Stato attuale e requirements

Stato attuale (1)

- Il sistema di AAI del TIER-1 è attualmente basato su LDAP (autorizzazione) e Kerberos (autenticazione)
  - Ognuno dei due servizi prevede un server primario ed uno secondario.
- Account creati e gestiti in modo semi-automatico (alcuni script di ausilio)
  - Prerequisito: firma di accettazione del Disciplinare dell'INFN
  - Scadenza della validità delle password gestita in automatico (scadenza annuale).
- Frontiera costituita da un bastione (bastion.cnaf.infn.it)
  - Una macchina di produzione ed una di scorta (cold spare).
  - Non c’e’ home-directory condivisa

Stato attuale (2)

- LDAP effettua mapping fra username e credenziali Unix (uid, gid).
  - Mapping non biettivo: (persona, exp) → user
  - Esclusi utenti con uid<500 (e.g. root è sempre un utente locale).
  - Home directory su UI, wn, etc.. organizzate secondo lo schema <exp>/<user>

UI, wn	Mapping utenti, authn, authz via LDAP/kerberos
disk-server	Solo utente root: non usa sistema LDAP/Kerberos
Gridftp, storm, xrootd	Download mapping utenti da LDAP (no real-time)

Stato attuale (3)

1. Accesso interattivo: Utente (U) per login su risorsa (R), viene autenticato da kerberos. R da LDAP ottiene mapping username
2. Accesso grid: U presenta proxy VOMS a R che, tramite gridmap o altro, mappa su pool-account (e quindi via LDAP)
3. Accesso cloud: U viene rediretto da R a IAM e da questo ad un IDP

Punti deboli

- Il sistema non si interfaccia ne' con i nuovi protocolli di autorizzazione basati su token (OIDC) ne' con portali IdP (es. AAI INFN)
  - Solo credenziali Unix e certificati X.509
  - Cloud@CNAF usa sistema AAI separato
- SO dei server obsoleto
  - In corso test per upgrade
- Necessaria verifica ed eventuale consolidamento/automazione del sistema di backup dei server (Krb/LDAP);
- Manca elasticità associazione persona a piu' esperimenti
- Migliorare l'automatizzazione della creazione delle home directory
- Invio modulo AUP firmato non avviene in modalità web.

Requisiti sistema AAI

- Unico realm utenze locali
  - Uso di un database centrale (es. LDAP), in modalità’ real-time o meno, è essenziale per mantenere la coerenza delle credenziali Unix attraverso tutte le risorse del centro.
-

Requisiti strutturali

- Sostenibilità: basato su soluzioni open source, possibilmente adottate anche da altri centri simili al nostro e con, possibilmente, un buon supporto;
- Solidità e resilienza: no “single point of failure” ed "autoconsistenza";
- Scalabilità: in grado di rispondere a tutte le "query" dei nodi del centro (tenendo presente che il numero dei nodi aumenterà);
- Efficacia: Il sistema di autorizzazione delle domande di accesso dovrà essere semplice e mai bloccante;
- Tracciabilità (accountability): Tutte le operazioni di richiesta ed autorizzazione devono essere "Loggate" in modo opportuno in modo da avere traccia di chi è stato autorizzato, da chi e quando. Inoltre deve esserci traccia della accettazione del disciplinare o eventuali incarichi di amministrazione.

Requisiti funzionali (1)

- Gestione prima identificazione
  - Riconoscimento sicuro (tramite documento di identità presso una RA o simile)
    - Utenti INFN (con accesso AAI) gia' identificati
  - Firma AUP in digitale (con timestamp)
    - Per WLCG fa testo MoU: e gli altri?
- Rispondenza a GDPR
  - Diritto ad oblio
  - Conservazione sicura dati sensibili (copie documenti se ci sono, dati anagrafici, email, altro?)
  - altro?

Requisiti funzionali (2)

- Implementazione single sign on su risorse Tier-1 e cloud@CNAF
  - Controllo centralizzato ed univoco utenti (e.g. uid/gid univoci per utente)
    - Gestione fine permessi per gruppo/utente e risorsa;
    - Possibilità di avere delle "viste" differenti, per consentire una maggiore flessibilità sugli utenti creati (i.e. evitare di creare multipli account per lo stesso utente su diversi esperimenti);
    - Verifica periodica account ed eventuale cancellazione.
  - Stoccaggio della propria chiave ssh al fine di poter fare login senza pwd su tutti nodi abilitati
- Compatibilitá con cloud, grid, locale
  - Possibilità di importare utenti da AAI, evitando doppie registrazioni per utenti INFN
  - Compatibilitá con GSI, OIDC, Oauth2, SAML, CAS, etc.