Document objective : Ensure all managers involved in the project are aware of the project, and they are involved proactively on the project.

Project title

Remove technical debt from the Authentication and Authorization infrastructure

Project manager

Sarah Butcher and Marc Riera

Project Sponsor

Internal TSC funding

Stakeholders

- SDO members: System owners
- TSC members: Direct system users
- EBI members: System users
- EMBL members: Federation of AAI

Project approval requirements

What items need to be approved?

- PoC
- Support structure with Evolveum (£)
- L1/L2/L3 approach
- Communication strategy

Who will have sign-off authority?

- Andy Cafferkey as Head of TSC

Who will define the criteria for considering a project successful?

- Sarah Butcher
- Marc Riera
- Tomasz Nowak

Project Scope Statement

Some context can be found in the following RT ticket and its children.
A map of the existing AAI relationships can be found here(map)

Project purpose

There are several reasons for this project, some of them would be valid by themselves.

- AAI technical debt is currently blocking the federation EBI with oneEMBL
- SCORE (internally developed AAI) system has reached EOL on several of its layers
    - Base code is python2 which has EOL since 2019.
    - UI system used by score was last updated on 2011
    - Some unfinished transitions divided the system into several databases which have drifted away from their original purpose
- Unify ITSM service catalogue related to Account Management
    - We need a single account management system, which unifies cloud, windows and unix accounts.

Objectives

(Specific, Measurable, Achievable and Agreed, Relevant, Time-bound)

- Shut down systems (voyager, score , scoreAPI)
- Deliver a secure and auditable AAI for the EMBL-EBI
- New AAI should be API driven
- Provide EBI users with a self service account management system for transfer accounts and virtual accounts.
- Transfer services will provide the new AAI as the way for users to request and manage ftponly accounts
- EBI will provide the new AAI as the way for GTL's to manage virtual accounts
- EBI will provide the new AAI as the way for GTL's to manage sponsored member and collaborator accounts

- Less RT tickets related to account management
- Webin accounts to be ported to the new AAI

Scope

- Pushing EBI information into EMBL-LDAP, EBI-LDAP and ActiveDirectory
- All tasks currently being executed in voyager
    - Foreman netgroup management
    - Eduroam affiliation management
    - Account lifecycle management
- Synchronisation of accounts between EMBL, EBI , AD and GCP
- Report creation
- Schedule account closure
- Password change enforcement
- Pilot of a RBAC or ABAC access control, for example HPC access if property X is set by the manager.

Out-of-scope

- Upgrade of AD
- In the future we may want to manage the GCP and AWS identities directly from the new AAI, skipping the AD , but this is not in the scope of the existing project.
- ContentDB
- ServiceNow
- SAP
- Standard Operating Procedures
- Webin managers will be given instructions on how to transition to the new system, but they will have to do the transition themselves.

Milestones

1. Parallel PoC with midpoint evolveum and openIAM
2. Installation of a dev/test system including EMBL-LDAP
3. Installation of new production AAI
4. Groups of existing accounts synched by new AAI
5. Stop score pull operator
6. Stop score push operator
7. Stop scoreAPI cluster
8. Stop voyager
9. Retire mysql and oracle(syspro) database
10. Webin accounts ported to new AAI

High-level risks

(obstacles that might affect your project)

- Influx of L1 tickets requiring time of the SDO engineers involved in the project may block progress. Without progress the tickets will continue and the project will become stale.

Assumptions

(hypotheses you assume to be true)

- All SDO engineers involved in the project will stay with the project until completion.
- TSC management is on board with the changes, and all TSC teams will follow through without creating parallel/alternative systems or workflows.

Constraints

(obstacles that might limit the project's outcomes)

- SDO engineers will need work on many storage changes while doing this project as well

Dependencies

(conditions that a project relies on)

- Evolveum support or OpenIAM support
- TSC support

Communication Strategy

(how & when the team & stakeholders will communicate)

- TBD

Annex