CNAF Reloaded:
AAI

Andrea Ceccanti

CNAF Reloaded Meeting
8 Aprile 2021

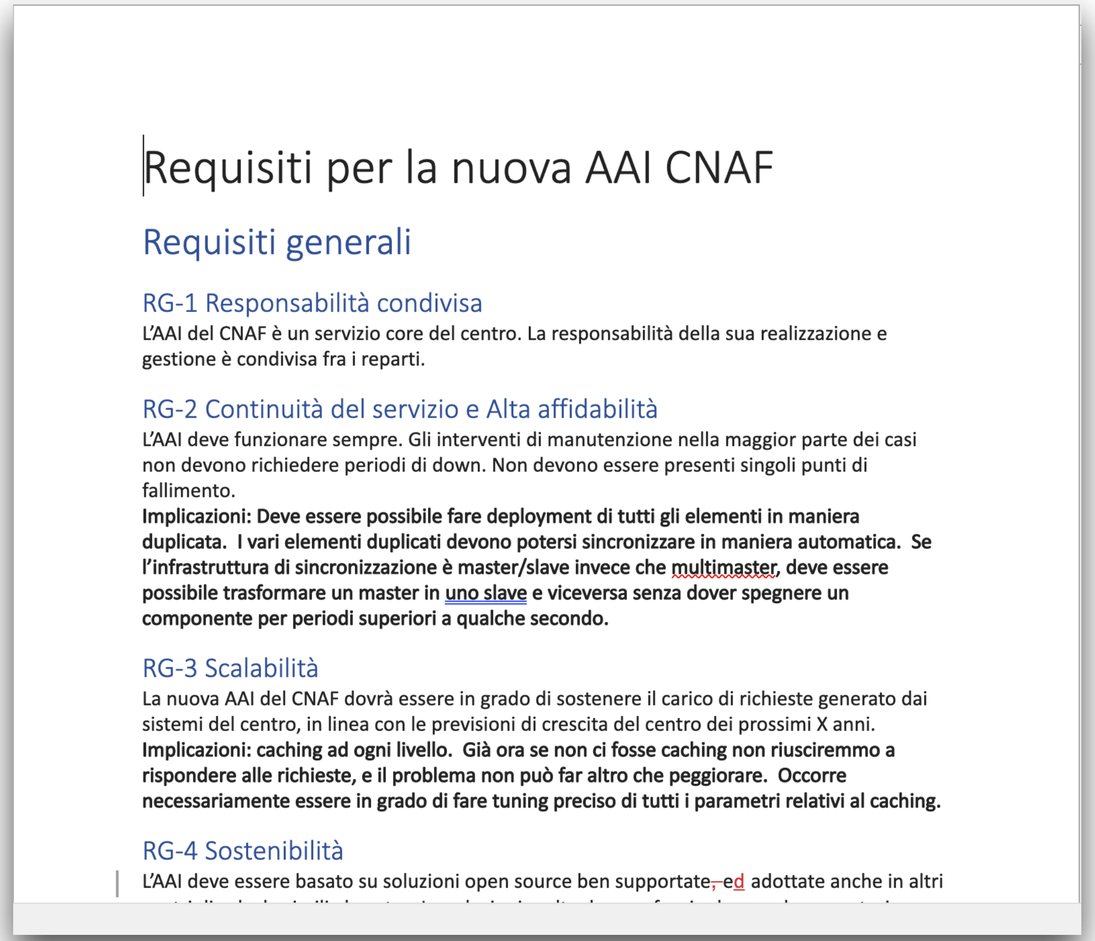
Requisiti per la nuova AAI del CNAF

Documento "vivo"

Frutto delle discussioni nei mesi passati

Requisiti di alto livello e funzionali, e.g.:

- Responsabilità condivisa
- Sostenibilità
- Usabilità
- …
- Supporto di Autenticazione a fattori multipli
- Gestione ciclo di vita degli account



Requisiti per la nuova AAI CNAF

Requisiti generali

RG-1 Responsabilità condivisa

L'AAI del CNAF è un servizio core del centro. La responsabilità della sua realizzazione e gestione è condivisa fra i reparti.

RG-2 Continuità del servizio e Alta affidabilità

L'AAI deve funzionare sempre. Gli interventi di manutenzione nella maggior parte dei casi non devono richiedere periodi di down. Non devono essere presenti singoli punti di fallimento.

Implicazioni: Deve essere possibile fare deployment di tutti gli elementi in maniera duplicata. I vari elementi duplicati devono potersi sincronizzare in maniera automatica. Se l'infrastruttura di sincronizzazione è master/slave invece che multimaster, deve essere possibile trasformare un master in uno slave e viceversa senza dover spegnere un componente per periodi superiori a qualche secondo.

RG-3 Scalabilità

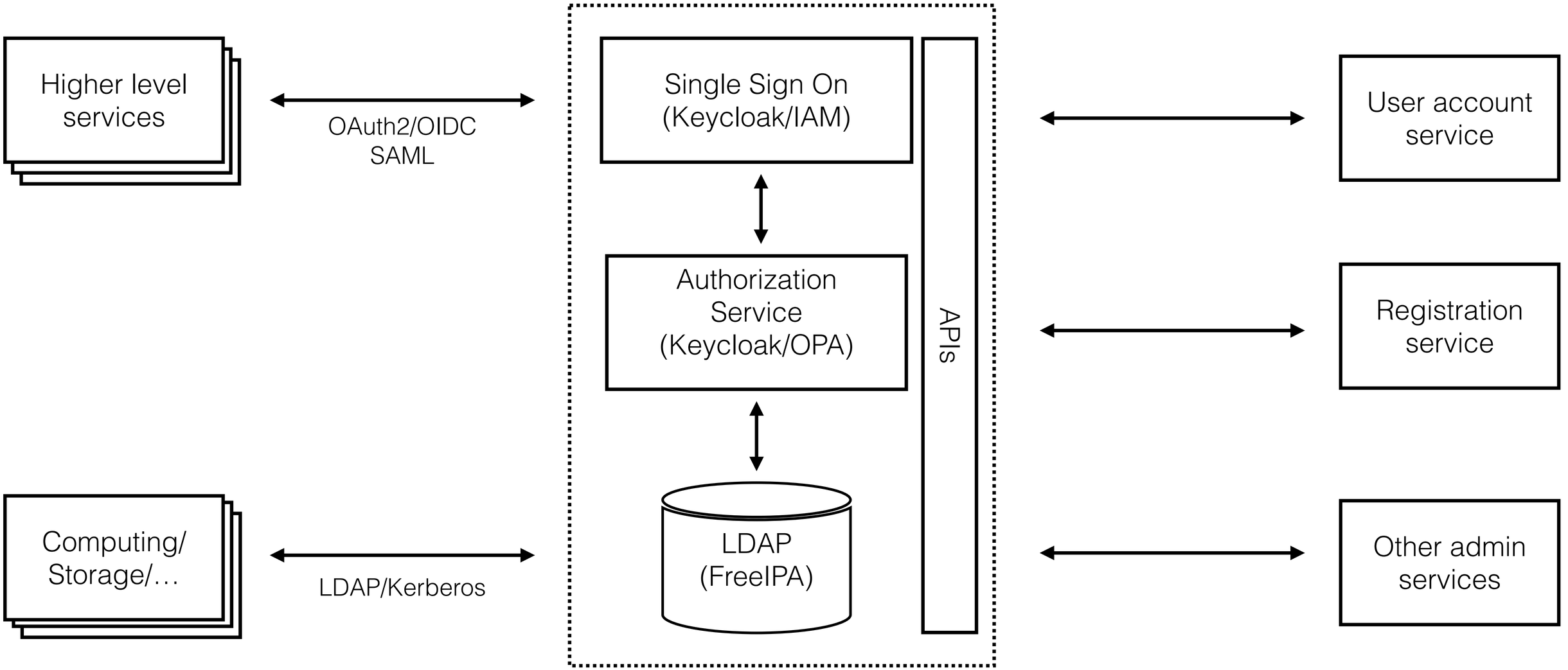
La nuova AAI del CNAF dovrà essere in grado di sostenere il carico di richieste generato dai sistemi del centro, in linea con le previsioni di crescita del centro dei prossimi X anni.

Implicazioni: caching ad ogni livello. Già ora se non ci fosse caching non riusciremmo a rispondere alle richieste, e il problema non può far altro che peggiorare. Occorre necessariamente essere in grado di fare tuning preciso di tutti i parametri relativi al caching.

RG-4 Sostenibilità

L'AAI deve essere basato su soluzioni open source ben supportate~~,~~ ed adottate anche in altri

Architettura proposta della nuova AAI del CNAF



Architettura della nuova AAI del CNAF

Da definire formalmente, ispirandosi all'esperienza di centri con esigenze simili al nostro

Componenti principali:

- **Directory and authentication service**: implementa l'albero LDAP del CNAF e il server Kerberos
  - Tecnologia proposta: FreeIPA
- **Single Sign On service:** abilita l'integrazione con meccanismi di autenticazione esterna (EduGAIN, INFN AAI), implementa supporto a MFA e fornisce un OpenID Connect/SAML authentication/authorization hub verso l'LDAP del CNAF
  - Tecnologia proposta: Keycloak/IAM
- **Authorization service:** definisce le policy di autorizzazione per l'accesso alle risorse.
  - Tecnologia proposta: Keycloak + API sviluppate internamente + Open Policy Agent
- **User account service:** permette all'utente di gestire il proprio account (e.g., reset della password, richiesta di appartenenza a gruppi, etc…)
  - Tecnologia proposta: Keycloak/sviluppo interno web application
- **Registration service:** implementa la procedura di registrazione per ottenere un account al CNAF
  - Tecnologia proposta: Keycloak/sviluppo interno web application
- **Altri servizi di gestione**: e.g., gestione pool account, etc…
  - Tecnologia proposta: Scripting su API FreeIPA/sviluppo interno

Attività principali e stima manpower

#	Main activities	Effort (PM)
2.2.1	• Requirements gathering & architecture definition • Technology selection & initial prototyping	6
2.2.2	• HA setup for core AAI components (FreeIPA, Keycloak) • Integration with CNAF provisioning & monitoring	12
2.2.3	• Definition & test of migration strategies from the current AAI	6
2.2.4	• Test integration with resources (WNs, UIs, storage, bastion, mail services, VPN,…) • Test integration with higher level services con Keycloak (Cloud@CNAF, K8S@CNAF, …)	18
2.2.5	• Definition of requirements and procedures for the account lifecycle • Design and development of user account and registration services • Integration with CNAF provisioning and monitoring	18
2.2.5	• Evaluation of Open Policy Agent and Keycloak authorization services • Design and development • Integration with CNAF provisioning and monitoring	12

Milestone

Una serie di milestone collegate alle attivita' principali sono state definite nella bozza del TDR

Manca ancora una stima per milestone delle presunte date di consegna (difficile da fare senza senza avere una visione chiara dell'effort a disposizione)

Milestone number	Milestone name	Delivery date	Comments
M2.2.1	Definition of CNAF AAI requirements	TBD	
M2.2.2	Definition of CNAF AAI architecture		
M2.2.3	Definition of migration strategy from the current infrastructure		
M2.2.4	Prototype for the HA deployment setup for core AAI services		
M2.2.5	Prototype working AAI integration with worker nodes and computing services		
M2.2.6	Prototype working AAI integration with storage services		
M2.2.7	Prototype working AAI integration with mailing services		

Timeline di massima

	2021				2022				2023			
Activity	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Definition of requirements & architecture												
Deployment core services @ CNAF												
Migration strategy definition & testing												
Integration testing												
Design, develop & testing User, Registration & Authorization services												
Deployment of AAI services @ Tecnopolo												
Integration & testing @ Tecnopolo												

Criticita’

Effort

- chi lavora su questa migrazione/evoluzione dell’AAI? in che percentuale di tempo?

Difficile avere un reale bootstrap delle attività in mancanza di una risposta a questa domanda