. 18 16:53:31 - INFO - All entries: 3, to modify entries: 3, successfully modified entries: 3, errors: 0
janv. 18 16:53:31 - INFO - Starting clean for MySyncTask
janv. 18 16:53:31 - INFO - All entries: 3, to modify entries: 0, successfully modified entries: 0, errors: 0
clement@adeo-worleksi:~/Téléchargements/lsc-2.3.6/sample/hsqldb$
```

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

The screenshot displays the MidPoint web interface for editing a user profile. The header shows 'midPoint' and 'Modifier Person « leonardo »'. The left sidebar contains navigation menus for 'LIBRE SERVICE' (Accueil, Profil, Informations d'identification, Demander un accès) and 'ADMINISTRATION' (Tableaux de bord, Utilisateurs, Tous les utilisateurs, Personnes, Nouveau utilisateur, Modifier un utilisateur, Organigramme, Rôles, Services, Politiques, Ressources). The main content area shows the user 'Leonardo da Vinci (leonardo)' from the 'Department of Machines'. It includes a profile picture, status (Active), and role (Personne). Below this are tabs for 'Base' and 'Propriétés'. The 'Propriétés' tab is active, showing fields for Name, Full name, Given name, Artistic Name, Family name, Nickname, Email, Telephone number, Personal Number, and Jpeg photo. The 'Base' tab shows a list of properties with icons for each. The footer indicates 'Powered by Evolveum® midPoint. Abonnement de démonstration.'

Fusion Directory



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

A screenshot of the Fusion Directory web application interface. The interface is in French and shows the 'Gérer les utilisateurs' (Manage users) section. On the left is a sidebar with navigation links: 'Utilisateurs et groupes', 'Configuration', 'Rapports', 'Mon compte', and 'Utilisateur'. The main area is divided into several tabs: 'Utilisateur', 'Groupes et rôles', and 'Références'. The 'Utilisateur' tab is active, showing a form for user management. The form includes sections for 'Informations personnelles' (Name, Surname, First name, Description, Photo), 'Compte utilisateur' (Base, Identifiant, Langue préférée, Méthode de mot de passe, Mot de passe, Mot de passe (re-saisir)), 'Informations de contact organisationnelles' (Lien, Département, Adresse, No. de bureau, Téléphone, Mobile, Fax, Site web), 'Informations de contact personnelles' (Nom à afficher, Adresse postale, Téléphone privé), and 'Informations sur l'organisation' (Titre, Organisation, Département, Numéro de département, Numéro d'employé, Type d'emploi, Responsabilité). At the bottom right are buttons for 'OK', 'Appliquer', and 'Annuler'.

LTB Service Desk

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



The screenshot shows the 'Service Desk' application interface. At the top, there's a navigation bar with 'Service Desk', 'Create entry', 'Dashboards', and 'Audit logs'. A search bar is on the right. The main content area displays a user profile for 'Samantha Carter'. The profile form includes fields for Identifier (samantha.carter), First name (Samantha), Last name (Carter), Title, Mail (samantha.carter@my-example.com), Phone, Mobile, Manager (Jack O'Neill), and Secretary. A green '+' button is next to the Mail field. At the bottom, there are 'Submit' and 'Cancel and go back to entry' buttons. The footer text reads 'LDAP Tool Box Service Desk - version 0.7'.

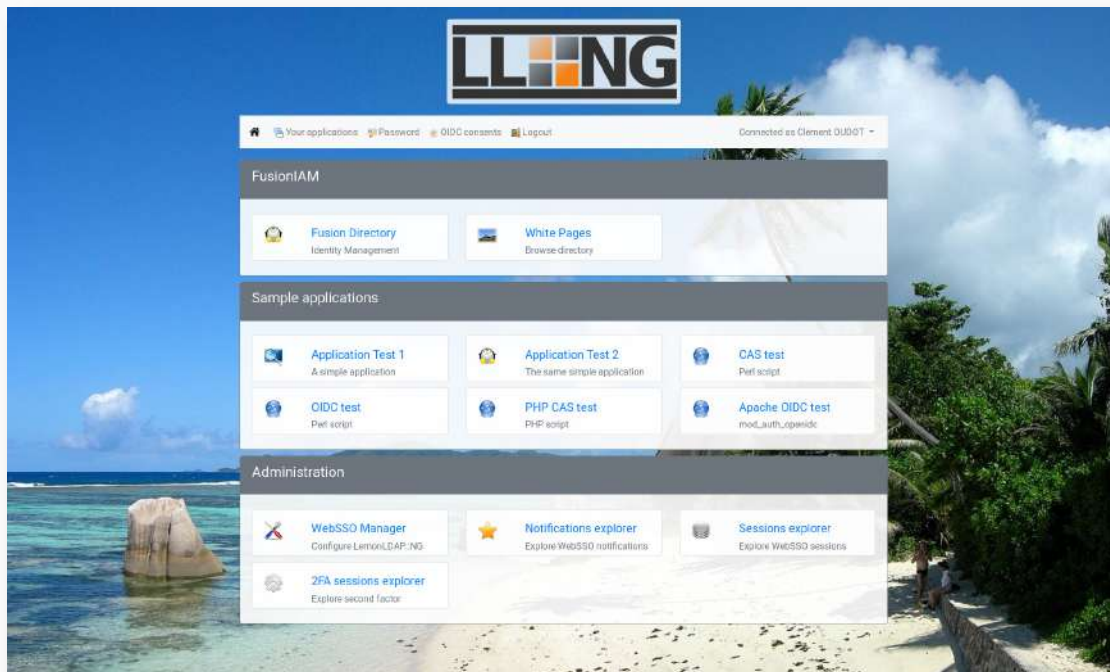
Samantha Carter	
Identifier	samantha.carter
First name	Samantha
Last name	Carter
Title	
Mail	samantha.carter@my-example.com
Phone	
Mobile	
Manager	Jack O'Neill
Secretary	



Authentication

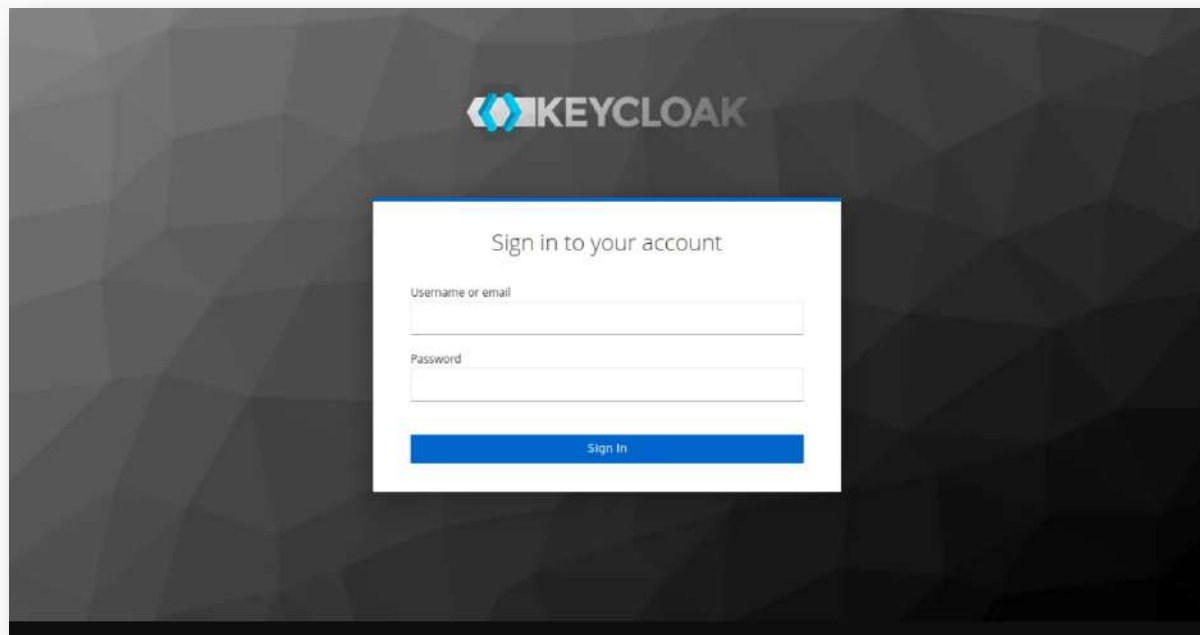
LemonLDAP::NG

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



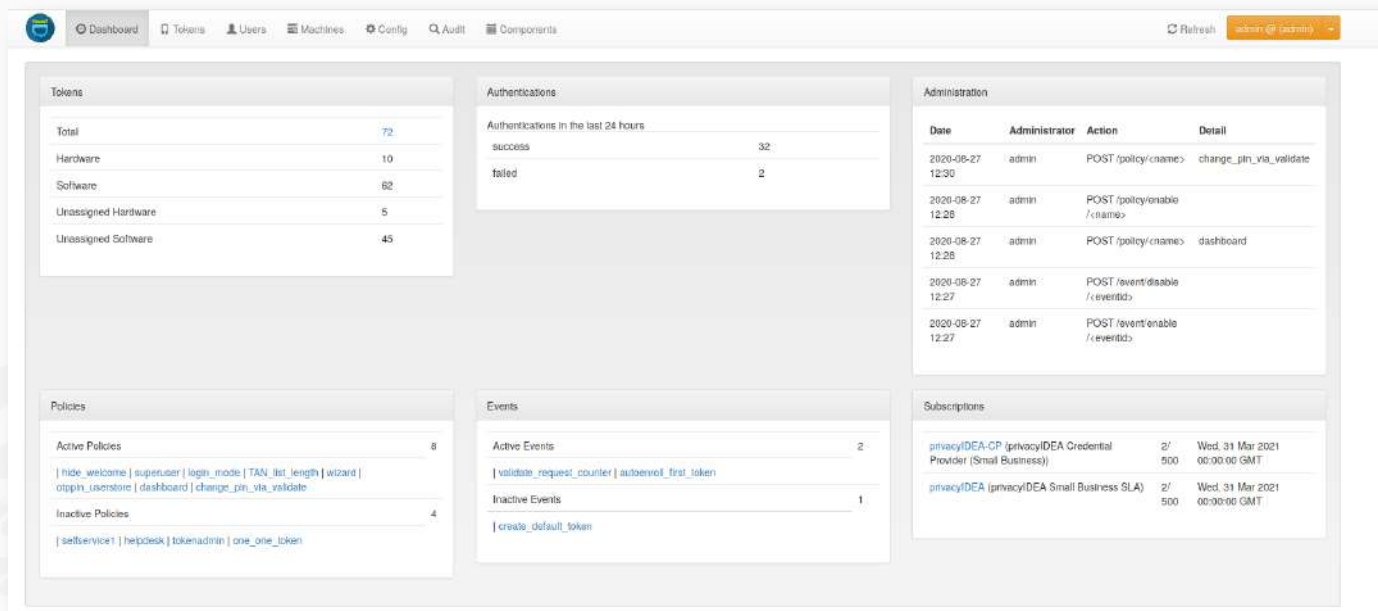
Keycloak

- Authentication SSO
- Protocoles SAML et OpenID Connect
- 2FA
- Version 26.4 en octobre 2025



Privacy ID3A

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

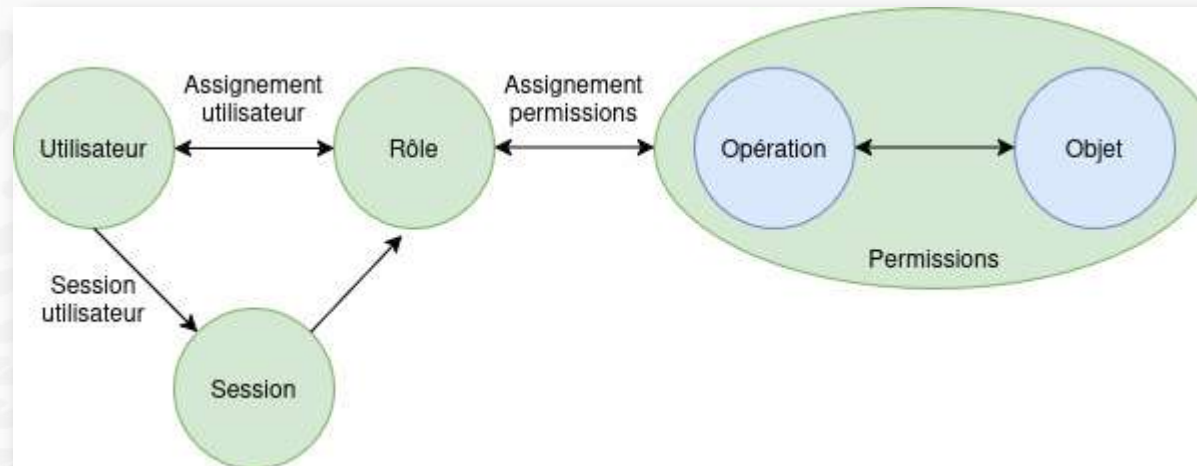




Permissions

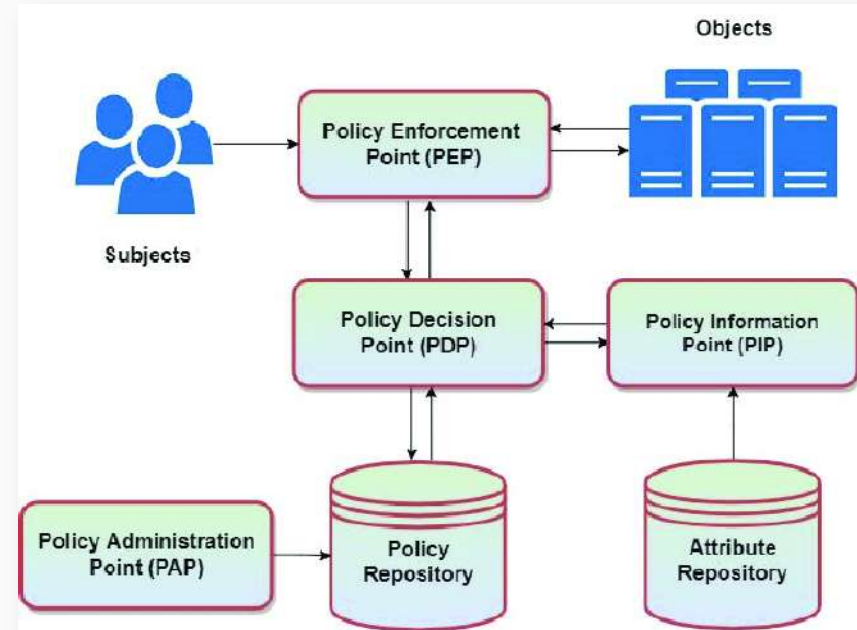
RBAC (2004)

- 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)



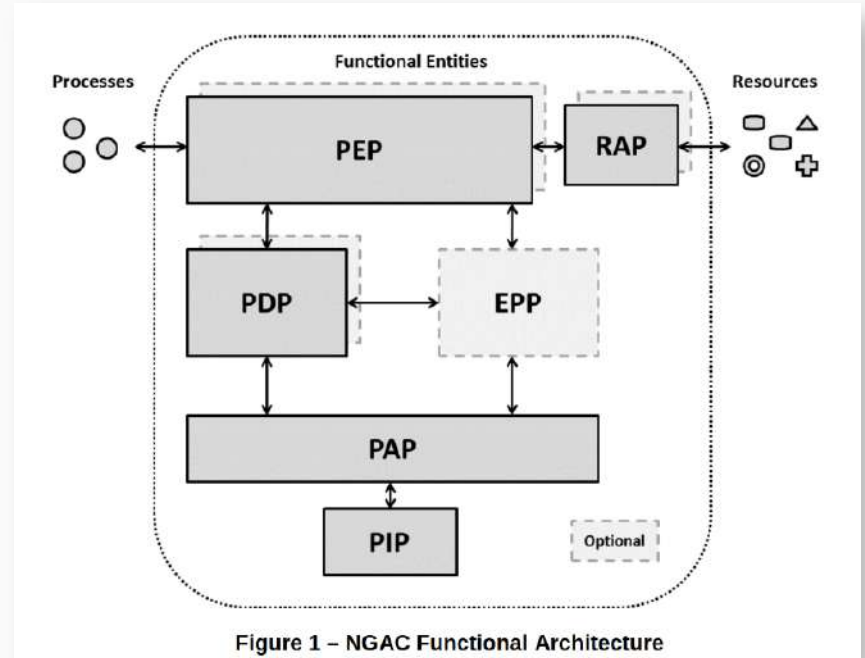
ABAC (2016)

- 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>



NGAC example

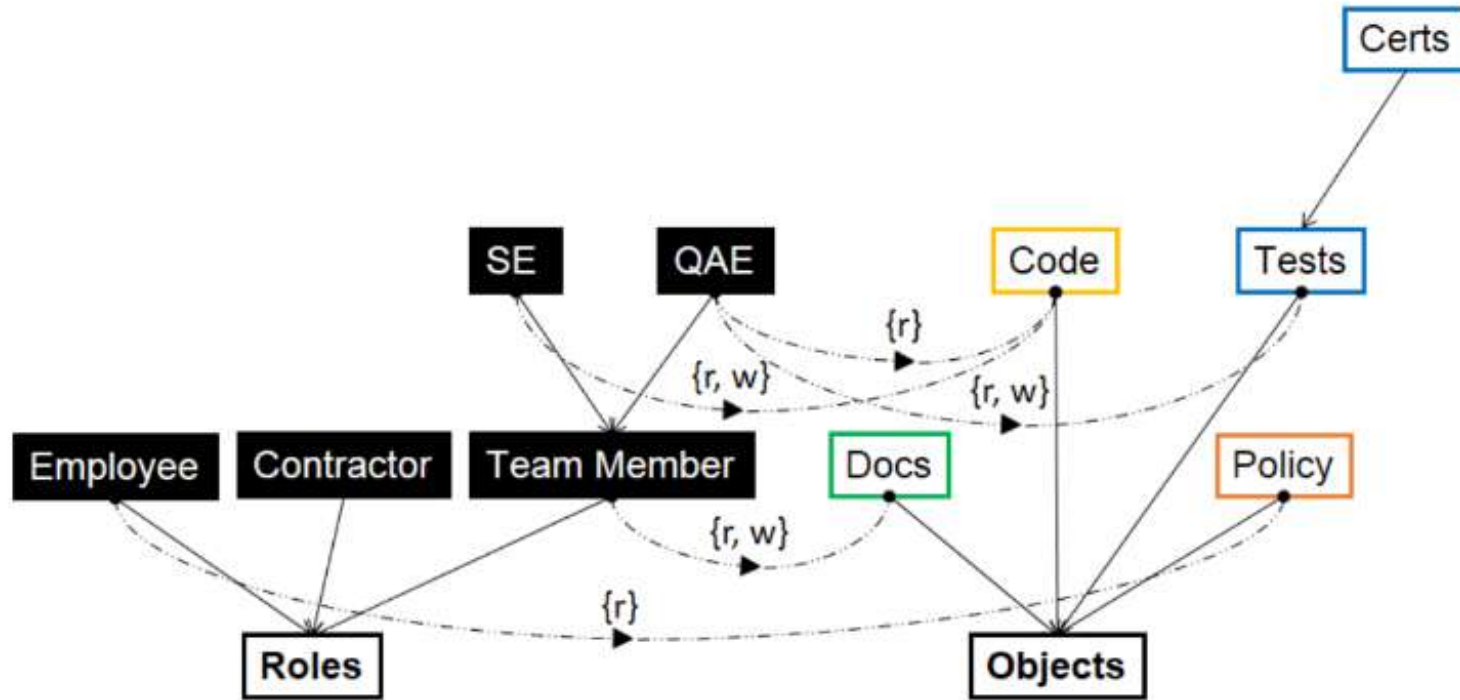


Figure B.4 – Permission Assignment Representation

Implementations Open Source

- **RBAC** : Apache Directory Fortress
- **ABAC** :
 - Apache Directory Fortress
 - XACML (<https://authzforce.ow2.org/>)
 - OpenAZ
(<https://github.com/apache/incubator-retired-openaz>)





www.worteks.com

✉ info@worteks.com

☎ +33 1 84 20 86 47

🌐 worteks_com

🌐 [worteks](https://www.linkedin.com/company/worteks)