オープンソースIDMの追加調査

SCIM（System for Cross-domain Identity Management）

- プロビジョニングやデプロビジョニング用のID情報をRESTfulなAPIでCRUD操作可能な標準プロトコル

- RFC7642(http://www.rfc-editor.org/rfc/rfc7642.txt)
  定義、概要、概念、および要件やユースケースについて

- RFC7643(http://www.rfc-editor.org/rfc/rfc7643.txt)
  コアスキーマについて

- RFC7644(http://www.rfc-editor.org/rfc/rfc7644.txt)
  プロトコルについて

SCIM実装/オープンソース

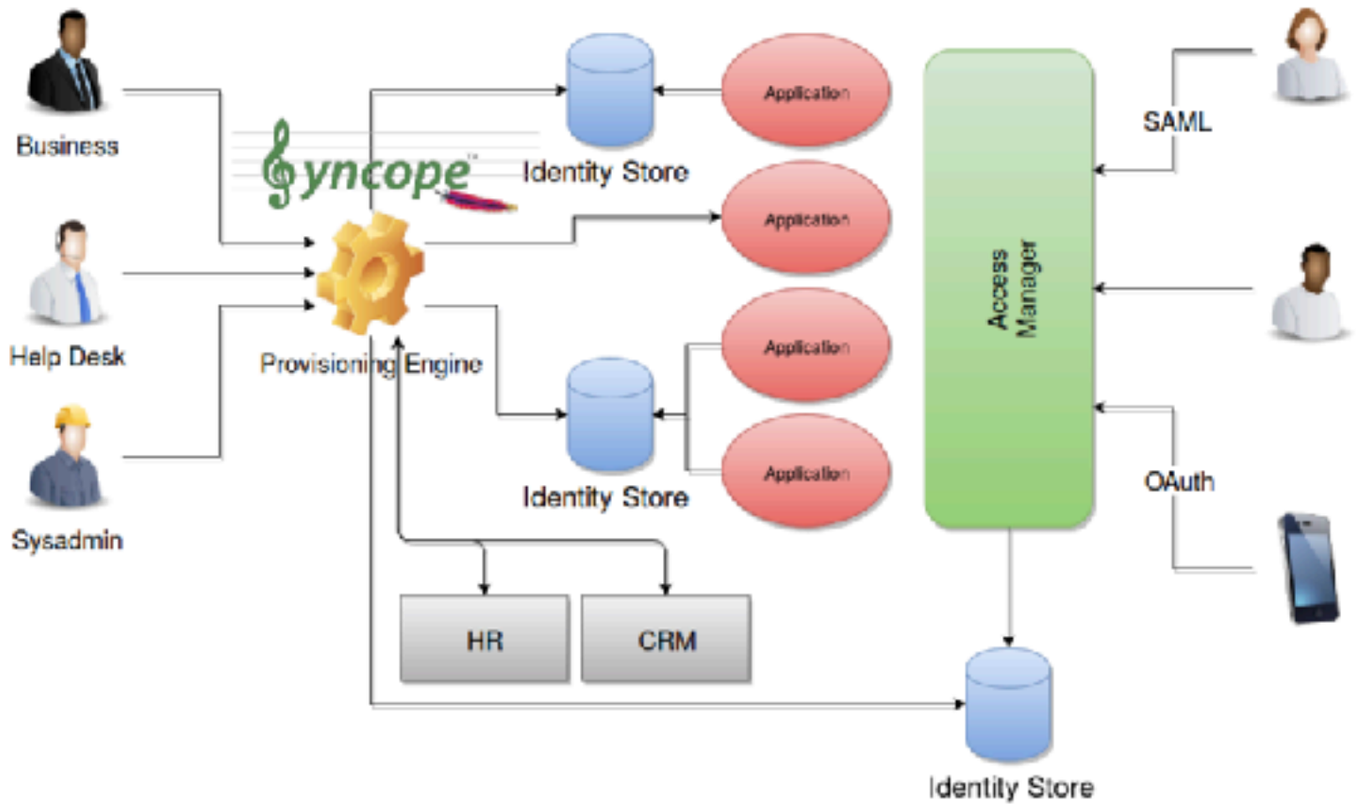
Project Name	Client	Server	Open Source	Developer
AuthX	Yes	No	Yes, MIT License	The Control Group
CzechIdM SCIM module	No	Yes	Yes, MIT License	BCV solutions
django_scim	No	Yes	Yes, MIT License	Atlassian
django-scim2	No	Yes	Yes, MIT License	Paul Logston @ 15Five
eSCIMo	Yes	Yes	Yes, ASL 2.0	Apache Software Foundation
Gluu	Yes	Yes	Yes, MIT License	Gluu.org
GoSCIM	No	Yes (openended building blocks + an example	Yes, MIT License	Weinan Qiu
hscim	No	Yes	Yes, AGPL License	Wire Swiss GmbH
OSIAM	Yes	Yes	Yes, MIT License	osiam.org team
Owin.Scim	No	Yes	Yes, MIT License	PowerDMS
SimpleIdentityServer	Yes	Yes	Yes	Habart Thierry
SOFFID IAM	Yes	Yes	Yes	www.soffid.com
Syncope	Yes	Yes	Yes, ASL 2.0	Apache Software Foundation
UnboundID SCIM 2 SDK for Java	Yes	Yes	Yes. GPL, LGPL, or UnboundID Free License.	Ping Identity (acquirer of UnboundID)
WSO2 Charon	Yes	Yes	Apache 2.0 License	WSO2 Inc

http://www.simplecloud.info

syncope.apache.org

Apache Syncope

Identity and Access Management - Reference Scenario

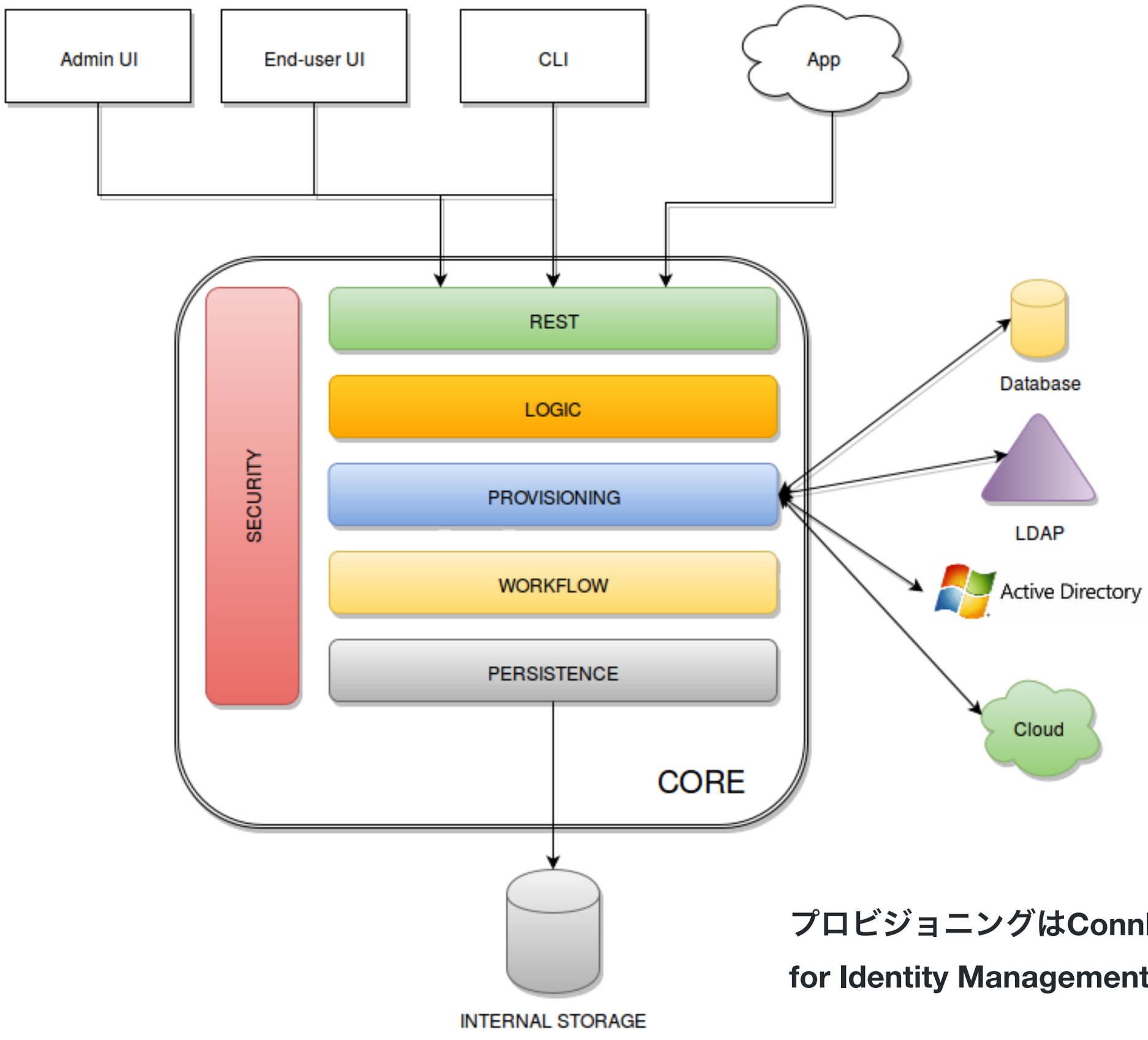


The picture above shows the tecnologies involved in a complete IAM solution:

- ***Identity Store***
  (as RDBMS, LDAP, Active Directory, meta- and virtual-directories), the repository for account data
- ***Provisioning Engine***
  synchronizes account data across identity stores and a broad range of data formats, models, meanings and purposes
- ***Access Manager***
  access mediator to all applications, focused on application front-end, taking care of authentication (Single Sign-On), authorization (OAuth, XACML) and federation (SAML, OpenID Connect).

As you can notice, **Apache Syncope is primarily a provisioning engine** .

Syncope Architecture



プロビジョニングはConnId (Connectors for Identity Management)に依存

ConnId

Java

Name	Source	Wiki	Issues	
Active Directory	https://github.com/Tirasa/ConnIdADBundle	wiki	issues	build passing
Azure	https://github.com/Tirasa/ConnIdAzureBundle	wiki	issues	build passing
CMD	https://github.com/Tirasa/ConnIdCMDBundle	wiki	issues	build passing
CSV Directory	https://github.com/Tirasa/ConnIdCSVDirBundle	wiki	issues	build passing
Database	https://github.com/Tirasa/ConnIdDBBundle	wiki	issues	build passing
Flat File	https://github.com/Tirasa/ConnIdFlatFileBundle	wiki	issues	build passing
FreeIPA	https://github.com/Tirasa/ConnIdFreeIPABundle	wiki	issues	build passing
Google Apps	https://github.com/Tirasa/ConnIdGoogleAppsBundle	wiki	issues	build passing
LDAP	https://github.com/Tirasa/ConnIdLDAPBundle	wiki	issues	build passing
OpenAM	https://github.com/Tirasa/ConnIdOpenAMBundle	wiki	issues	build passing
REST	https://github.com/Tirasa/ConnIdRESTBundle	wiki	issues	build passing
SCIM 1.1	https://github.com/Tirasa/ConnIdSCIMv11Bundle	wiki	issues	build passing
ServiceNow	https://github.com/Tirasa/ConnIdServiceNowBundle	wiki	issues	build passing
SOAP	https://github.com/Tirasa/ConnIdSOAPBundle	wiki	issues	build passing
UNIX	https://github.com/Tirasa/ConnIdUNIXBundle	wiki	issues	build passing
Zimbra	https://github.com/Tirasa/ConnIdZimbraBundle	wiki	issues	build passing

https://github.com/Tirasa/ConnId

開発項目の対応

開発項目	OpenIDM	Syncope
(1) ユーザアカウント統合管理システムのユーザ登録画面およびユーザ管理 DB の作成		
登録画面(ユーザ登録 Web UI)	☑	☑
ユーザ管理 DB	☑	☑
(2) データ登録系システム((ii)D-way)へのデータ登録スクリプトの作成		
OpenDJ ディレクトリサービスに登録するデータを生成するスクリプト	☑	☑
メール承認機能	☑	☑
OpenDJとの自動的な連動	☑	☑
(3)　スパコン LDAP へのデータ登録スクリプトの作成		
LDAP ディレクトリサービスに登録するデータを生成するスクリプトを作成	☑	☑
LDAP へのデータ登録スクリプトはスパコン SE が手動	☑	☑

Syncope Docker

https://syncope.apache.org/docs/2.1/getting-started.html#docker-compose-samples

git clone git@github.com:apache/syncope.git
https://github.com/apache/syncope/blob/syncope-2.1.3/docker/src/main/resources/docker-compose/docker-compose-postgresql.yml

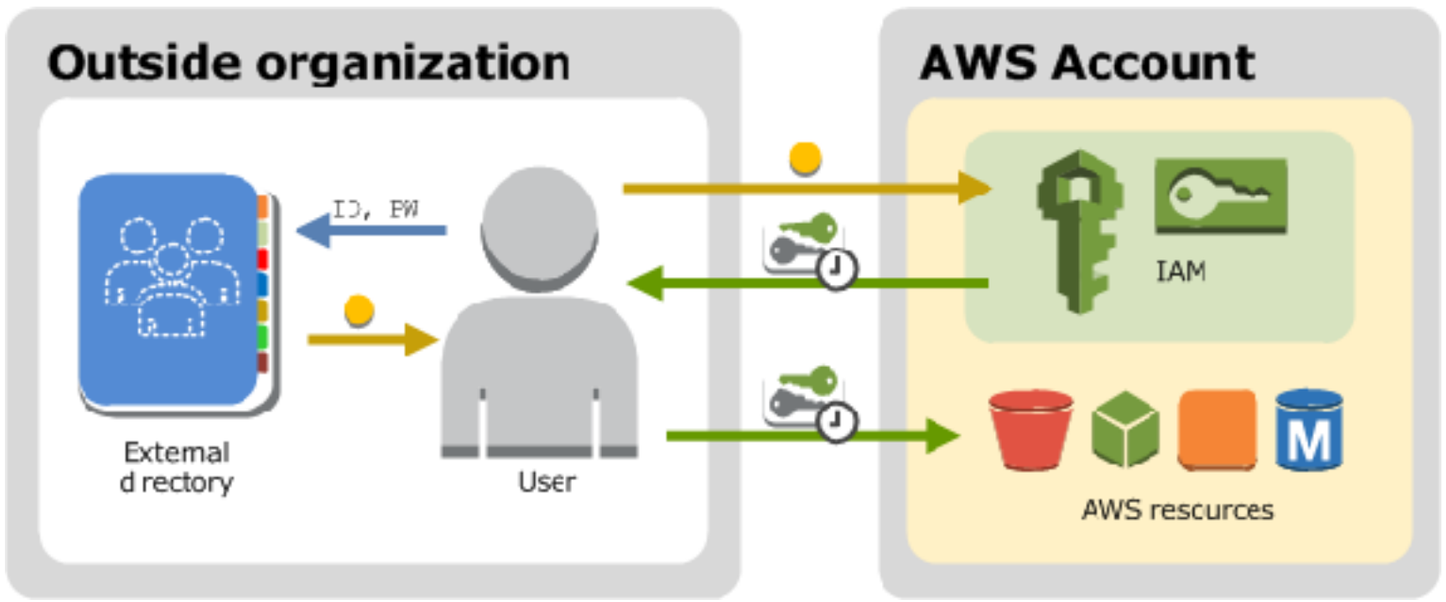
%docker-compose -f docker-compose-postgresql.yml up

Complete REST API reference	http://localhost:18080/syncope/index.html
Swagger UI	http://localhost:18080/syncope/swagger
Administration console	http://localhost:28080/syncope-console
End-user UI	http://localhost:38080/syncope-enduser

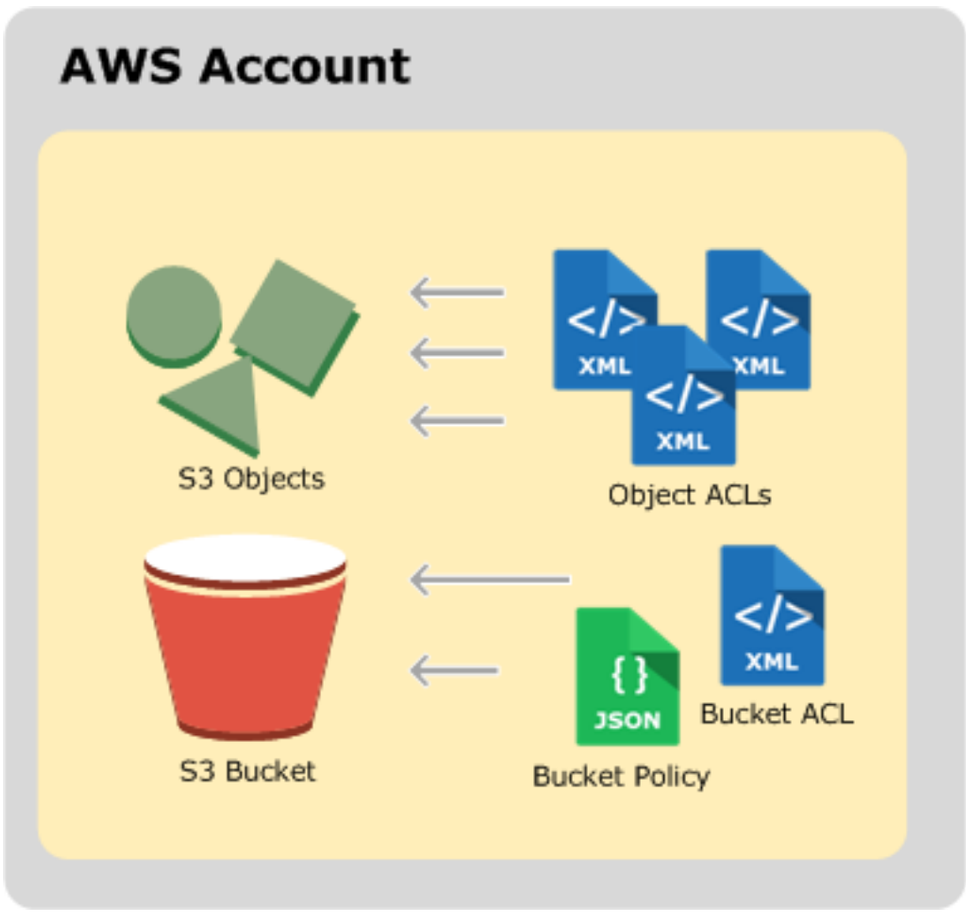
オープンソースIDM比較

Vaatimus	Apache Syncope	MidPoint	OpenIDM	Soffid	Keycloak	Unity	OpenIAM	Shibboleth	WSO2 Identity Server	Gluu	Jasig	FreeIPA	Aerobase	Grouper
Toimii Linux-palvelimella	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Avoimen lähdekoodin järjestelmä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä (community versio)	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Kaikille ilmainen	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Lisenssi	Apache 2.0 (FSF:n hyväksymä)	Apache 2.0 (FSF:n hyväksymä)	CDDL 1.0 (FSF:n hyväksymä)	GNU GPL v3 (FSF:n hyväksymä)	Apache 2.0 (FSF:n hyväksymä)	Oma lisenssi, ICM Uniwersytet Wasrszawski	Apache / GPL v3 (FSF:n hyväksymä)	Apache 2.0 (FSF:n hyväksymä)	Apache 2.0 (FSF:n hyväksymä)	Kaostuu monista [3]	LGPL (FSF:n hyväksymä)	GNU GPL v3 (FSF:n hyväksymä)	Apache 2.0 (FSF:n hyväksymä)	Apache 2.0 (FSF:n hyväksymä)
Ingestointimalleja rajapinnat	AD, Azure, Google Apps, Linux/Unix, Tietokannat, LDAP, CSV, XML jne. [4]	AD, Linux/Unix, Office365, Google Apps, SAP, Tietokannat, LDAP, CSV jne. [5]	AD, Google Apps, Salesforce, tietokannat, LDAP, XML, CSV, SSL jne. [6]	AD, Google Apps, Linux, Tietokannat, AWS, SAP, Oracle LDAP, ISO9N jne. [7]	AD, LDAP, SSO jne. [8]	LDAP, SAML, Oauth2 jne. [9]	Kts. LT2	Kts. LT2	AD, tietokannat (JDBC).	AD, LDAP	Kts. LT3	AD ja Linux	Kts. LT4	LDAP ja tietokannat.
Valmiit connectorit	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	Kyllä	Kts. LT4	Kyllä
Mahdollisuus tehdä omia connectoreita	Kyllä	Kyllä	Kyllä	Kyllä [4]	Kyllä	Ei	Kts. LT2	Kts. LT2	Kyllä	Ei saatu tietoon	Kts. LT3	Ei saatu tietoon	Kts. LT4	Ei saatu tietoon
Tapahtumien kirjaus lokeihin	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	Kyllä	Kts. LT4	Kyllä
Eri salasanatodennustasoisiin järjestelmiin, tukee järjestelmien omia käytäntöjä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	Kyllä	Kts. LT4	Ei tietoa
Kehitetaan aktiivisesti	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	Kyllä	Kts. LT4	Kyllä
Governance	Ei tietoa	Kyllä	Ei tietoa	Kyllä	Ei tietoa	Ei tietoa	Kts. LT2	Kts. LT2	Ei tietoa	Ei	Kts. LT3	Ei tietoa	Kts. LT4	Ei tietoa
Toimeksiantojen hyväksyntä	Kyllä	Kyllä	Kyllä	Ei tietoa	Kyllä	Ei tietoa	Kts. LT2	Kts. LT2	Kyllä	Ei tietoa	Kts. LT3	Ei tietoa	Kts. LT4	Ei tietoa
Salasanojen hallinta	Kyllä	Kyllä	Kyllä	Kyllä	Osittain	Ei tietoa	Kts. LT2	Kts. LT2	Kyllä	Osittain	Kts. LT3	Kyllä	Kts. LT4	Ei tietoa
Vuorollaan työyhdisteimien tunnuksen lehtävälasoisesti	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	ei tietoa	Kts. LT4	Ei tietoa
Tunnusten jaadytys ja poisto	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä		Kts. LT2	Kts. LT2	Kyllä		Kts. LT3		Kts. LT4	
Henkilö- ja käyttäjätunnusprofiilien muokkausmahdollisuus	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	Kyllä	Kts. LT4	Ei tietoa
Hakumahdollisuus	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kts. LT2	Kts. LT2	Kyllä	Kyllä	Kts. LT3	Kyllä	Kts. LT4	Kyllä
Reporttien luonti	Kyllä	Kyllä	Kyllä	Kyllä	Ei		Kts. LT2	Kts. LT2	Ei		Kts. LT3		Kts. LT4	
Manuaaliprovisiointi	Kyllä	Kyllä	Ei tietoa	Ei tietoa	Ei tietoa		Kts. LT2	Kts. LT2	Ei tietoa		Kts. LT3		Kts. LT4	
Soveltuu suurille yrityksille	Kyllä	Kyllä	Kyllä	Kyllä	Oletettavasti kyllä****		Kts. LT2	Kts. LT2	Kyllä		Kts. LT3		Kts. LT4	
GitHub-starrit (kpl)	1401 *	998	44	0	4597	17	Kts. LT2	Kts. LT2	625	0	Kts. LT3	409	Kts. LT4	0
Referenssejä (kpl)	33 (1 suomalainen)	29 (1 suomalainen)	2	2	0	0	Kts. LT2	Kts. LT2	8	0	Kts. LT3	0	Kts. LT4	2
Google Trends 2v keskiarvo (kpl)	42	34	44	25	52	30	Kts. LT2	Kts. LT2	42	40	Kts. LT3	42 **	Kts. LT4	0
Google Trends 5v keskiarvo (kpl)	26	46	47	16	37	30	Kts. LT2	Kts. LT2	38	22	Kts. LT3	41 **	Kts. LT4	0
Google Scholarissa julkaistujen patenttien ja														

AWS Identity and Access Management (IAM)



S3 リソースベースのポリシー



- Security Assertion Markup Language 2.0 (SAML 2.0) 互換性

- OpenID Connect (OIDC) 互換 ID プロバイダー