Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

# L'Identity Provider in the Cloud GARR:servizio IdP in the Cloud

*IdP in the cloud staff*

14 febbraio 2019

Webinar GARR IdP in the Cloud service

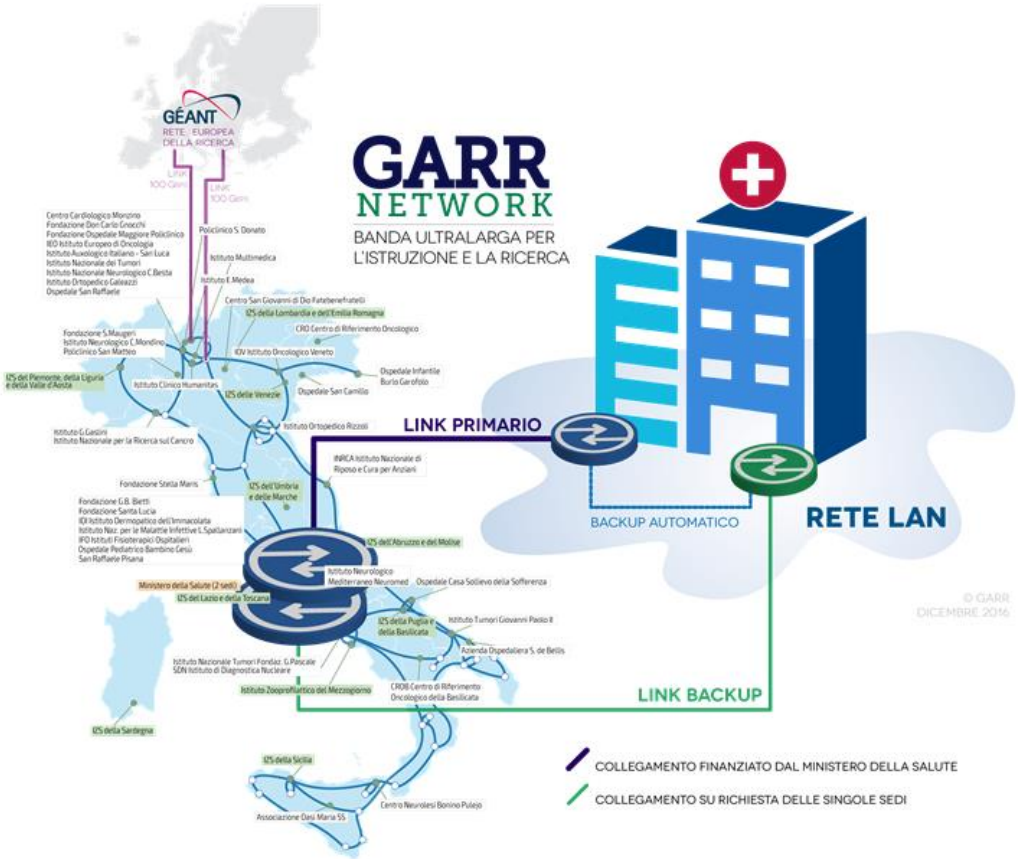
# GARR la rete nazionale della ricerca e dell'istruzione

**GARR** è innanzitutto una comunità: quella delle Università, della ricerca, dell'Istruzione e della cultura

**GARR** progetta, implementa e gestisce la Rete Italiana della Ricerca e dell'Istruzione, fornendo:

- ✓ connettività ad altissima banda, simmetrica e trasparente
- ✓ servizi tecnologicamente avanzati
- ✓ supporto alle E-Infrastructure e Infrastrutture di Ricerca

# Distribuzione nazionale degli istituti del Ministero della Salute




Infrastruttura è caratterizzata da:

- un circuito di accesso di ampia capacità di banda
- un apparato (tipo router) utile per l'attestazione del collegamento di accesso primario

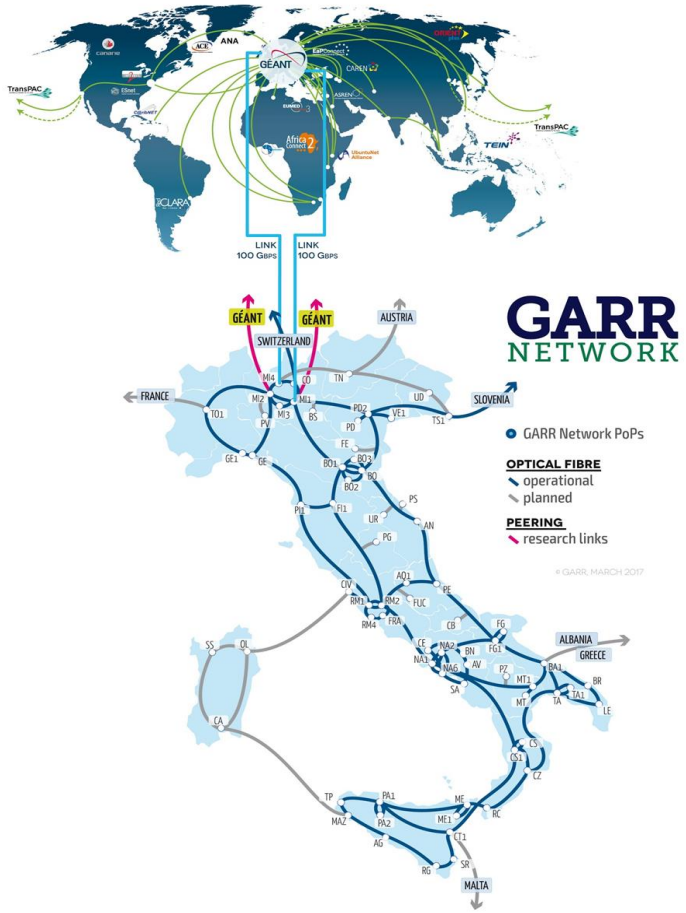
46 sedi IRCCS, 10 sedi IZS, sede CNAO, 2 sedi Ministero della Salute

# GARR: La Rete Nazionale della Ricerca e dell'Istruzione

GARR è innanzitutto una comunità: quella delle Università, della ricerca, dell'Istruzione e della cultura

Il GARR progetta, implementa e gestisce la Rete Italiana della Ricerca e dell'Istruzione, fornendo:

- connettività ad altissima banda, simmetrica e trasparente
- servizi tecnologicamente avanzati
- supporto alle E-Infrastructure e Infrastrutture di Ricerca



# Identity Providers e Federazione

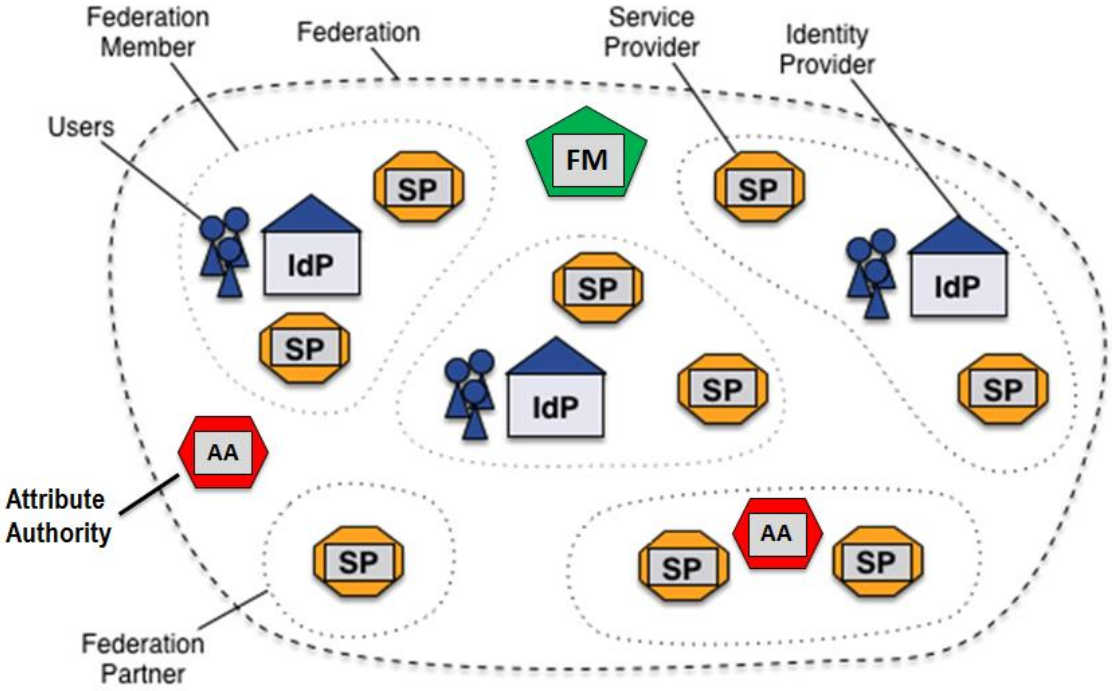
Le Federazioni di Identità del settore Ricerca e Istruzione mettono in relazione fornitori di identità (**IdP - Identity Providers**) e fornitori di servizi (**Service Providers**):

Creano e garantiscono un cerchio di fiducia in cui tutti gli attori sono tenuti a rispettare regole condivise

Riducono il carico amministrativo per la sottoscrizione dei servizi

Garantiscono il rispetto degli standard tecnici e di sicurezza

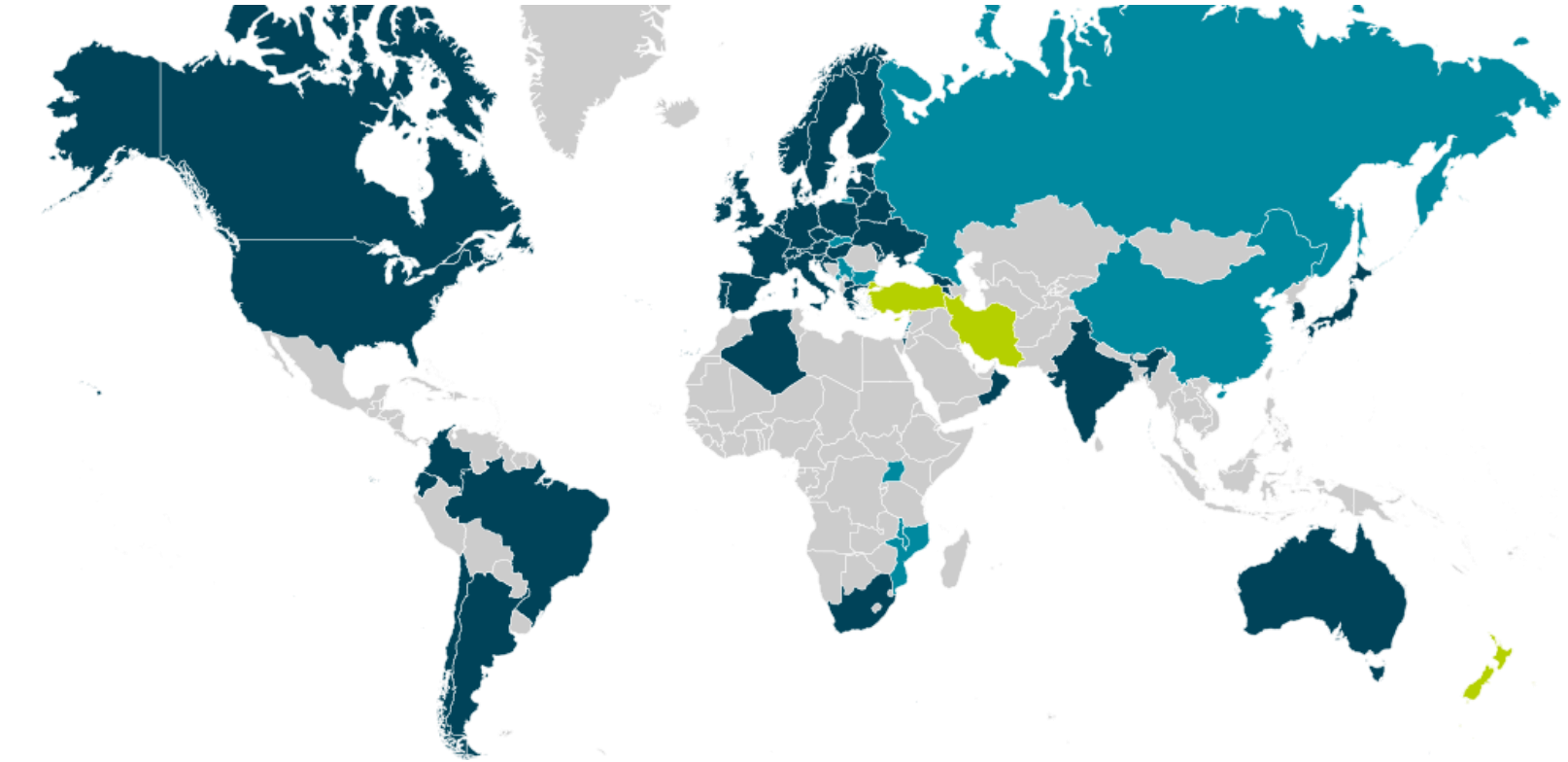
Tramite servizi di inter-federazione, permettono l'accesso ad analoghe federazioni di altre nazioni, ampliando di molto il numero di utenti e di servizi disponibili



# La Federazione Nazionale di Identità IDEM

- IDEM (www.idem.garr.it) è la Federazione Nazionale di Identità per l'istruzione e la ricerca
  - ✓ Permette il Single Sign On degli utenti su servizi federati (soprattutto web, ma non solo web)
  - ✓ Consente di condividere Servizi ed Utenti in un contesto federato di reciproca fiducia
  - ✓ Si basa su standard aperti e condivisi (SAML)
- Fa parte dell'inter-federazione **mondiale eduGAIN** (59 federazioni)
- Attualmente (Febbraio 2019) gestisce:
  - ❑ 97 Identity Providers
  - ❑ 119 Service Providers
  - ❑ 1 Attribute Authority

# La Federazione Nazionale di Identità IDEM




**eduGAIN** nel mondo:2993 IdPs,2352 SPs,4 AAs (Febbraio 2019)

# Servizio IdP in the Cloud

Il progetto prevede la disponibilità del servizio *IdP in the Cloud*

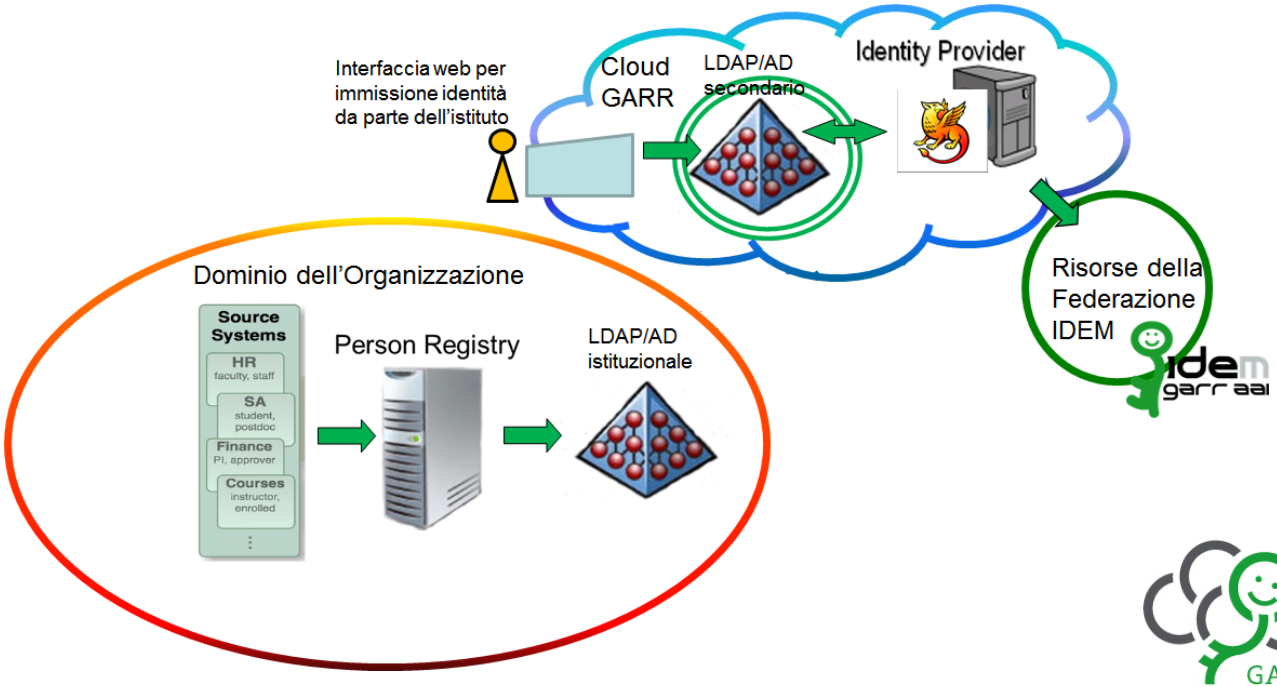
Istituti coinvolti:

- Istituti di Ricovero e Cura a Carattere Scientifico (**IRCCS**)
- Istituti Zooprofilattici Sperimentale (**IZS**)
- Direzione Generale della Ricerca e dell'Innovazione in Sanità (**Workflow Ricerca**)

Per ciascuno istituto è prevista l'attivazione del servizio

Gli IdP in the Cloud attualmente in produzione sulla GARR Cloud sono 26 (Febbraio 2019)

# Identity Provider = identità digitale senza confini




IDP IN THE cloud
GARR

- un Identity Provider con IDM dedicato e residente nella cloud GARR
- soluzione chiavi in mano e pronta all'uso da parte dell'organizzazione
- garantisce la sicurezza del processo di autenticazione anche da dispositivi mobili e all'esterno dell'istituto.

# Punti di forza di GARR come Cloud IdP provider

- GARR gestirà l'istanza IDP in maniera conforme alle norme EU GDPR
- GARR ospiterà l'istanza sulla sua infrastruttura Cloud
- Sicura
- Monitorata
- GARR ha il controllo completo dello stack
- Rete
- Cloud
- Applicativo
- Gli operatori di Federazione IDEM (IDEM Fed Ops) ed il personale GARR CSD (Cloud Ops) opereranno in completa e costante sinergia
- Avendo il controllo completo dello stack cloud e di quello applicativo (Shibboleth, MySQL, Web)
- Integrando gli strumenti di monitoring Cloud a quelli IDEM
- GARR popolerà ogni istanza con gli utenti forniti dall'Anagrafica dei Ricercatori del Workflow della Ricerca

# Architettura di IdP in the cloud

Dati tecnici

- Servizio in cloud
- Deployment automatizzato (ansible)
- Procedure di backup e restore automatizzate
- Sistema operativo: Debian Linux 9
- Identity Provider: Shibboleth 3.3.x
- Interfacce multilingua
- HTTPS e STARTTLS per LDAP
- Sistema di gestione delle identità (IDM) di facile utilizzo
- Sistema di statistiche sugli accessi
- Blocco/Sblocco utenze

Privacy

- Privacy policy:
- contitolarità del trattamento dei dati
- scopo del trattamento dei dati
- dati personali trasmessi solo con il consenso e solo per per gli scopi espliciti del servizio
- Raccolta log solo per funzionamento e sicurezza del servizio
- Log rimossi dopo un mese dalla raccolta

# IdP in the cloud

Il servizio IdP in the Cloud è un servizio di Identity Provider "as a Service", in cloud con IdM (Identity Management) collegato a una o più federazioni di identità (IDEM & eduGAIN)

| **Requisiti di Progettazione** | **Vantaggi conseguiti** |
|---|---|
| Semplicità di utilizzo | Semplici interfacce utente |
| Conformità ai più comuni standard di sicurezza e riservatezza dei dati | Manutenuto (Aggiornamenti e standard di sicurezza) |
| Interoperabilità con le risorse federate interne e/o esterne all'istituzione | Affidabile (backup, disaster recovery e monitoraggio) |
| Accessibilità ovunque in quanto erogato su una cloud | Non richiede risorse dedicate all'interno dell'istituto |
| Interconnessione alla Federazione IDEM e all'interfederazione eduGAIN per usufruire di migliaia di risorse web. | Universale (accesso da ogni dispositivo: PC, smartphone, tablet) |

# Il ciclo di vita delle identità digitali

Operazioni richieste al **Referente Tecnico** dell'IdP:

- ✓ Identificazione dell'utente
- ✓ Creazione dell'identità digitale (se non proveniente dal Workflow)
- ✓ Consegna username utente: nome.cognome
- ✓ Assegnamento dell'autorizzazione alle risorse: inserimento di valori specifici per gli attributi necessari alle risorse federate
- ✓ Aggiornamento dei dati dei profili utente
- ✓ Gestione recupero password (in casi straordinari: no password, no email)
- ✓ Disabilitazione/Terminazione dell'utente

La gestione interna all'IRCCS permette di gestire il ciclo di vita delle identità in modo ottimale, con informazioni aggiornate in tempo reale relativamente allo status di tutti gli attori coinvolti: ricercatori, medici, personale a supporto dell'attività di ricerca

# Cosa farà GARR durante le attivazioni degli IdP (1/2)

- chiederà ai referenti tecnici degli istituti di fornire informazioni istituzionali utili per personalizzare IdP (logo istituzione, colore, dominio, etc)
- fornirà supporto nella procedura di adesione alla Federazione IDEM e eduGAIN con il proprio IdP-in-the-Cloud.
- pubblicherà la documentazione relativa al servizio sul wiki di federazione
- preparerà i certificati server per SSL per gli IdP
- si occuperà della corretta registrazione in DNS delle istanze

# Cosa farà GARR durante le attivazioni degli IdP (2/2)

- preparerà gli script (**playbook Ansible**) per l'installazione e la configurazione automatizzate in 3 fasi
  - **Ansible Openstack** (creando la VM per l'IdP sulla Cloud GARR)
  - **Ansible Monitoring** (per configurare il monitoring associato alla VM)
  - **Ansible Shibboleth** (per installare e configurare l'IdP)
- Installerà e configurerà l'IdP, lo collauderà e lo registrerà in federazione IDEM di test con un utente di test a garanzia del suo corretto funzionamento
- Dopo un collaudo definitivo, lo registrerà nella Federazione di Produzione IDEM e nell'interfederazione eduGAIN

# Attivazione degli account utente

Ogni UTENTE accede autonomamente al SISTEMA di registrazione (FLUP):

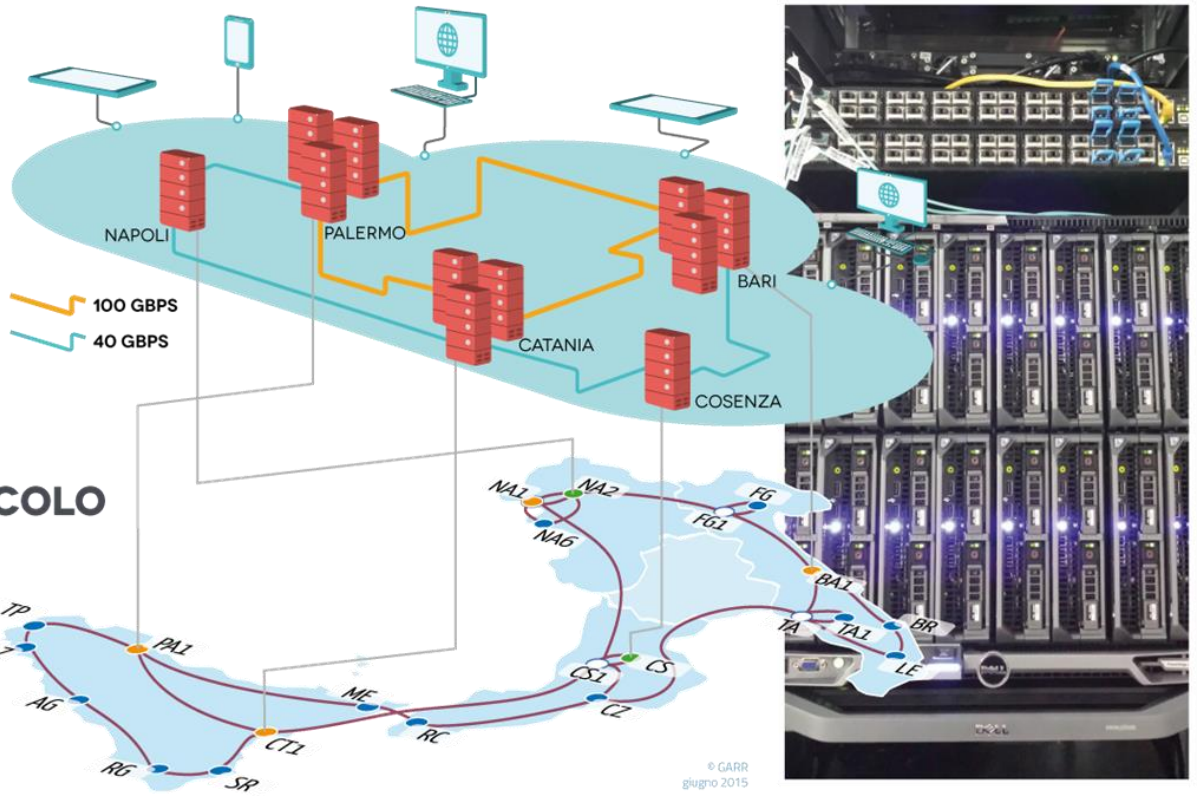
- inserisce il proprio **codice fiscale**
- inserisce la email personale
- il sistema invia un messaggio alla **email** inserita con la url per impostare la password
- l'UTENTE segue la **url**, imposta la **password** e attiva il suo **account**

# Cosa farà GARR durante la gestione dell'IdP

- Il personale GARR CSD collaborerà direttamente con gli operatori di federazione (IDEM Fed Ops) per monitorare lo stato di salute della macchina virtuale dedicata all'IdP

- Gli aspetti che verranno costantemente monitorati sono i seguenti:
  - ✓ Test funzionali periodici dell'IdP
  - ✓ Monitoring completo dell'istanza attraverso Check_MK(Nagios) monitoring
  - ✓ Monitoring interno all'infrastruttura Cloud GARR sulla VM e sullo storage

# L'infrastruttura Cloud del dipartimento CSD GARR




## INFRASTRUTTURA DI CALCOLO E STORAGE DISTRIBUITO

- 5 siti distribuiti
- 8.448 virtual CPU
- 10 PB spazio storage

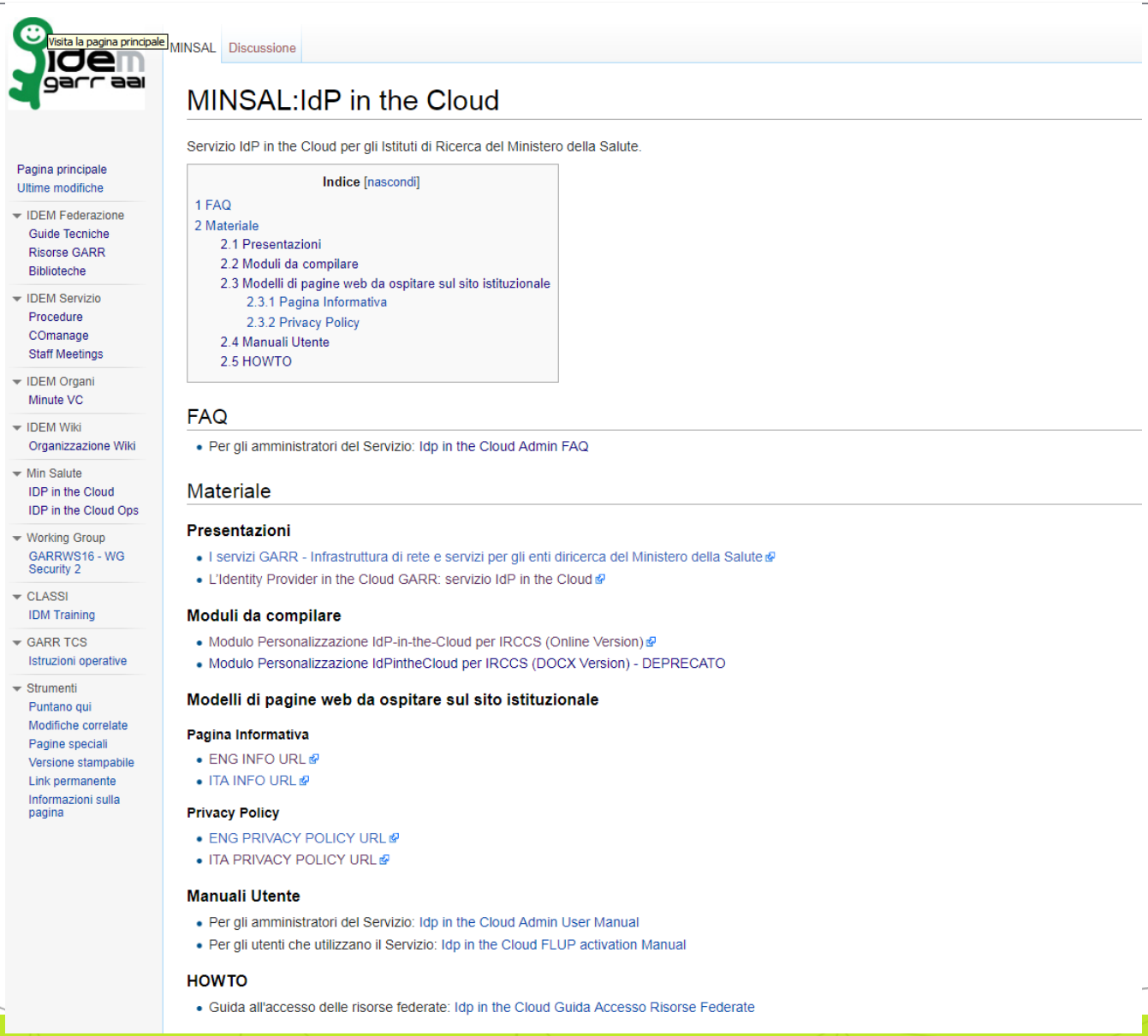
# La Cloud Federata GARR

- GARR offre alla sua comunità utenti accesso ed integrazione risorse sulla sua Cloud federata basata su standard open source
  - ❑ OpenStack - per l'implementazione della Cloud
  - ❑ Canonical Juju + MaaS per l'automazione del deployment

- Gli utenti possono accedere attraverso le loro credenziali
  - ❑ IDEM (SAML)
  - ❑ eduGAIN (SAML)
  - ❑ OpenIDConnect (Google Login)
  - ❑ Keystone local

- La Cloud GARR è accessibile a partire da https://cloud.garr.it
- La dashboard è disponibile su https://dashboard.cloud.garr.it

# Documentazione
# (https://wiki.idem.garrservices.it/wiki/index.php/MINSAL:IdP_in_the_Cloud)



Visita la pagina principale

MINSAL | Discussione

## MINSAL:IdP in the Cloud

Servizio IdP in the Cloud per gli Istituti di Ricerca del Ministero della Salute.

**Indice** [nascondi]

1 FAQ
2 Materiale
2.1 Presentazioni
2.2 Moduli da compilare
2.3 Modelli di pagine web da ospitare sul sito istituzionale
2.3.1 Pagina Informativa
2.3.2 Privacy Policy
2.4 Manuali Utente
2.5 HOWTO

### FAQ

- Per gli amministratori del Servizio: Idp in the Cloud Admin FAQ

### Materiale

**Presentazioni**

- I servizi GARR - Infrastruttura di rete e servizi per gli enti diricerca del Ministero della Salute
- L'Identity Provider in the Cloud GARR: servizio IdP in the Cloud

**Moduli da compilare**

- Modulo Personalizzazione IdP-in-the-Cloud per IRCCS (Online Version)
- Modulo Personalizzazione IdPintheCloud per IRCCS (DOCX Version) - DEPRECATO

**Modelli di pagine web da ospitare sul sito istituzionale**

**Pagina Informativa**

- ENG INFO URL
- ITA INFO URL

**Privacy Policy**

- ENG PRIVACY POLICY URL
- ITA PRIVACY POLICY URL

**Manuali Utente**

- Per gli amministratori del Servizio: Idp in the Cloud Admin User Manual
- Per gli utenti che utilizzano il Servizio: Idp in the Cloud FLUP activation Manual

**HOWTO**

- Guida all'accesso delle risorse federate: Idp in the Cloud Guida Accesso Risorse Federate

Pagina principale
Ultime modifiche
IDEM Federazione
Guide Tecniche
Risorse GARR
Biblioteche
IDEM Servizio
Procedure
COmanage
Staff Meetings
IDEM Organi
Minute VC
IDEM Wiki
Organizzazione Wiki
Min Salute
IDP in the Cloud
IDP in the Cloud Ops
Working Group
GARRWS16 - WG Security 2
CLASSI
IDM Training
GARR TCS
Istruzioni operative
Strumenti
Puntano qui
Modifiche correlate
Pagine speciali
Versione stampabile
Link permanente
Informazioni sulla pagina

# Domande?