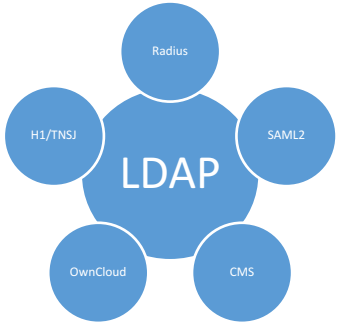
A&A INAF


H1
anagrafica
OwnCloud
eduRoam
CAT
ICT
TNSJ
missioni
IDEM
MAIL
eduGAIN
CED
IA2

Autenticazione&Autorizzazione

- **AUTENTICAZIONE**: è l'operazione di riconoscimento della persona che cerca di accedere ad una risorsa, sia hardware (collegamento al network o login su di un computer), sia software (utilizzo di una web application o di una applicazione software);
  - È gestita direttamente dal computer che fornisce il login o l'applicazione (per Linux PAM) o demandata ad un sistema remoto (LDAP, radius, Kerberos, MySQL);
  - INAF usa un server LDAP di Ente per l'autenticazione dei propri utenti, può gestire gruppi e informazioni di autorizzazione in modo diretto.
  - Il server LDAP è utilizzato da diversi framework di autenticazione come Shibboleth (SAML2) per IDEM o freeRadius per eduRoam;



  - È comunque preferibile per le applicazioni che coinvolgono più enti, sia nazionali che internazionali, avere un sistema di autorizzazione gestito direttamente dall'applicazione. Non è pensabile l'inserimento o la modifica di un attributo su più server distribuiti geograficamente e gestiti da persone diverse.

Autenticazione&Autorizzazione

- **AUTORIZZAZIONE**: dopo il “CHI?” dell’autorizzazione, gestisce il “COSA” dell’applicazione. Che cosa si è autorizzati a utilizzare di una risorsa di calcolo o di un sistema informativo, dipende dal tipo di account che possediamo, a quale gruppo appartiene il nostro account, quali i ruoli e quali i privilegi;

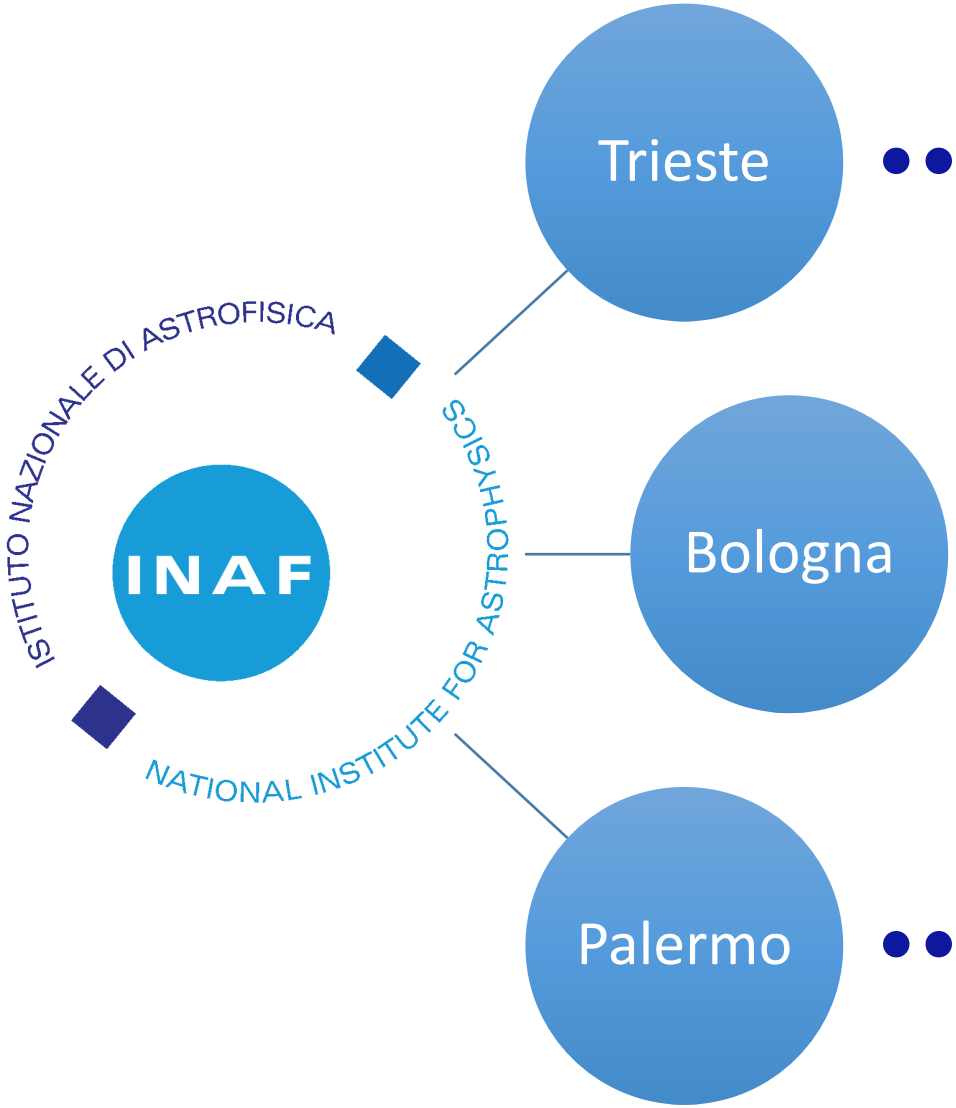
- Può essere gestita direttamente dal calcolatore in base al gruppo passato in fase di autenticazione (PAM/passwd) il comando uid sul mio Mac produce:

  uid=501(ftinarel) gid=20(staff) groups=20(staff),701(com.apple.sharepoint.group.1),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),399(com.apple.access_ssh),703(com.apple.sharepoint.group.3),33(_appstore),100(_lpoperator),204(_developer),395(com.apple.access_ftp),398(com.apple.access_screensharing),704(com.apple.sharepoint.group.4),702(com.apple.sharepoint.group.2)

- Può essere ricavata dal server LDAP attraverso il passaggio di particolari Entitlement, lo vedremo parlando dell’IdP Shibboleth;

- Può essere delegata a software come GROUPER che permette di creare e gestire una struttura complessa di gruppi e inserire o muovere utenti in/tra gruppi. È in grado di importare/esportare utenti/gruppi da e verso LDAP e DBMS, mette a disposizione API per dialogare direttamente con le applicazioni.

Server OpenLDAP CentOS 7



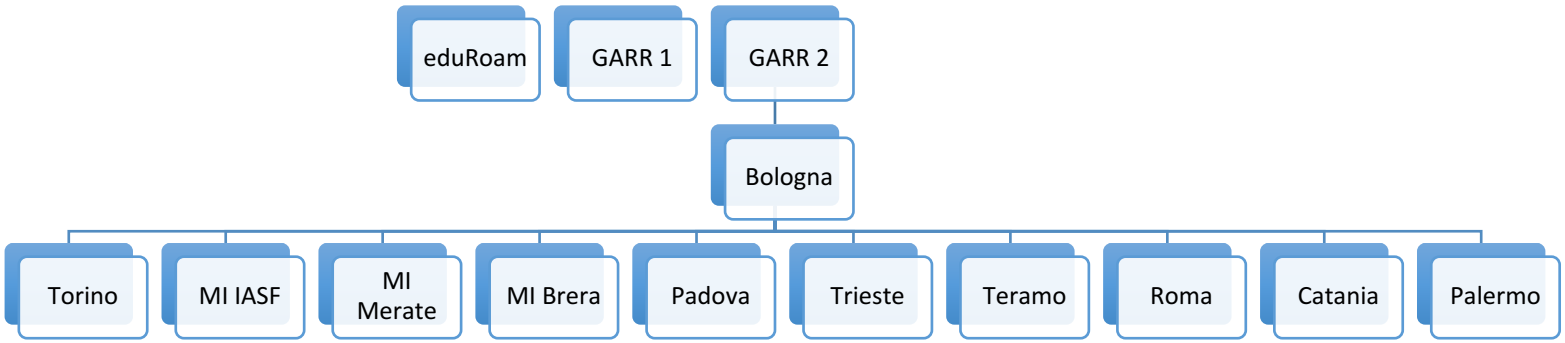
••REPLICA
140.105.72.40
ldapinaf.oats.inaf.it
TLS abilitato
rrDNS ldap.inaf.it

••MASTER
192.167.173.2
ldap.ced.inaf.it
TLS abilitato

••REPLICA
194.119.212.23
eduiasf.ifc.inaf.it
TLS abilitato
rrDNS ldap.inaf.it

Server freeRadius: eduRoam

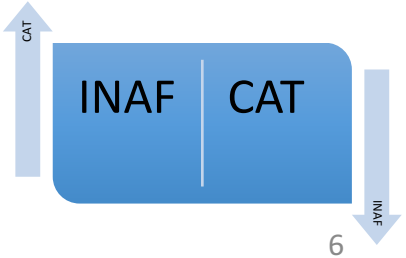
- Il server **freeRadius** installato a Bologna connette il **realm @inaf.it** ad **eduRoam** attraverso i due accessi italiani del **GARR**;
- **freeRadius** usa il server **LDAP** dell'Ente per le operazioni di **Autenticazione**, essendo **eduRoam** un servizio di accesso alla rete, l'autenticazione e l'autorizzazione corrispondono;
- Al server freeRadius di Bologna sono collegati in proxy 10 server INAF distribuiti su area geografica;
- Essendo un sistema gerarchico **eduRoam** deve sapere a quale **realm** appartiene una richiesta di autenticazione.
- Gli utenti **INAF** per autenticarsi devono usare il proprio account **nome.cognome** aggiungendo il realm **@inaf.it** (es. **franco.tinarelli@inaf.it**)
- Per facilitare la **configurazione** del proprio client di rete esiste un'applicazione chiamata **CAT** fornita da GÉANT agli enti accreditati;



eduRoam: CAT

eduroam Configuration Assistant Tool: https://cat.eduroam.org/?lang=it

- CAT serve per configurare facilmente il proprio dispositivo per la connessione WiFi a eduRoam;
- È stato preconfigurato per la connessione al server freeRadius di INAF e per accettarne il certificato server;
- Tutto il personale è autorizzato a scaricare il programma d'installazione;
- Dopo aver scelto INAF come organizzazione di appartenenza si entra nella pagina di Download;
- Eseguendo il programma scaricato viene configurata la connessione a eduRoam sul proprio dispositivo;



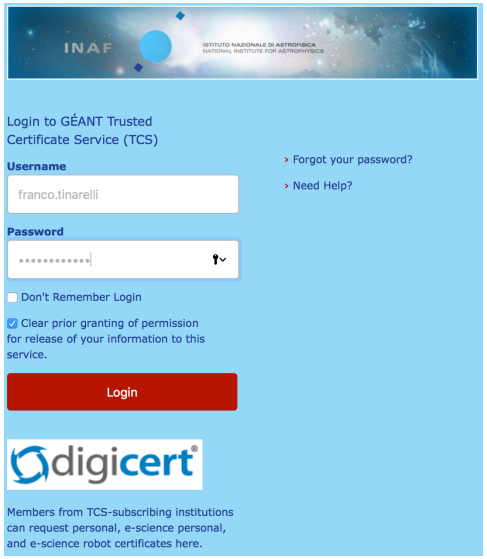
freeRadius: Proxy per eduRoam

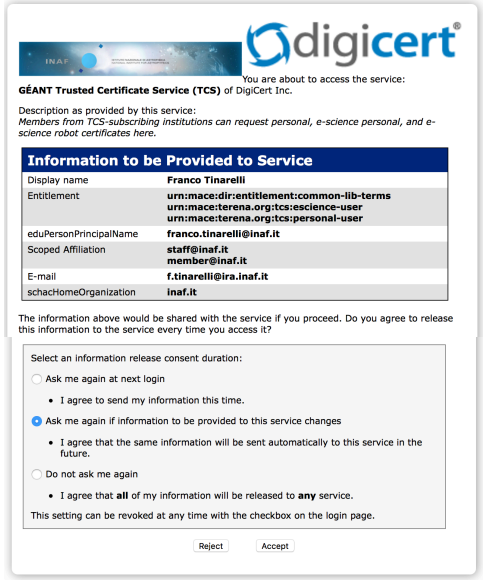
1. Configurate un server freeRadius per fornire il servizio ai vostri Access Point;
2. Configurate gli AP con **SSID eduroam,** è una precisa richiesta del consorzio;
3. Scaricate dal server web del CED tre files di esempio su come configurare il vostro freeRadius per fare proxy sul server principale: **http://www.ced.inaf.it/serv25/index.php/infrastruttura/infrastruttura/196-configurare-a-p-edu-roam**;
4. Mandatemi le informazioni sul vostro server: IP address e secret (password per accettare la connessione). Come esempio il record di Trieste registrato nel server principale:

```
# Proxy Trieste
client  eriador.oats.inaf.it {
        ipaddr          =  140.105.72.79/32
        secret          =  xxxxxxxxxxxx
        shortname       =  oats
```

5. Dopo alcuni test per verificare il corretto instradamento delle richieste di connessione inviatemi il file xml che descrive i vostri AP eduRoam, si trova nella stessa pagina web, modificate la sezione <location>…</location>, aggiungete più <location> per sedi diverse.

Server IDEM: Shibboleth IdP 3.2.1





- In giugno è stato aggiornato l'IdP di INAF, la versione è ora la 3.2.1.
- È stato abbandonato Tomcat per il più leggero Jetty;
- È cambiato il layout della finestra di login;
- È stata aggiunta la richiesta di autorizzare il rilascio delle proprie informazioni; Chiaro che se non le approvate non vi viene fornito il servizio!!!
- È registrato nell'Interfederazione eduGAIN;
- Usa **LDAP** per l'**autenticazione** degli utenti e per il rilascio di attributi di **autorizzazione** richiesti da alcuni servizi:
  - eduPersonEntitlement: urn:mace:dir:entitlement:common-lib-terms
  - eduPersonEntitlement: urn:mace:terena.org:tcs:escience-user
  - eduPersonEntitlement: urn:mace:terena.org:tcs:personal-user
- La username o **userID** per accedere ai servizi **IDEM** è **nome.cognome**;

- Statistica veloce da luglio 2016:
  - 1155 accessi;
  - Vconf il servizio più usato: 391 accessi;
  - Filesender: 103 accessi;
  - Science Direct: 97 accessi;
  - Nilde: 62 accessi;

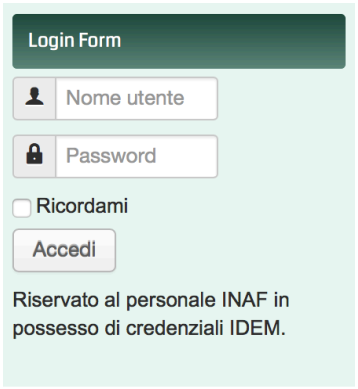
Assemblea Membri IDEM 01/12/2016 Firenze
Conferenza GARR The CreActive Network 30/11-02/12

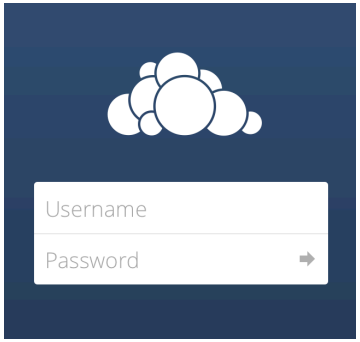
Con particolare riferimento al **Punto 7) all'OdG "Nuove proposte di candidature per il Comitato Tecnico Scientifico"** si ritiene utile precisare che nel corso della riunione in argomento, gli Enti Membri della Federazione potranno presentare nuove candidature per il Comitato Tecnico Scientifico al fine di arricchire il CTS già in carica.
Le nuove candidature per il Comitato Tecnico Scientifico dovranno essere accompagnate da un *Curriculum Vitae* dell'interessato, nonché da una *dichiarazione di disponibilità del candidato* e, ove prescritto, del suo ente di appartenenza a dedicare parte del proprio tempo lavorativo per gli scopi della Federazione.
Queste candidature potranno essere sottomesse via email al Coordinatore del CdI IDEM, Ing. Sandro Tumini (s.tumini@univpm.it) **entro il 28/11/2016 ore 12:00.**
Per maggiori informazioni sui compiti del CTS si veda l'art. 5.3 del Regolamento della Federazione IDEM.

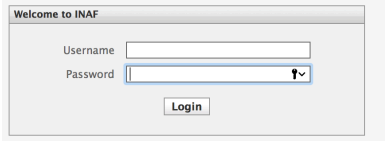
L'agenda della VII Assemblea dei Membri della Federazione IDEM sarà consultabile alla url: **http://www.eventi.garr.it/it/conf16/programma/assemblea-idem.** Nella stessa pagina web, saranno inoltre disponibili:

- le informazioni per il collegamento da remoto con Adobe Connect per i membri che non potranno essere presenti in loco e vorranno partecipare ed intervenire all'assemblea, ma senza diritto di essere eletti nè di votare;
- i documenti di supporto in riferimento ai Punti all'Ordine del Giorno.

CMS & OwnCloud & Mail







- I server web del **CED** e di **ICT** usano il **CMS Joomla** con modulo di **autenticazione LDAP;** Risolto il problema della registrazione con passaggio alla vers. 3.6 (Federico Gasparo);
- **OwnCloud** usa il server **LDAP** per l'autenticazione degli utenti INAF;
- del **Mail** Server di **INAF** ce ne ha parlato Francesco Bedosti, è il futuro, e se come spero sarà gestito internamente userà il server **LDAP** per l'autenticazione;
- Tutti **registrano** gli **utenti** al primo login in un loro data base interno **per** aggiungere informazioni di **autorizzazione**;
- La Username o il Nome utente è **nome.cognome**;

PER RIASSUMERE:

IDEM, OwnCloud, CMS: **nome.cognome**
eduRoam: **nome.cognome@inaf.it**

Stessa password per tutti i sistemi che si basano sul server LDAP **se il reset/cambio password viene fatto in modo corretto.**

Grazie per l'attenzione!