

WORK
SHOP
GARR
2022

**NET
MAKERS**

IdP in the Cloud 3.0

Davide Vagheti

GARR

IdP in the Cloud

Caratteristiche

- *Identity Provider federato*
- *Directory dedicata (opzionale)*
- *Identity Management System (opzionale)*

Enti a cui e' dedicato

- *Poche risorse*
- *Poco personale IT*
- *Comunità di piccole dimensioni e/o partizionate*

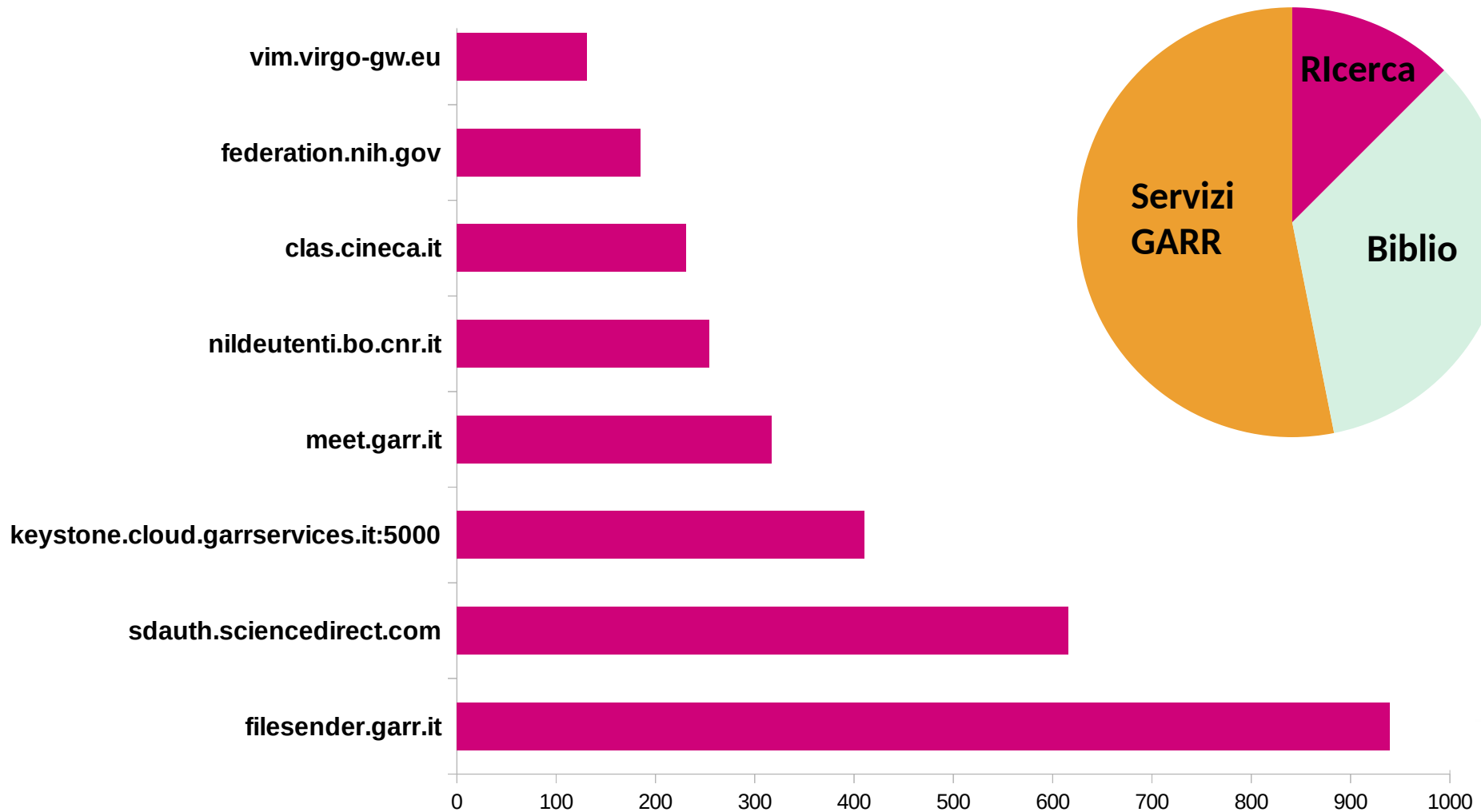
IDP IN THE CLOUD

41 IdP

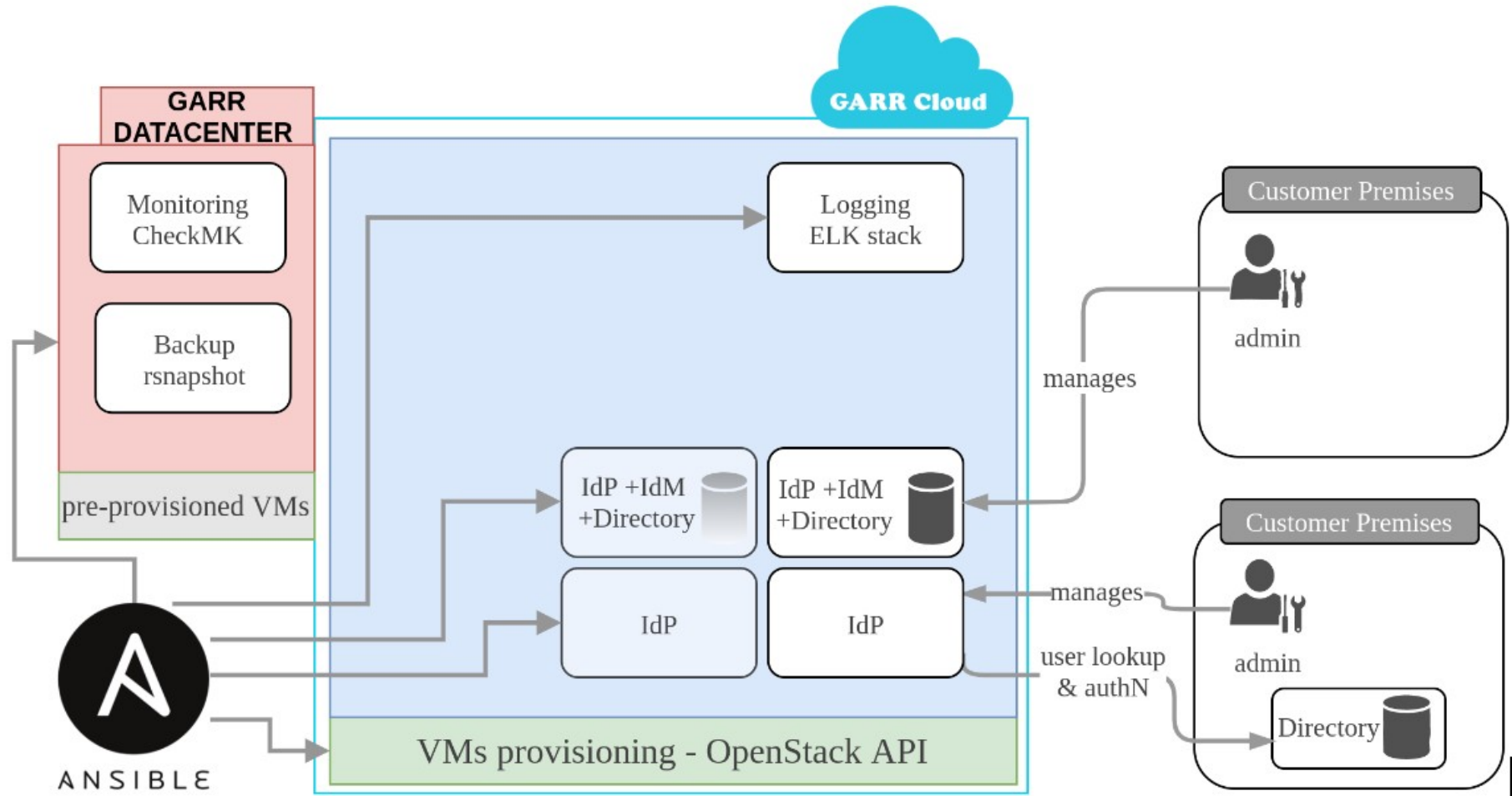
3500+ Utenti

8000 AuthN/Anno

Accesso alle risorse



Architettura IdP in the Cloud 2.0



IDP IN THE CLOUD

**Risorse
impiegate**

82 VM

328 GB RAM

164 Virtual CPU

~2 TB Storage

82 Indirizzi IP

Efficacia

IdP in the Cloud 2.0 - 2018

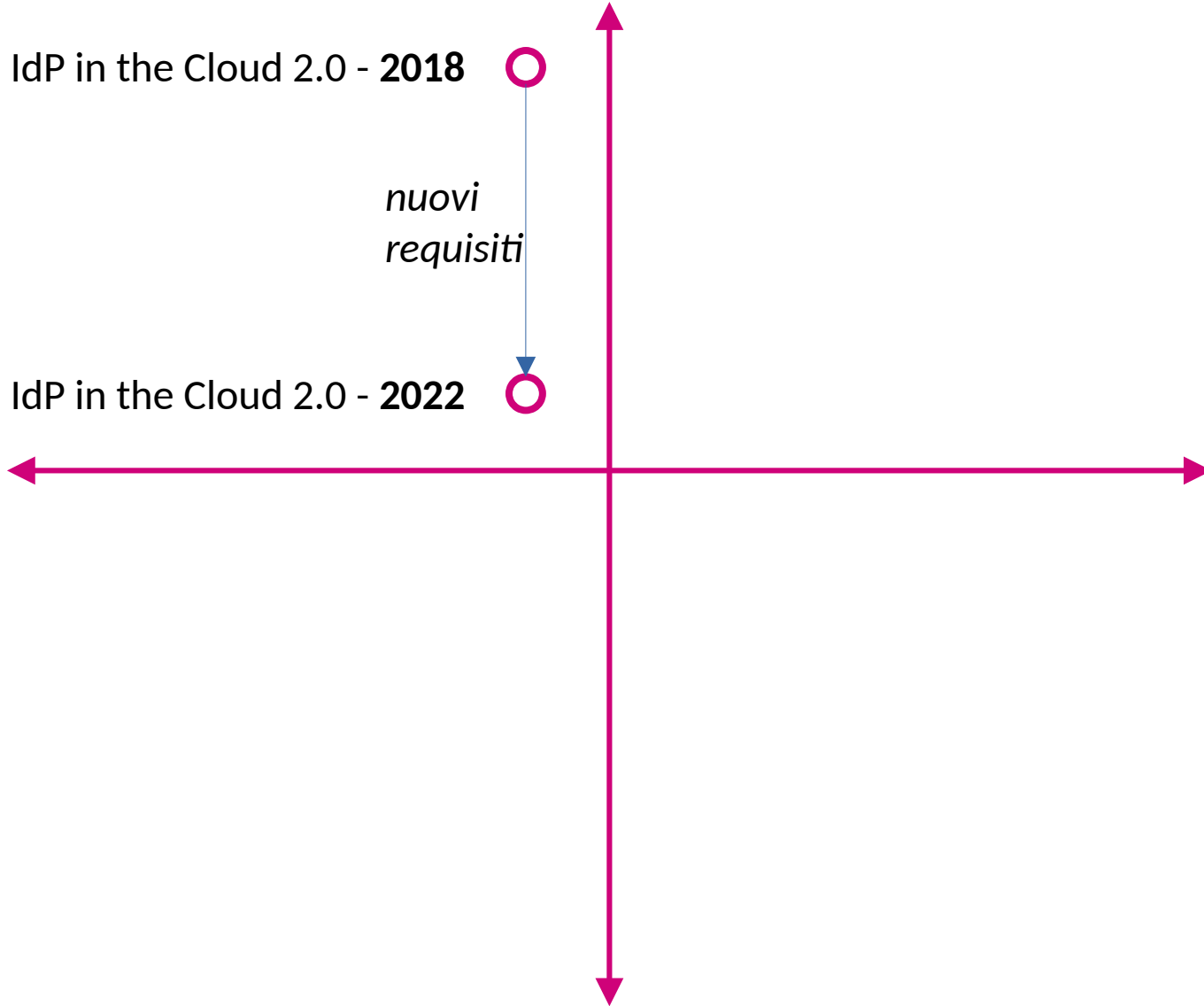


*nuovi
requisiti*

IdP in the Cloud 2.0 - 2022



Efficienza



IDP IN THE CLOUD

v 3.0

RIPROGETTATA DA 0

MULTITENANT

IDM DEDICATO

MULTI FACTOR AUTHENTICATION

VERIFICA ACCREDITAMENTO VIA API

CONTAINER - AUTOMAZIONE - ALTA AFFIDABILITA'

SVILUPPO

IdP in the Cloud 3.0: kanban

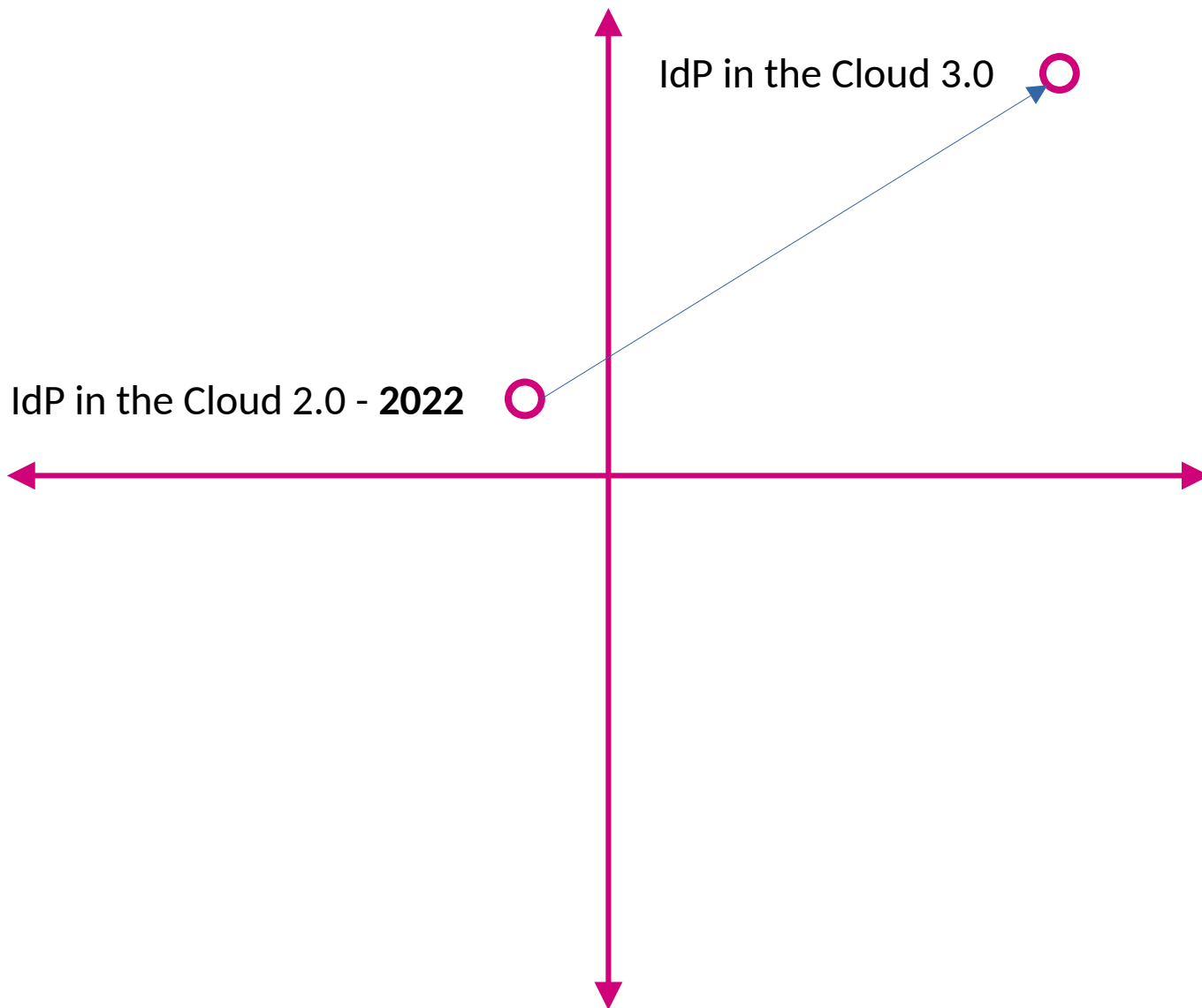
IDEM > idpcloud > Issue Boards

Development Search Edit board Create list

- Backlog** (13 items)
 - (R1) Analizzare e documentare le dipendenze lato directory di privacyidea. IDEM/idpcloud/idpcloud-userdb#1
 - (R2.7) Gli amministratori possono inviare notifiche e messaggi custom agli utenti di ogni istituto tramite l'interfaccia di gestione. IDEM/idpcloud/idpcloud-idm#17
 - (R1) Documentare installazione e configurazione del modulo di integrazione tra privacyIDEA e SSP. IDEM/idpcloud/idpcloud-idp#1
 - (R1) Installare e configurare il modulo MFA privacyidea-SSP. IDEM/idpcloud/idpcloud-idp#2
 - (R1) Implementare le dipendenze di privacyidea nella directory. IDEM/idpcloud/idpcloud-userdb#2
 - (R3.3) Supporto e valorizzazione attributo "eduPersonEntitlement" per istituto e per utente per l'accesso alle risorse federate. IDEM/idpcloud/idpcloud-idm#2
 - (R3.4) Supporto pairwise-id e subject-id. IDEM/idpcloud/idpcloud-idp#12
- ToDo** (7 items)
 - (R6) L'accesso all'interfaccia web dell'IdM avviene tramite autenticazione federata dell'IdP di afferenza. IDEM/idpcloud/idpcloud-idm#5 Aug 31
 - (R6) L'IdM e' un SP locale per tutti gli IdP abilitati. IDEM/idpcloud/idpcloud-idp#15 Aug 26
 - (R6) Creazione e configurazione di un Service Provider per l'IdM. IDEM/idpcloud/idpcloud-idm#6 Aug 12
 - (R2.4) Creazione documento con specifiche per la verifica degli utenti su WFR. IDEM/idpcloud/idpcloud-idm#14 Aug 19
 - (R2.3) Implementare creazione utenti tramite CSV nell'interfaccia IDM lato amministratori. IDEM/idpcloud/idpcloud-idm#10 Aug 19
 - (R9) Definire tutte le stringhe dell'IdM in modo che possano essere tradotte dal modulo multi-lingua. IDEM/idpcloud/idpcloud-idm#7 Aug 19
 - (R3.7) Personalizzazione messaggi di errore dell'Identity Provider basati sullo stato dell'utente IDEM/idpcloud/idpcloud-idp#22 Aug 26
- Doing** (5 items)
 - (R2) Definizione degli attributi che stabiliscono i ruoli di ogni utente. IDEM/idpcloud/idpcloud-userdb#5
 - (R2.4) Per ogni utente inserito verificare la presenza sul Workflow della ricerca (WFR) di CBIM tramite il webservice relativo. IDEM/idpcloud/idpcloud-idm#13 Aug 19
 - (R2.6) Implementare un processo di invio notifiche (ad es. notifica di disabilitazione utente all'approssimarsi della scadenza). IDEM/idpcloud/idpcloud-idm#16 Aug 26
 - (R2.1) Scadenza utente: a data definita dall'amministratore + ogni anno a Gennaio. L'IDM deve poter attivare processi di gestione utente basati sulle scadenze. IDEM/idpcloud/idpcloud-idm#11 Aug 26
 - Implementare unit test e test funzionali per l'IDM IDEM/idpcloud/idpcloud-idm#20 Aug 12
- Done** (8 items)
 - (R2.8) Implementare verifica batch di tutti gli utenti (o tutti gli utenti di un istituto) su WFR. IDEM/idpcloud/idpcloud-idm#18
 - Implementare test funzionali per il funzionamento dell'IdP IDEM/idpcloud/idpcloud-idp#23 Aug 11
 - (R2.8) Implementare verifica utilizzo account (deve poter rispondere alla domanda: "questo utente si e' autenticato almeno una volta negli ultimi 6 mesi?") IDEM/idpcloud/idpcloud-userdb#11 Aug 12
 - (R2) Creazione gruppo amministratori sulla directory. IDEM/idpcloud/idpcloud-userdb#10 Aug 19
 - (R6) Creare un amministratore dell'IdP per ogni IdP configurato. IDEM/idpcloud/idpcloud-idm#4 Aug 26
 - (R2.5) Attivazione degli utenti tramite invio di una mail con link di attivazione. L'invio avviene in seguito all'inserimento e alla verifica. IDEM/idpcloud/idpcloud-idm#15 Aug 19
 - (R2.2) Implementare interfaccia di inserimento e gestione utenti tramite FORM (IDM lato admin). IDEM/idpcloud/idpcloud-idm#12 Aug 19

Efficacia

Efficienza



GRAZIE

