Istituto Nazionale di Fisica Nucleare

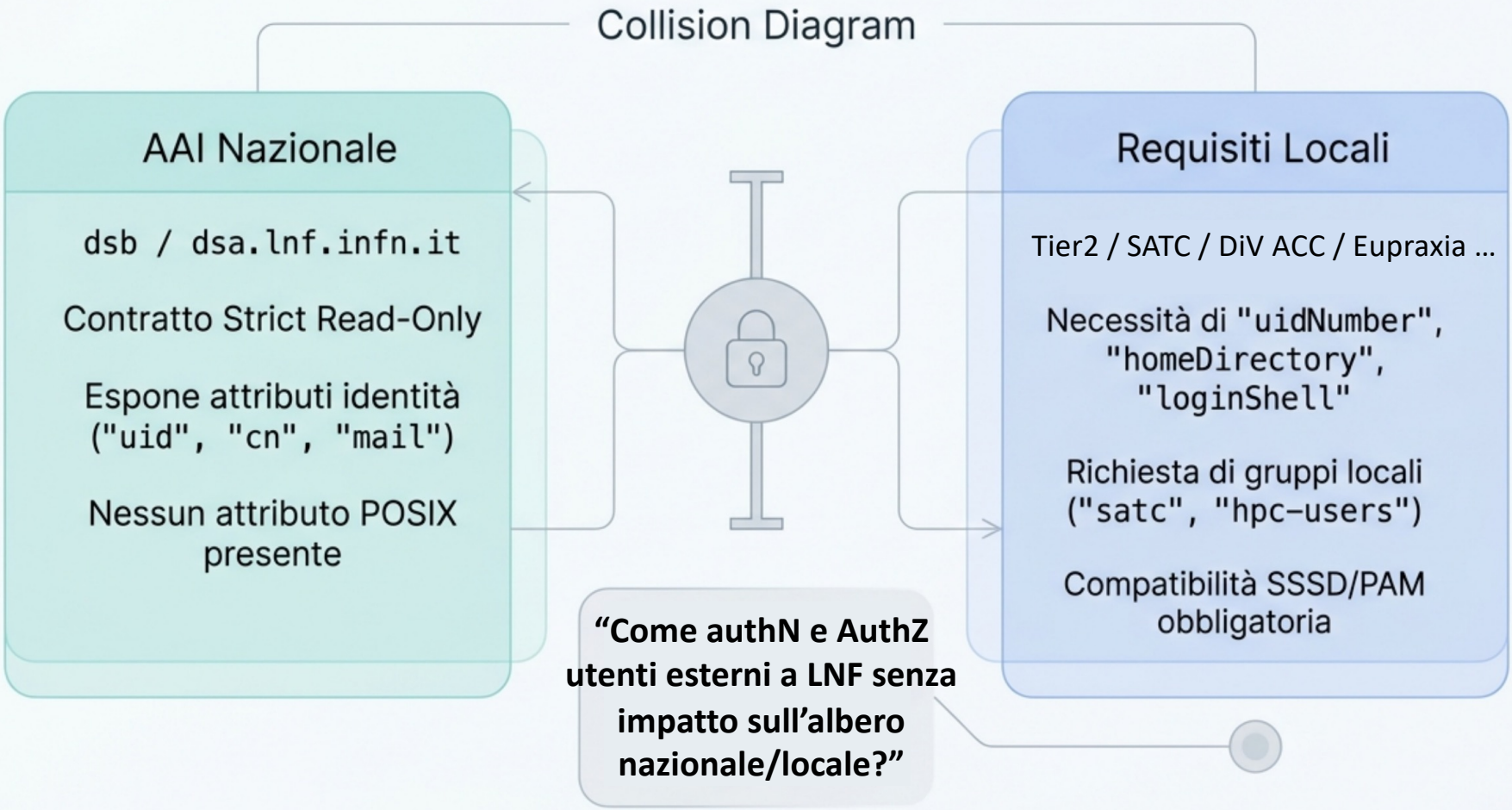
Autenticazione POSIX su AAI INFN: L'Approccio Translucent Overlay

Architettura a doppio database per estensioni locali a impatto zero sul backend nazionale.

Riccardo Gargana, Igor Abritta Costa, Dael Maselli

Workshop CCR 2026 - 11-15/05/2026

Il blocco architetturale: AAI immutabile vs Requisiti POSIX



Analisi delle alternative: Perché "slapo-translucent" ?

Criterio	Modifica AAI	Branch Locale	Albero per Progetto	Translucent Overlay
Impatto sul tree nazionale	Alto	Medio	Medio-Alto	**Nessuno**
Duplicazione entry utente	No	Sì	Sì	**No**
Rischio collisioni uid/gid	Alto	Medio	Alto	**Basso/Locale**
Compatibilità SSSD	Nativa	Richiede tuning	Richiede tuning	**Nativa**
Complessità Operativa	Alta	Media	Molto Alta	**Bassa**
Costo politico/governance	Molto Alto	Medio	Alto	**Basso**

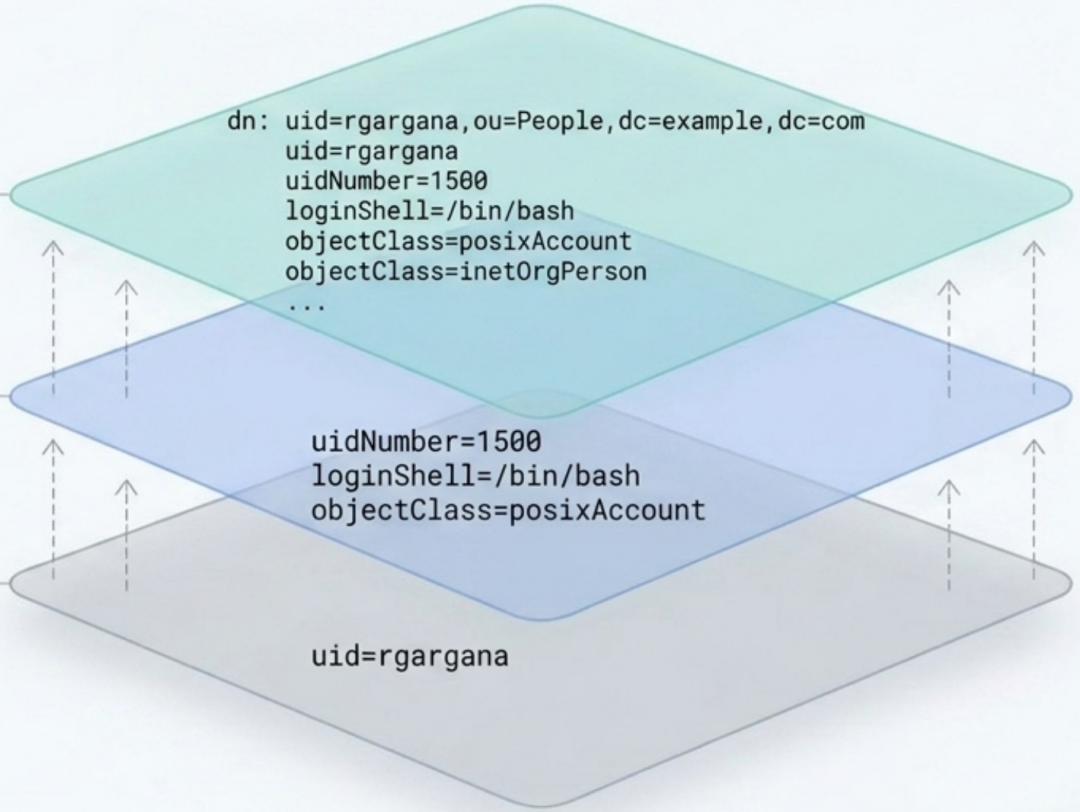
La Soluzione: Overlay `slapo-translucent`

Fusione attributi a tempo di ricerca. Nessuna duplicazione.

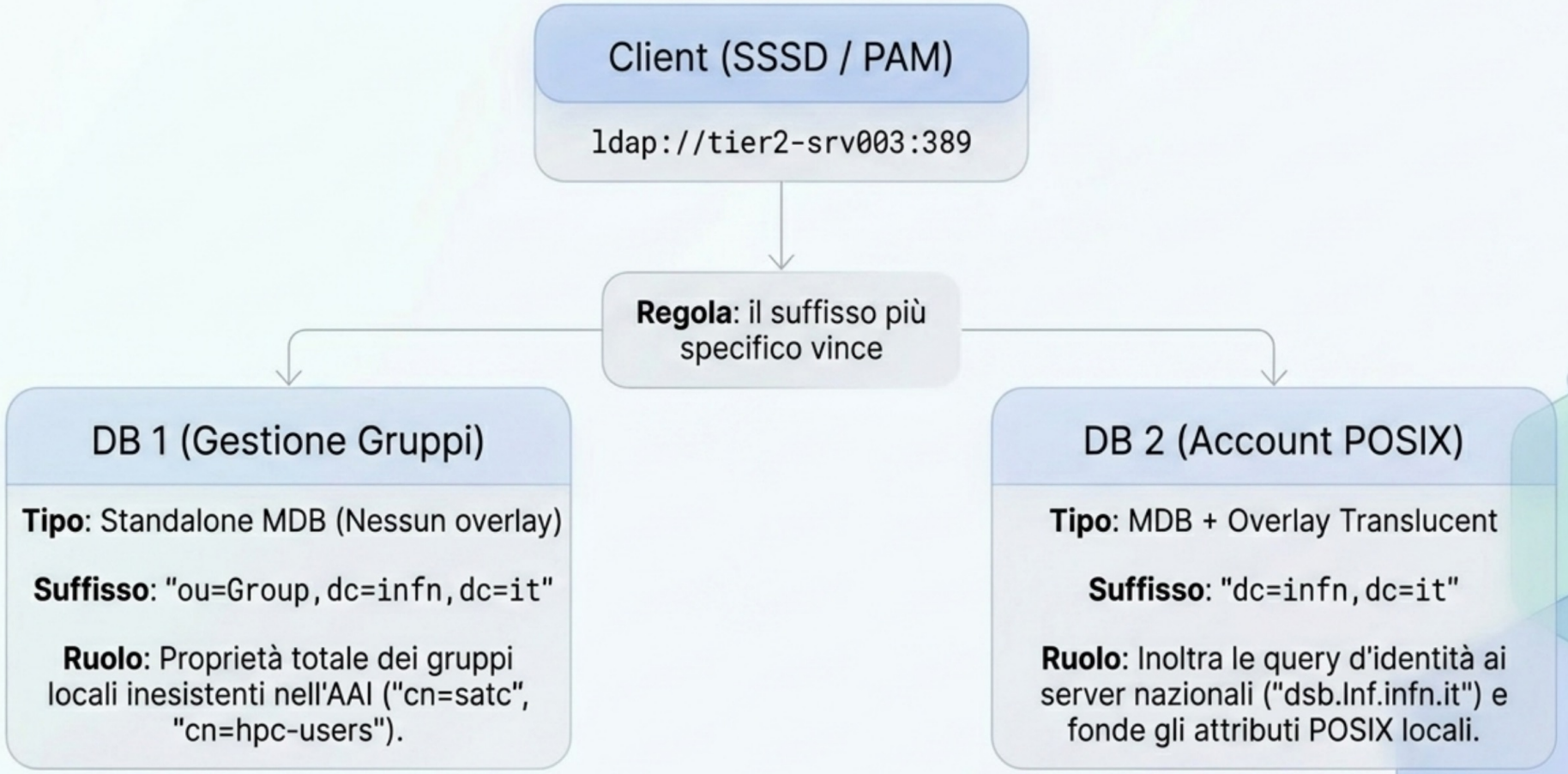
Risultato (Client): SSSD vede un'unica entry combinata e coerente.

Database MDB Locale: Aggiunge o sovrascrive attributi per entry.

Backend Remoto: Mantiene la canonicalità dell'identità (AAI intatto).



Architettura del motore a due database



La sala macchine: Direttive di configurazione (“slapd.conf”)

```
database    mdb
suffix      "dc=infn,dc=it"

overlay     translucent
uri         "ldap://dsb.lnf.infn.it
             ldap://dsa.lnf.infn.it"

translucent_local  objectClass
                   uidNumber
                   gidNumber
                   ...
translucent_remote uid

translucent_strict
```

Gli attributi POSIX e l'abilitazione del filtro SSSD ("**objectClass=posixAccount**") sono letti esclusivamente dal database MDB locale.

Il "uid" rimane il parametro canonico recuperato dal backend.

Protezione attiva: Blocca qualsiasi tentativo di scrittura verso l'AAI nazionale.

Caso d'uso

```
ldapsearch -x -H ldap://tier2-srv003.lnf.infn.it:389 -b 'ou=people,dc=infn,dc=it' '(&(uid=rgargana)(objectClass=posixAccount))'
```

```
mail: Riccardo.Gargana@lnf.infn.it
o: Istituto Nazionale di Fisica Nucleare
ou: Laboratori Nazionali di Frascati
EDUPERSONORGDN: dc=infn,dc=it
SCHACHOMEORGANIZATION: infn.it
SCHACHOMEORGANIZATIONTYPE: urn:schac:homeOrganizationType:it:researchInstituti
 on
EDUPERSONAFFILIATION: staff
EDUPERSONAFFILIATION: member
l: lnf
SCHACPROJECTMEMBERSHIP: staff-lnf
SCHACPERSONALUNIQUECODE: urn:schac:personalUniqueCode:it:infn.it:matricola:000
 1200969
SCHACPERSONALUNIQUECODE: urn:schac:personalUniqueCode:it:infn.it:BADGE:731023
SCHACPERSONALUNIQUECODE: urn:schac:personalUniqueCode:it:infn.it:RFID:23102b52
 1276ee4a4cdc869d717c8743
loginShell: /bin/bash
homeDirectory: /home/rgargana
gidNumber: 3127
uidNumber: 6982

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Merge degli attributi del back-end con quelli del translucent

```
[root@tier2-ui006 ~]# id rgargana
uid=6982(rgargana) gid=3127(macchina) groups=3127(macchina),3805(satc),30020(hpc-opt),30000(hpc-users)
[root@tier2-ui006 ~]# getent passwd rgargana
rgargana:*:6982:3127:Riccardo Gargana:/home/rgargana:/bin/bash
[root@tier2-ui006 ~]#
```

Dispiegamento di sssd tramite puppet

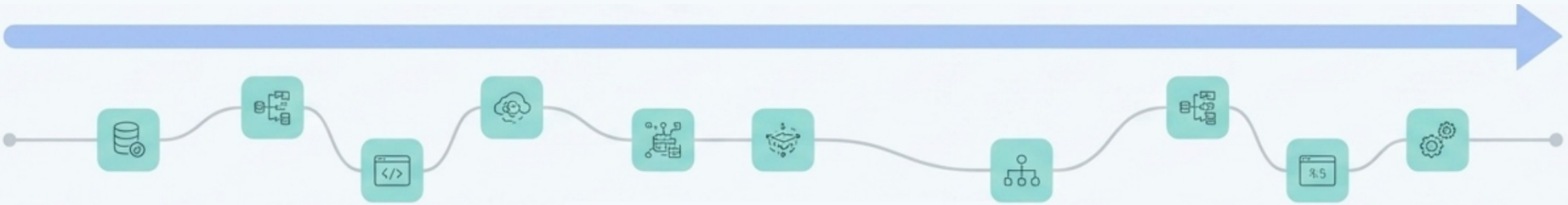
Puppet Class Parameters

Puppet Class	Name	Value	Omit
infn_accounts	auth_provider	ldap	☐
	automount_media_gnome_disable	false	
	change_root_password	true	
	conf_ssh	true	
	enable_aai	true	
	enable_gdm_ldap_login	false	
	enablesudo	--- |	
	groupadd	"undef"	
	http_proxy_os_enabled	false	
	ldap_access_filter	(objectClass=posixAccount)	☐
	ldap_anonymous_bind	true	☐
	ldap_ca_cert_filename	ca_srv003_lnf.pem	☐
	ldap_default_bind_dn	${infn_accounts::params::ldap_default_bind_dn}	
	ldap_search_base	ou=People,dc=infn,dc=it	☐
	ldap_search_group_base	ou=Group,dc=infn,dc=it	☐
	ldap_uri	["ldap://tier2-srv003.lnf.infn.it"]	☐
	root_hash	${infn_accounts::params::root_hash}	
	server_options	"{\"HostKey\":[\"/etc/ssh/ssh_host_rsa_key\",\"/etc/ssh/ssh_host_ecdsa_key\",\"/	

Submit Cancel

Disaccoppiamento tra AAI ed esigenze locali

Governance Nazionale



Agilità Locale (SATC, HPC, DIVACC, Eupraxia…)

Scalabilità per progetto: un container slapd per sito senza creare molteplici alberature sul nazionale

Nessuna deriva dei dati: "uid" rimane canonico nel tree nazionale, eliminando del tutto la duplicazione.

Garanzia architettonica: La direttiva "translucent_strict" rende esplicito e inviolabile il contratto di sola lettura verso dsb/dsa.lnf.infn.it.

Le necessità posix locali sono pienamente soddisfatte mentre la struttura ldap nazionale rimane assolutamente intatta

USABILITÀ IN CASO DI VARIAZIONI SUL BACKEND

- Non ci sono impatti in locale se si aggiungo dati POSIX su alberatura Nazionale/Rami ad-hoc

FEATUREs

- Arbitrarietà shell utenti
- Arbitrarietà directory home degli utenti
- Demandare l'AuthN sul translucent e usare altri segreti*
- Enable RSA key sul translucent*
- Progetto dockerizzato
- Progetto su baltig anonimizzato
  https://baltig.infn.it/lnfsatc/ldap_translucent

* Test in progress