



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



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
- Dernière 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
- Dernière 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
- Dernière release en Août 2024
- Une release est attendue
- Utilisé dans LSC 2.2

Apache Directory Scimble



- Implémentation de la spécification SCIM 2.0
- Projet initié en 2018, 1ère release en Janvier 2024
- Une release est en préparation

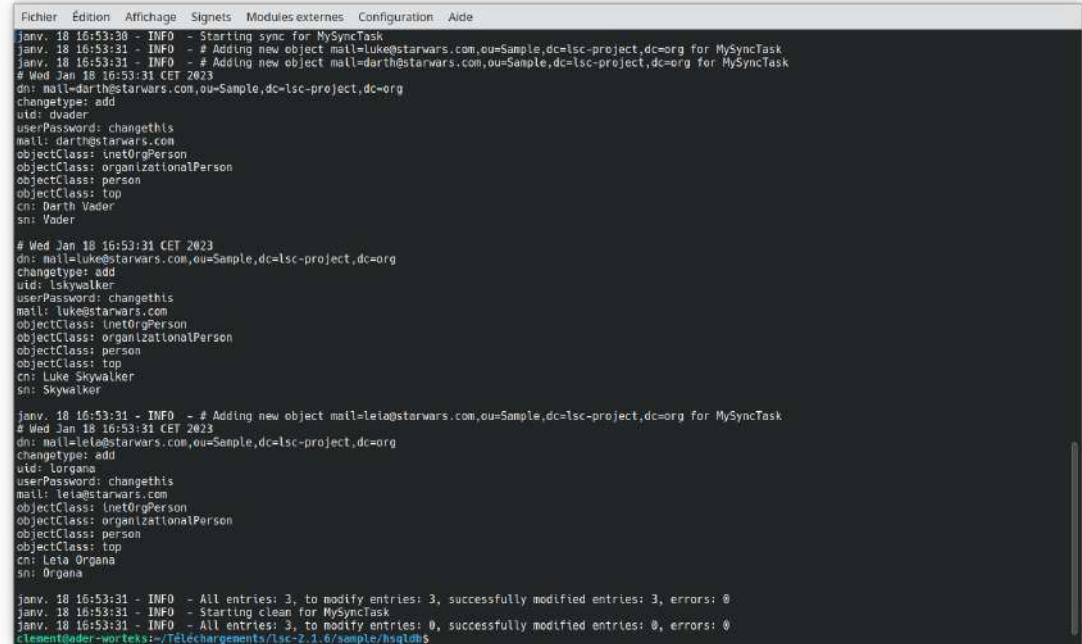
Apache Directory Fortress



- 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

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



```
Fichier Édition 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: darvor
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

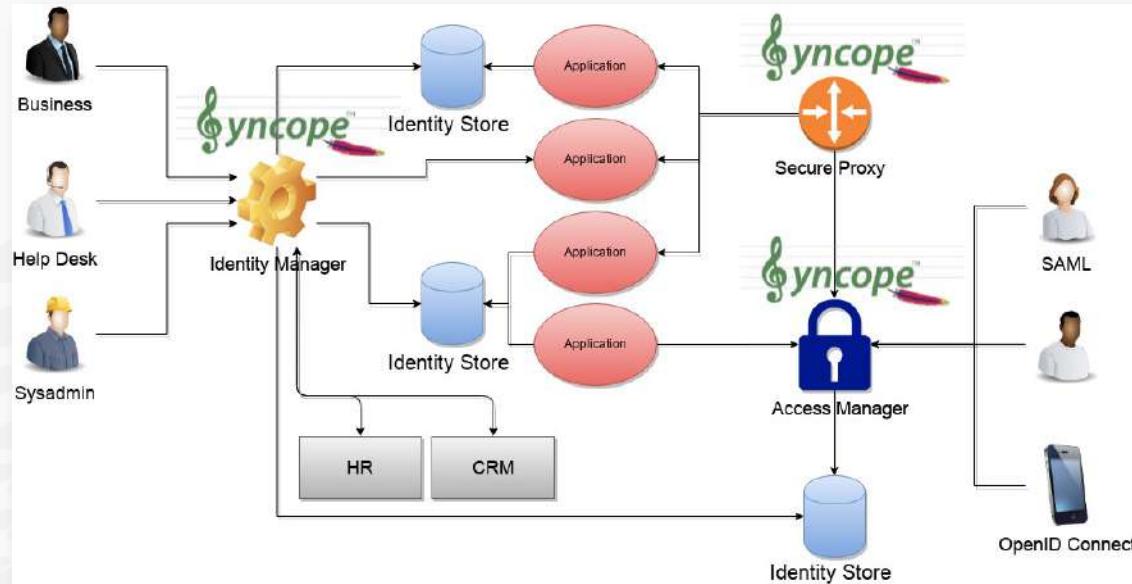
janv. 18 16:53:31 - INFO - # Adding new object mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lorgan
userPassword: changethis
mail: leia@starwars.com
objectClass: inetOrgPerson
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@ader-warreks:~/Téléchargements/lsc-2.1.6/sample/hsqlib$
```

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

A screenshot of the midPoint web interface. The title bar says "midPoint - Modifier Person < leonardo >". The left sidebar shows a navigation tree under "Utilisateurs": "Tous les utilisateurs", "Persons", "Nouvel utilisateur", and "Modifier un utilisateur" (which is selected). The main content area shows a summary for "Leonardo da Vinci (leonardo)" from "Department of Machines". Below it, the "Base" section lists "Projections", "Tous les accès", "Attributions", "Activation", "Mot de passe", and "Historique". The "Propriétés" section displays various attributes with their values:

Attribut	Valeur
Name	leonardo
Full name	Leonardo da Vinci
Given name	Leonardo
Artistic Name	Leonardo
Family name	da Vinci
Nickname	Leontardo
Email	leonardo@leonardo-workshop.org
Telephone number	+39 6 6667797
Personal Number	1
Jpeg photo	No file selected.

A "Browse..." button is available for the jpeg photo field. The bottom of the page is 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

The screenshot shows the 'Gérer les utilisateurs' (Manage users) screen in the Fusion Directory web interface. A user profile for 'Clement' is selected. The interface is divided into several sections:

- Informations personnelles:** Includes fields for Name (Clement), First name (Olivier), Description, and Photo (Browse).
- Compte utilisateur:** Includes fields for Base (Y), Identifier (Clement), Language (French (Français)), Method of password change (When), and Mot de passe (Password).
- Informations sur l'organisation:** Includes fields for Title, Organization, Department, and Numéro de département.
- Informations de contexte organisationnelles:** Includes fields for Bureau, Department, Address, Office number, Telephone, Mobile, Bio, Fax, and Site web.
- Informations de contexte personnelles:** Includes fields for Nom à afficher, Adresse postale, and Téléphone privé.

At the bottom right are buttons for Ok, Appliquer (Apply), and Annuler (Cancel).

LTB Service Desk

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

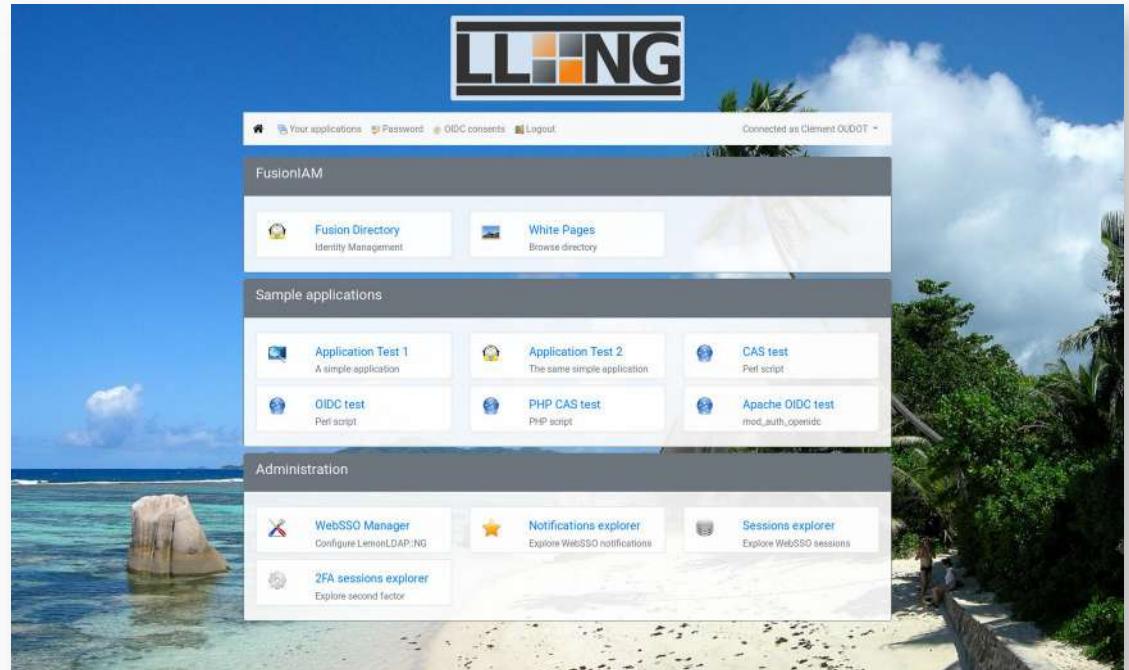


A screenshot of the LTB Service Desk application. The interface is set against a background of a star-filled galaxy. At the top, there's a navigation bar with links for 'Create entry', 'Dashboards', and 'Audit logs'. A search bar is located in the top right corner. The main area shows a modal dialog for editing a user profile. The dialog is titled 'Samantha Carter' and contains fields for 'Identifier' (samantha.carter), 'First name' (Samantha), 'Last name' (Carter), 'Title' (empty), 'Mail' (samantha.carter@my-example.com), 'Phone' (empty), 'Mobile' (empty), 'Manager' (Jack O'Neill), and 'Secretary' (empty). There are 'Submit' and 'Cancel and go back to entry' buttons at the bottom. The footer of the application displays the text 'LDAP Tool Box Service Desk - version 0.7'.

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

The screenshot shows the Privacy ID3A dashboard with several sections:

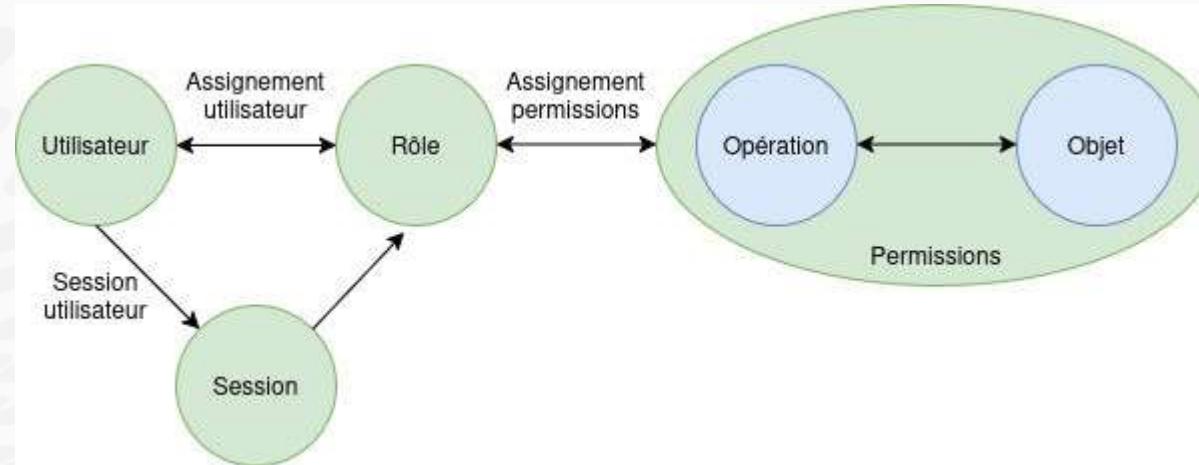
- Tokens:** Total tokens: 72. Breakdown: Hardware (10), Software (62), Unsigned Hardware (5), Unsigned Software (45).
- Authentications:** Authentications in the last 24 hours: success (32), failed (2).
- Administration:** Log of administrator actions:

Date	Administrator	Action	Detail
2020-08-27 12:30	admin	POST /policy/cname	change_pin_via_validate
2020-08-27 12:26	admin	POST /policy/enable	/<name>
2020-08-27 12:26	admin	POST /policy/cname	dashboard
2020-08-27 12:27	admin	POST /event/disable	/<eventid>
2020-08-27 12:27	admin	POST /event/enable	/<eventid>
- Policies:** Active Policies (8): [nice_welcome | superuser | login_mode | TAN_list_length | wizard | otppin_userstore | dashboard | change_pin_via_validate]. Inactive Policies (4): [selfservice1 | helpdesk | tokenadmin | one_one_token].
- Events:** Active Events (2): [validation_request_counter | autoenroll_first_token]. Inactive Events (1): [create_default_token].
- Subscriptions:** Subscriptions for privacyIDEA-CP and privacyIDEA Small Business SLA.

Permissions

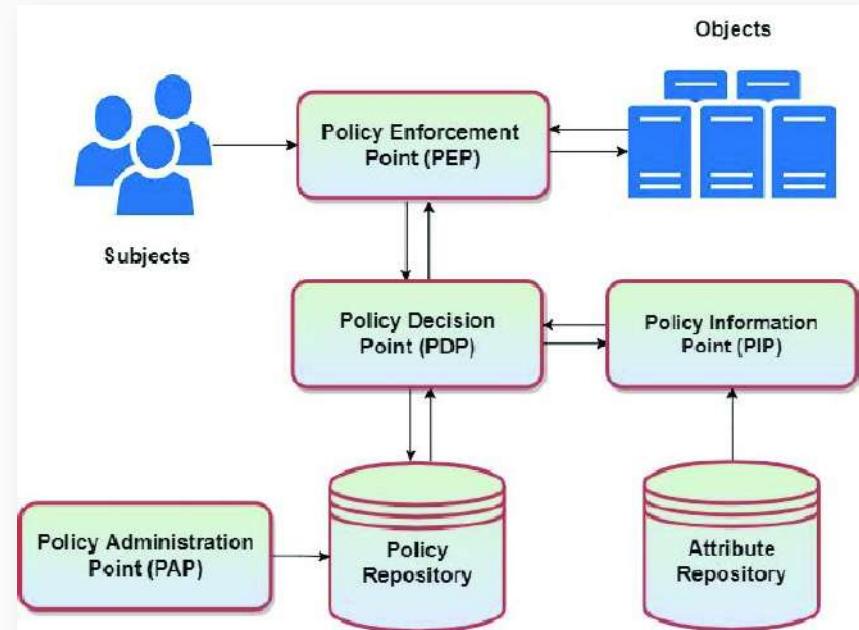
RBAC (2004)

- 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)



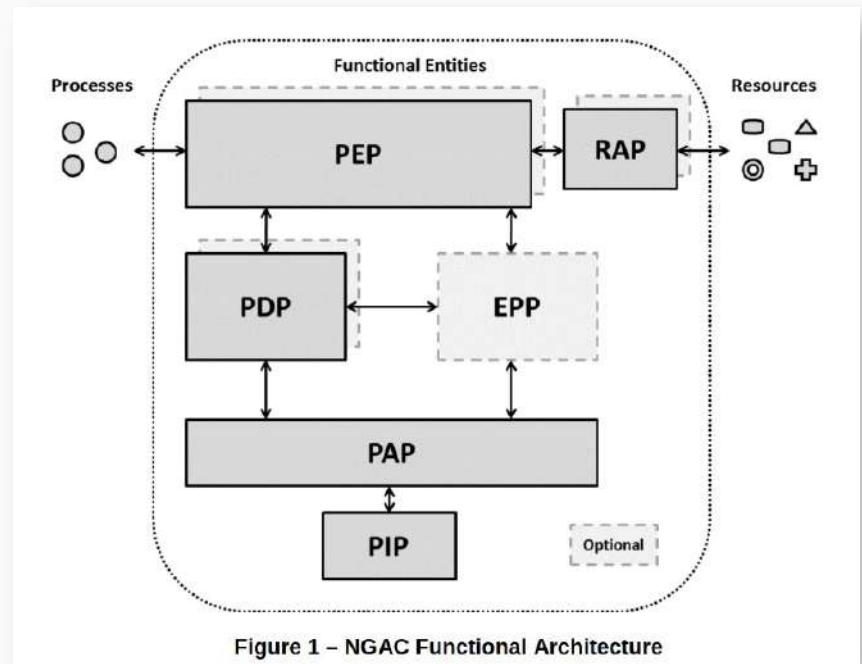
ABAC (2016)

- 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

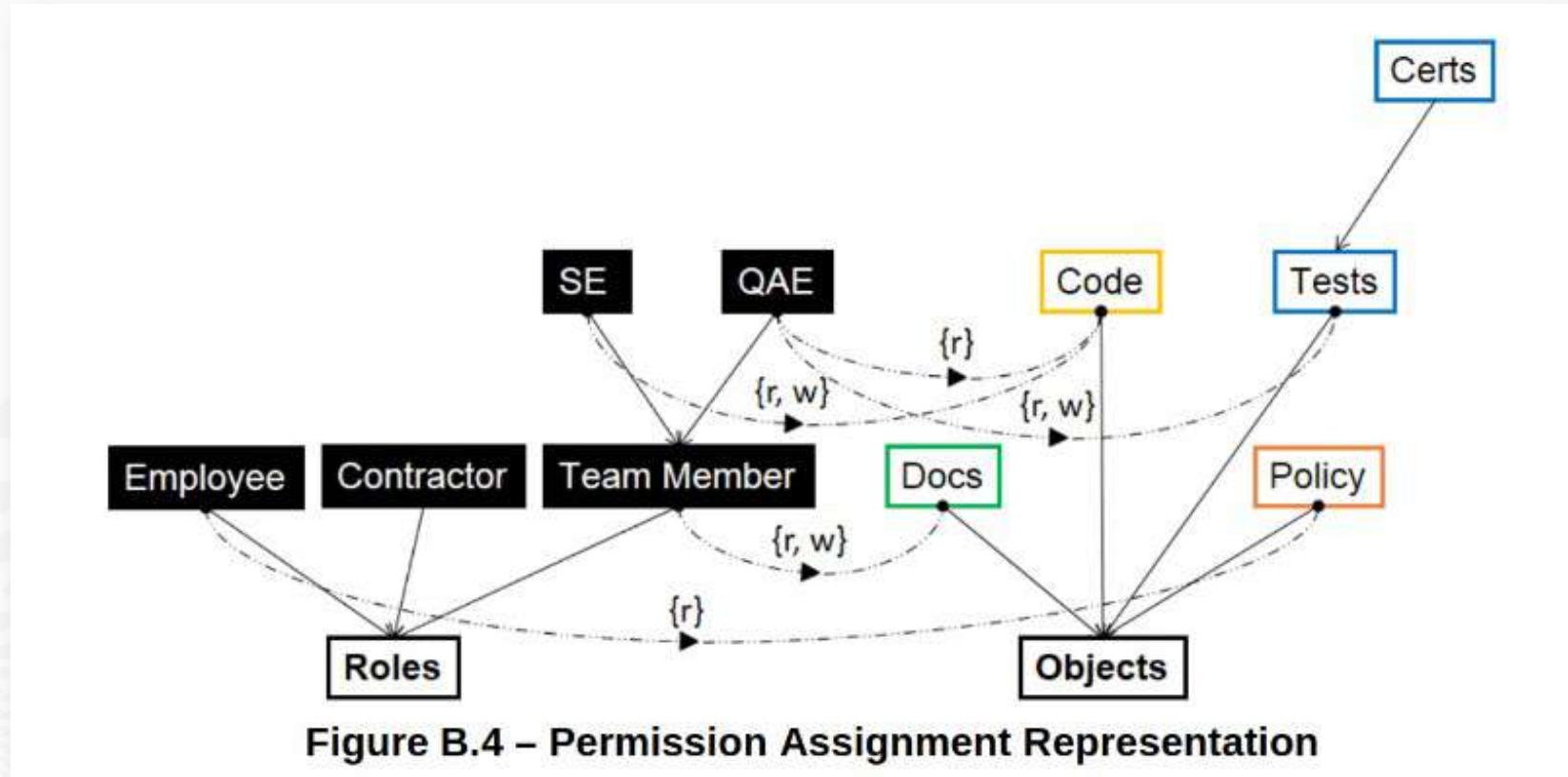


NGAC (2020)

- 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 exemple



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>)



WorTeKS

make IT work, make IT free

www.wortek.com

-  info@wortek.com
-  +33 1 84 20 86 47
-  [wortek_com](https://twitter.com/wortek_com)
-  [wortek](https://www.linkedin.com/company/wortek/)