AAI-2.0

Workshop sul calcolo nell'INFN

Paestum 26 maggio 2022

Antonella Monducci per AAI-WG

Perché AAI-2.0?

- INFN-AAI è uno strumento/infrastruttura essenziale per il funzionamento dell'INFN in quanto necessario all'accesso ai servizi nazionali ed ai servizi IT erogati dalla Direzione Sistemi Informativi
- Purtroppo finora, a parte i pochi casi "fortunati" relativi a strutture che usano autenticazione Kerberos, INFN-AAI non è usata per l'accesso ai servizi IT nelle strutture
- AAI-2.0 vuole continuare ad avere il ruolo chiave nell'AA dei sistemi nazionali e fornire tutti gli strumenti necessari per il suo utilizzo in ogni struttura

Il nuovo disegno: 4 pilastri fondamentali

- Sicurezza
- Identità vs Account
- Fruibilità
- Gestione

Sicurezza

2FA/MFA

- L'introduzione di un sistema di autenticazione a due fattori o multifattore è un processo ormai necessario.
- Dobbiamo ancora valutare quali sistemi adottare
- Saranno fondamentali alcuni parametri/caratteristiche
  - Supporto (sistemi supportati dalle varie applicazioni)
  - Infrastruttura necessaria/meccanismi di erogazione
  - Costo

Identità VS account

Identità Digitale VS account

- Il nuovo modello separa nettamente le identità digitali e dagli account permettendo l'assegnazione di più account ad una stessa identità digitale.
- Gli account potranno essere:
  - Account Personali
    - base
      - derivati
    - di ruolo
  - Account di servizio

Fruibilità

Arricchimento

- Possibilità di arricchire un account con l'inserimento di attributi (compatibili con lo schema LDAP) per vari scopi
  - POSIX
  - Mail routing (mailDrop)
  - …
  - 2FA/MFA
  - Entitlement ed altri attributi "ereditati" dall'identità

Gestione

LDAP tools & ACI

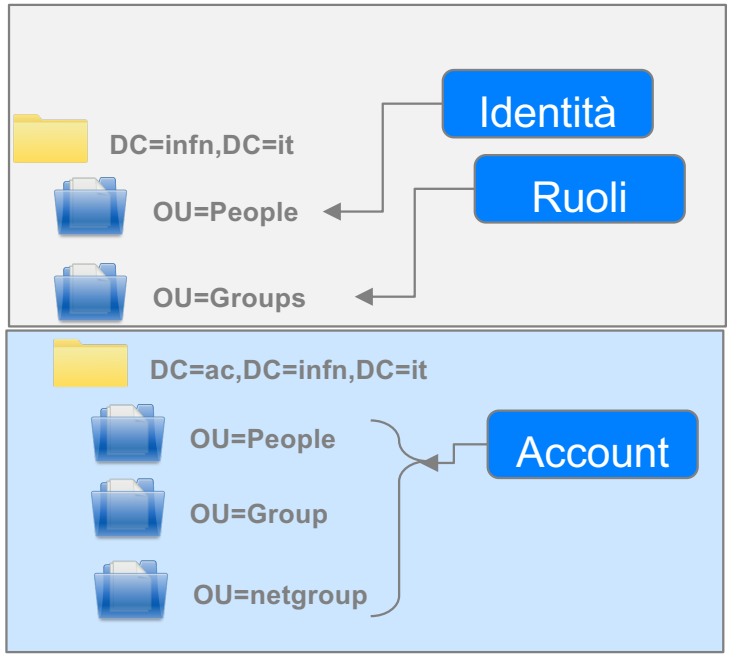
- Il 389 Directory Server permette di definire ACI (Access Control Instructions) che verranno quindi utilizzate per definire opportune policy di accesso.
- La gestione delle entry e degli attributi avverrà, per tutte le operazioni di modifica, usando gli strumenti standard LDAP.
- Per le sole operazioni di creazione di una entry e di modifica delle ACI dovrà essere utilizzato un opportuno wrapper che
  - Costruisca adeguatamente la ACI relativa all'entry
  - Garantisca i vincoli di definizione dell'entry stessa (es non deve essere possibile assegnare i medesimi attributi POSIX a identità differenti nella stessa struttura/scope/tag)

Modello implementativo

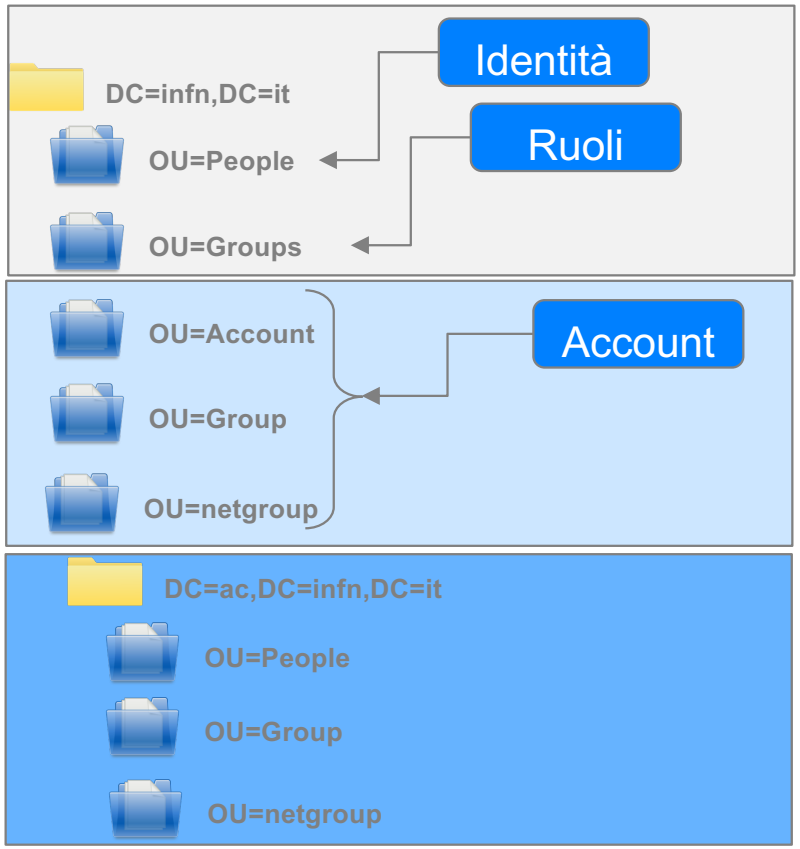
Disclaimer

- Quello che segue è solo un esempio di implementazione.
- Dobbiamo definire i dettagli sugli attributi da usare, effettuare verifiche di funzionalità e definire le policy di gestione degli account e degli attributi
- I punti fermi (finora) sono:
  - Albero LDAP basso e grosso con attributi discriminativi all'interno dell'entry
  - Gli account possono essere anche «multi-scope»

AAI VS AAI-2.0



Dati da GODiVA
Dati da Servizi Calcolo
Rami locali (mantenuti ad esaurimento)



Implementazione

- Gli account di AAI-2.0 saranno entry in un ramo dedicato dell'LDAP

  `OU=Account,DC=infn,DC=it`
- Ogni entry conterrà attributi che:
  - Identificano proprietario e gestore
    - infnLinkedUUID
    - infnAccountManager
  - Determinano l'utilizzabilità
    - POSIX
    - Servizi per i quali tale account è utilizzabile
      - infnAccountValid

```
# 18b4d521-6058-4668-82e2-87b170e34450, Account, infn.it
dn: infnUUID=18b4d521-6058-4668-82e2-87b170e34450,
 ou=account,dc=infn,dc=it
objectClass: top
objectClass: infnAccount
. . .
objectClass: posixAccountx
infnUUID: 18b4d521-6058-4668-82e2-87b170e34450
infnLinkedUUID: 6428a2a1-814b-4fd0-87cc-fe86dc4b8863
infnAccountManager: urn:mace:infn.it:ou:roma1:sicr
l: roma1
infnAccountValid: urn:mace:infn.it:ou:roma1:all-services
mail: John.Doe@infn.it
maildrop: johndoe@mbox3.roma1.infn.it
uidNumber: 12345
gidNumber: 3210
cn: John Doe
homeDirectory: /home/johndoe
loginShell: /bin/bash
uid: johndoe
userPassword::e1NTSEF9ekFyZUc4cmtXaXdoOW9ST3BBczRSY1d1WUJ5
d1JJcWVVOGFhdGc9PQ==
```

LDAP client

- I servizi dovranno essere configurati con appositi filtri LDAP per selezionare solo le entry abilitate a tale servizio
- Ad esempio, il filtro per un servizio di public login offerto dalla sezione di Roma1 potrebbe essere analogo al seguente

```
id_provider = ldap
access_provider = ldap

ldap_search_base = ou=account,dc=infn,dc=it
ldap_access_filter = (&(|(infnAccountValid=urn:mace:infn.it:ou:roma1:all-services)(infnAccountValid=urn:mace:infn.it:ou:roma1:login))
                      (|(eduPersonEntitlement=urn:mace:infn.it:ict-gracetime:true)(eduPersonEntitlement=urn:mace:infn.it:sicurezza-informatica-base)))
```

Account multi-site

- Account di questo tipo possono essere riutilizzati per fornire accesso ad altri servizi in altre strutture
  - Roma1: tutti i servizi
  - Le: solo login

```
# 18b4d521-6058-4668-82e2-87b170e34450, Account, infn.it
dn: infnUUID=18b4d521-6058-4668-82e2-87b170e34450,
 ou=account,dc=infn,dc=it
objectClass: top
objectClass: infnAccount
. . .
objectClass: posixAccountx
infnUUID: 18b4d521-6058-4668-82e2-87b170e34450
infnLinkedUUID: 6428a2a1-814b-4fd0-87cc-fe86dc4b8863
infnAccountManager: urn:mace:infn.it:ou:roma1:sicr
l: roma1
infnAccountValid: urn:mace:infn.it:ou:roma1:all-services
infnAccountValid: urn:mace:infn.it:ou:le:login
mail: John.Doe@infn.it
maildrop: johndoe@mbox3.roma1.infn.it
uidNumber: 12345
gidNumber: 3210
cn: John Doe
homeDirectory: /home/johndoe
loginShell: /bin/bash
uid: johndoe
userPassword::e1NTSEF9ekFyZUc4cmtXaXdoOW9ST3BBczRSY1d1WUJ5
d1JJcWVVOGFhdGc9PQ==
```

Account multi-site Roma1 e Lecce

- Configurazione client di Roma1

```
id_provider = ldap
access_provider = ldap

ldap_search_base = ou=account,dc=infn,dc=it
ldap_access_filter = (&(|(infnAccountValid=urn:mace:infn.it:ou:roma1:all-services)(infnAccountValid=urn:mace:infn.it:ou:roma1:login))
                      (|(eduPersonEntitlement=urn:mace:infn.it:ict-gracetime:true)(eduPersonEntitlement=urn:mace:infn.it:sicurezza-informatica-base)))
```

- Configurazione client di Lecce

```
id_provider = ldap
access_provider = ldap

ldap_search_base = ou=account,dc=infn,dc=it
ldap_access_filter = (&(|(infnAccountValid=urn:mace:infn.it:ou:le:all-services)(infnAccountValid=urn:mace:infn.it:ou:le:login))
                      (|(eduPersonEntitlement=urn:mace:infn.it:ict-gracetime:true)(eduPersonEntitlement=urn:mace:infn.it:sicurezza-informatica-base)))
```

Attributi POSIX

- Sulla carta SSSD può essere configurato per ri-assegnare uidNumber e gidNumber in funzione dei valori presi dall'LDAP, ma dobbiamo verificare
- L'idea è di definire un «offset» per struttura in modo che l'uidNumber 2214 di Lecce diventi un uidNumber AAI differente da quello ottenuto dallo stesso uidNumber di Genova. Ad esempio:
  - LE-offset = 1000000
    - uidNumber 2214 → uidNumber 1002214
  - GE-offset = 1010000
    - uidNumber 2214 → uidNumber 1012214

Slave di Sede

- Nessun cambiamento rispetto alla situazione attuale.
- Negli slave di sede verranno copiati i dati del ramo locale e del ramo nazionale.
- Da sottolineare che il ramo nazionale conterrà le OU relative ad Account, Group (POSIX), NetGroup, che al loro interno avranno i dati relativi alle varie strutture/scope/tag che specificano la validità dei vari oggetti.

Conclusioni

Norme transitorie

- Stiamo ancora raccogliendo feedback in modo da rendere AAI-2.0 utilizzabile a pieno in tutte le strutture ed nei vari scenari (farm, tier, …)
- Nelle prossime settimane fermeremo questo processo per definire il disegno del wrapper ed inizieremo lo sviluppo.
- Ovviamente AAI-2.0 sarà una estensione dell'attuale implementazione, ma non prevediamo di mantenere il "doppio forno" per il resto della vita
  - N (12?) mesi di supporto sull'attuale configurazione
  - Supporto alla migrazione alla nuova configurazione

The End

Grazie

Domande?