esup portail

02.Feb.2021

ONLINE

#esupdays31

#apereoparis21

apereo

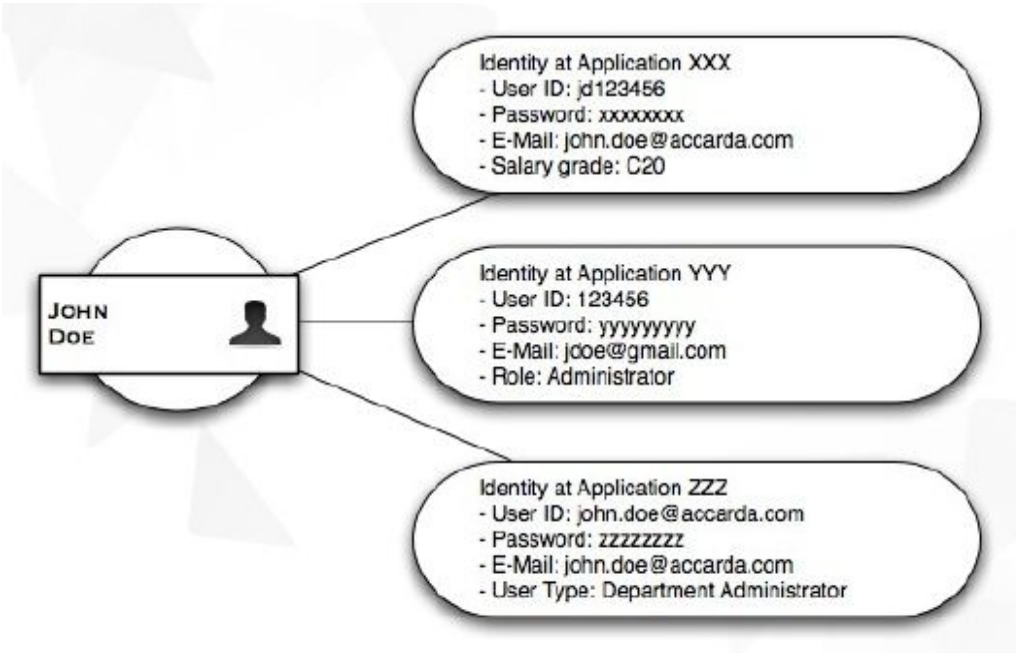
BUILDING OPEN SOURCE IDENTITY INFRASTRUCTURES

Francesco Chicchiriccò -- CEO at Tirasa
-- V.P., Apache Syncope at The Apache Software Foundation

SECTION #1: Vocabulary & Background

What is an "identity" about?

- Data records that contains a collection of data about a person:
  - "Data record" → Account
  - "Person" → Identity
- Account
  - Computers work with records of data about people
  - Such records contain technical information needed by the system for which the account is created and managed
- (Digital) Identity
  - Set of information related to a an entity in a specific domain (e.g. an employee in a organization)... it's You!

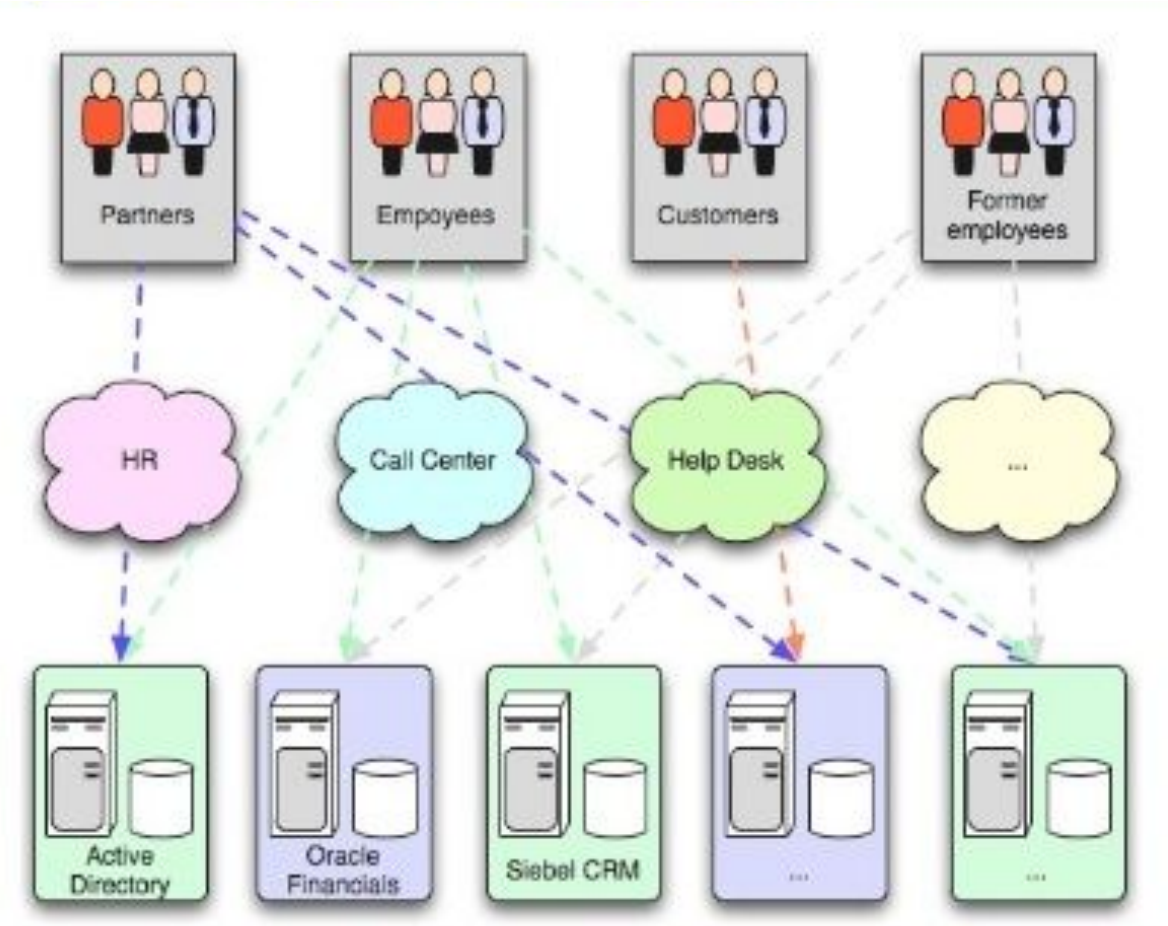


How do we deal with Identity issues?

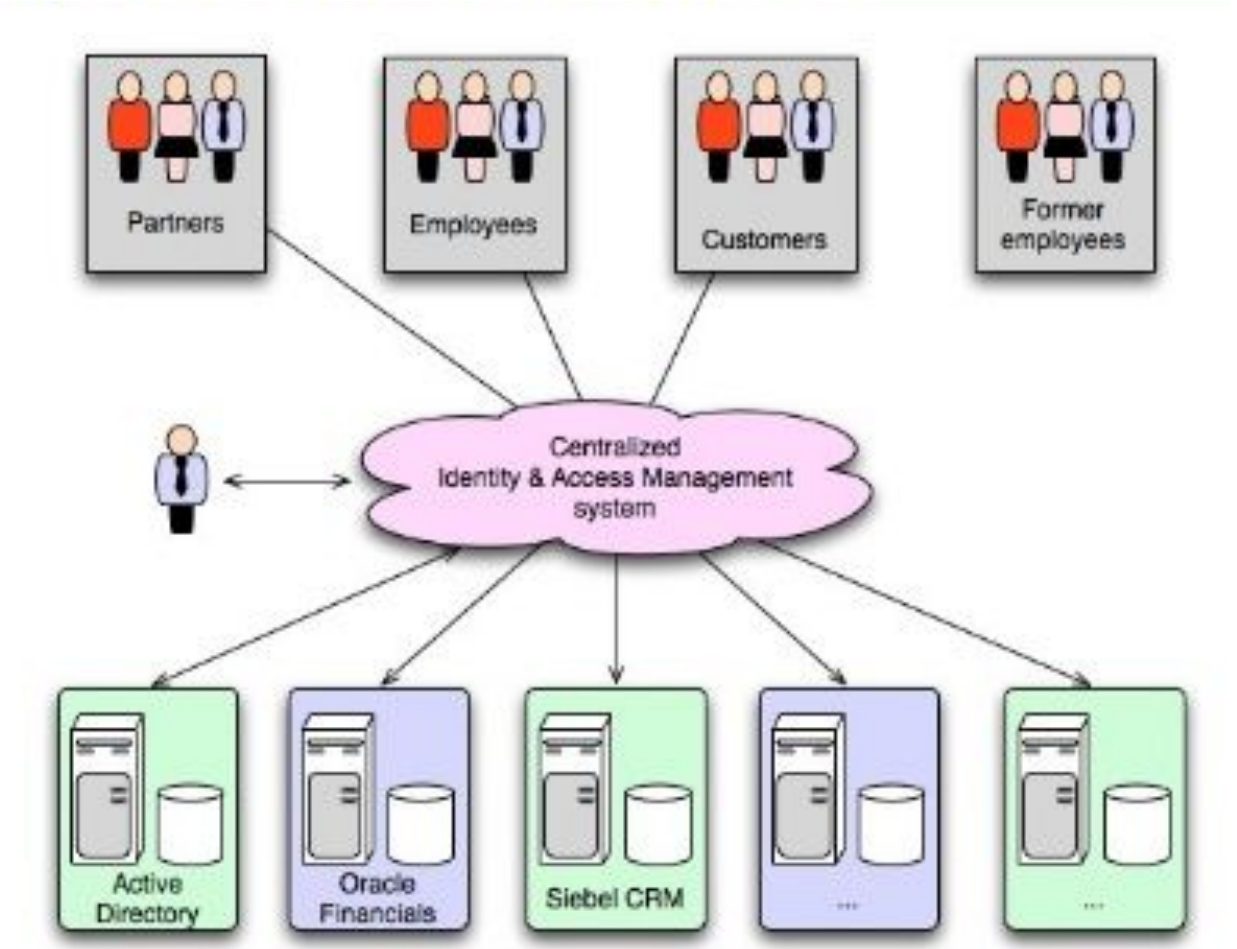
- Identity Management
  - Tools and practices to keep identity data consistent and synchronized across repositories, data formats and models
- Access Management
  - Systems, protocols and technologies supporting user authentication (how Users are let accessing a given system) and authorization (which capabilities each user owns on a given system).

Identity Management and Access Management are complementary: very often, the data synchronized by the former are then used by the latter to provide its features - e.g. authentication and authorization.

The Problem


Partners
Empoyees
Customers
Former employees
HR
Call Center
Help Desk
...
Active Directory
Oracle Financials
Siebel CRM
...
...

The Solution



Identity Stores

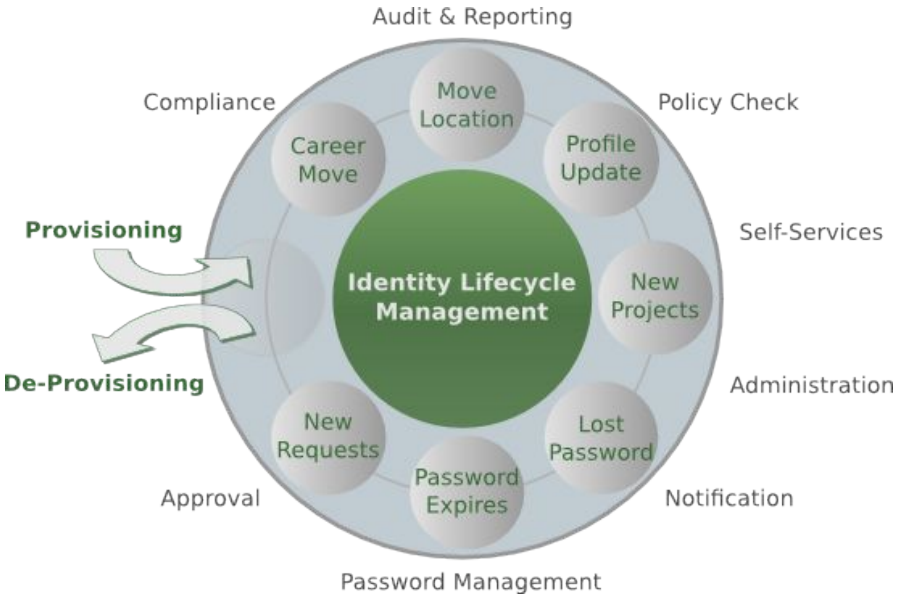
- The physical places where identity information is stored
- Examples:
  - LDAP / AD
  - Databases
  - Meta and Virtual Directories
  - Cloud
- Accounts can be created and managed
  - Each application manages authentication separately
  - Users may use the same password for all connected applications

Aren't Identity Stores enough?

- Heterogeneity of systems
- Lack of a single source of information
  (HR for corporate id, Groupware for mail address, ...)
- Often applications require a local user database
- Inconsistent policies across the infrastructure
- Lack of workflow management
- Hidden infrastructure management cost, growing with the size of the organization

Provisioning Engines

- Managing the Identity Lifecycle
- Keeping identity stores as much synchronized as possible
- Need to be customizable and flexible
- Focused on application back-end
- Communication:
  - Connector
  - Agents



Access Managers

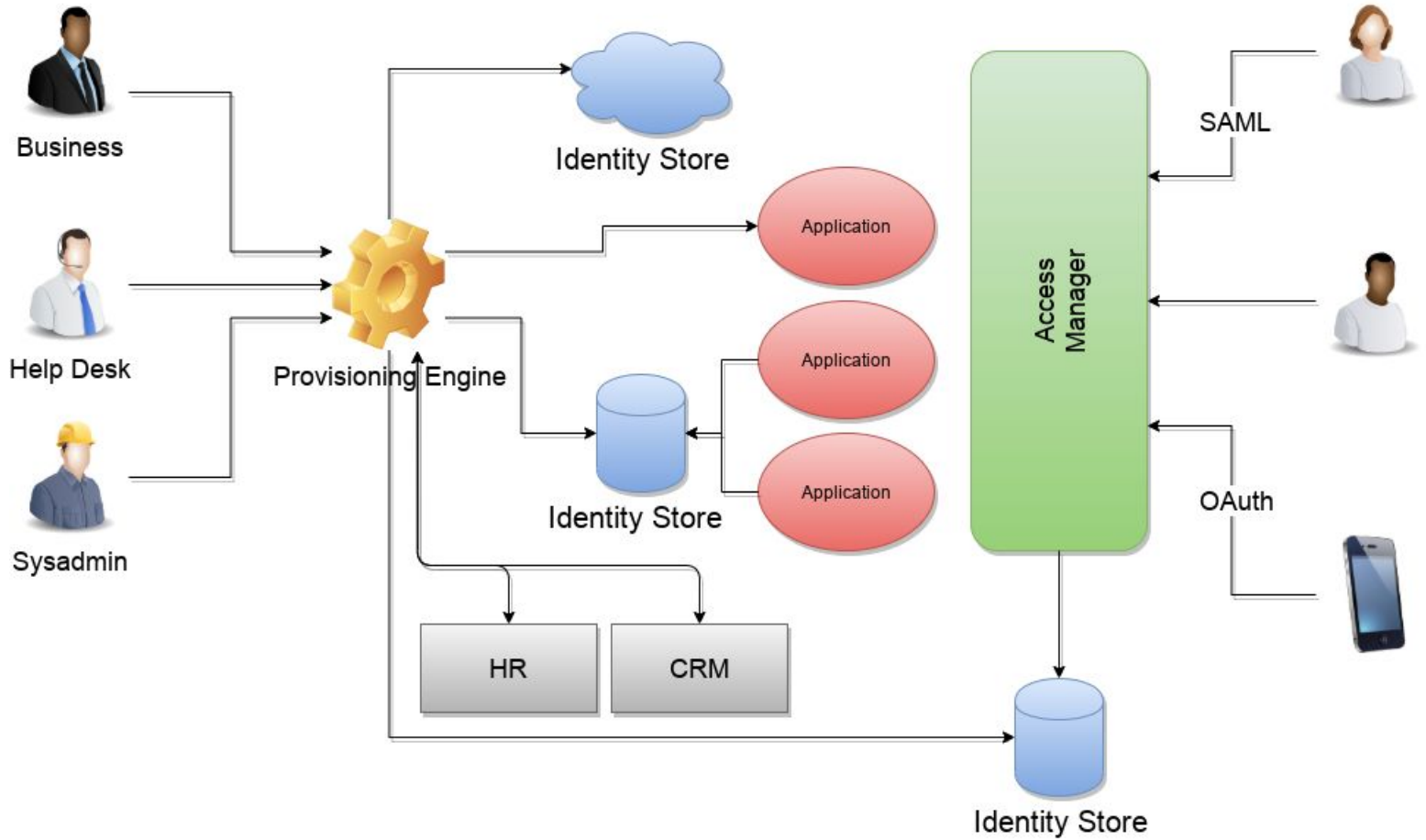
- Enforcing application access via authentication and authorization

- Single Sign-On
- MultiFactor Authentication

- OAuth
- SAML
- OpenID Connect
- XACML

- Focused on application front-end

The Complete Picture



SECTION #2: Selling Open Source IAM

NOBODY
EVER GOT FIRED
FOR CHOOSING IBM

Someone, Somewhere

Common challenges

- Adoption
  - Who's using it?
- Features
  - How can I do X?
- Security
  - Is OSS secure?
- Stability & Support
  - Who are you?

02.Feb.2021
ONLINE
#esupdays31
#apereoparis21

- Unbeatable flexibility
- No vendor lock-in
- Transparent security
- Involvement
  - Customers can be actually part of solution
  - Tools can last beyond contractor's lifespan

What can Open Source IAM offer, not to mention the price?

apereo

esup portail

The Open Source Identity Stack

- Apache Syncope
  - Identity Provisioning and Governance
  - https://syncope.apache.org
- Apereo CAS
  - Authentication and Authorization
  - https://apereo.github.io/cas/

SECTION #3: Designing (Open Source) IAM

Gather the identity and access flows...

- Number and type of identities
- Number of roles / groups (and what are they used for)

- External resources (all covered by standard connectors?)

- Approval workflows?
- User Requests?

- Self-service?

- Which applications to protect?
- Which authentication mechanisms?
- Which authorization types?

...design...

- Schema for various identities (users, roles, groups, ...)
- Identify mapping for all resources
  - Not too complex!
- Watch role number to avoid RBAC's role explosion
- Prioritize requirements
- Don't be tempted to redesign the whole thing
  - Provisioning needs to be flexible
  - Reduce impact of access management on existing applications

...build...

- Carefully choose the building blocks
  - Can't simply buy COTS
  - Often have to deal with pre-existing, partial and overlapping tools
- Where?
  - On-premises
  - As-a-service
- Scale/Load/Volume
- Consider prototyping the designed solution (PoC)

....and start again

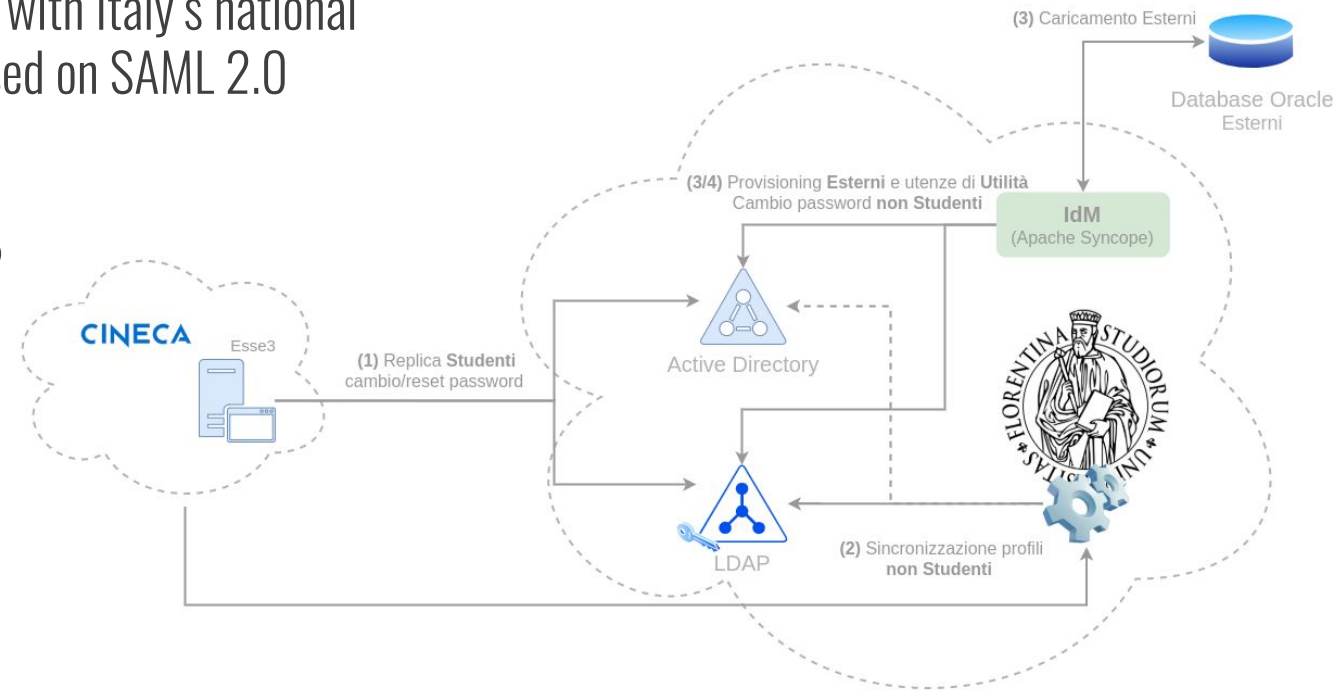
- IAM is a continuous process, not a product
  - New applications to protect
  - New resources to integrate
  - Identity flows evolution

- IAM deliveries frequently fail
  - Mix of complex and unrelated technologies
  - Unexpected interactions
  - Mess with internal processes
  - Discover Policy Vs Reality

SECTION #4: Delivering Open Source IAM

Case: University of Florence, Italy

- ~150k users including (ex) students, teachers, staff
- Applications with SSO integrated with Italy's national authentication system (SPID) based on SAML 2.0
- Provisioning different classes of users from DB to AD and LDAP
- Self-service profile management and password reset with user requests support



Case: Cruise Line headquartered in North America

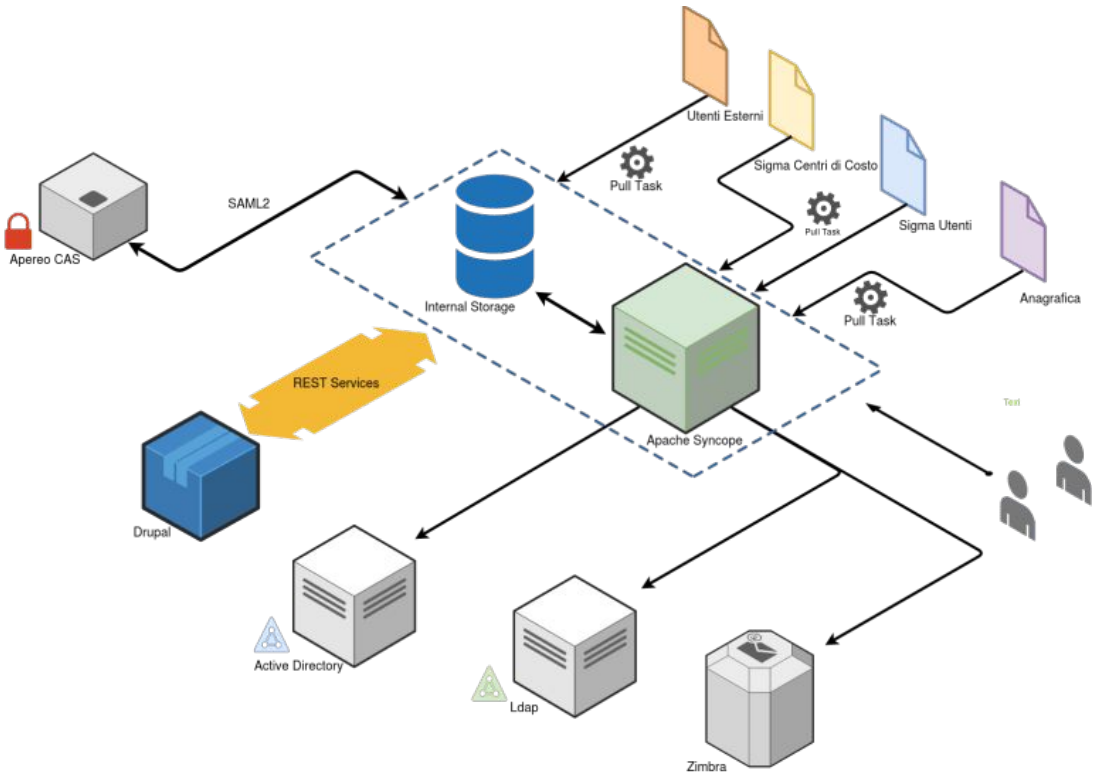
- Event-based (Apache Kafka) user create and update
- Provisioning to Azure AD, GSuite and Workday (ad-hoc connector)
- Identity flow orchestration across shore and ships
- Application SSO via OpenID Connect and SAML 2.0, with Google Auth support for MFA
- Continuous Deployment pipeline to Kubernetes

Case: Large foodservice distributor based in North America

- ~400k users across US and Canada
- Entitlement management
- Provisioning to and SSO with Okta
- Mobile-ready self-service profile management
- Extreme customization: look & feel, data model, authorization
- Continuous Deployment pipeline to Google Cloud Platform

Case: AULSS 6 Euganea of Padua (healthcare)

- Group-based provisioning to AD, GSuite, CSV, LDAP, DB
- User workflow customizations
  - approval
  - account expiration
  - password reset with SMS notification
- Custom reports
- Application SSO via SAML 2.0
- Front-end integration from Drupal via Syncope REST layer



T/RASA.
{open source excellence}

SECURE DIGITAL
IDENTITY MANAGEMENT
AND LOGICAL AND PHYSICAL
ACCESS CONTROL_

THANK YOU

-- More at https://www.tirasa.net

apereo

esup portail