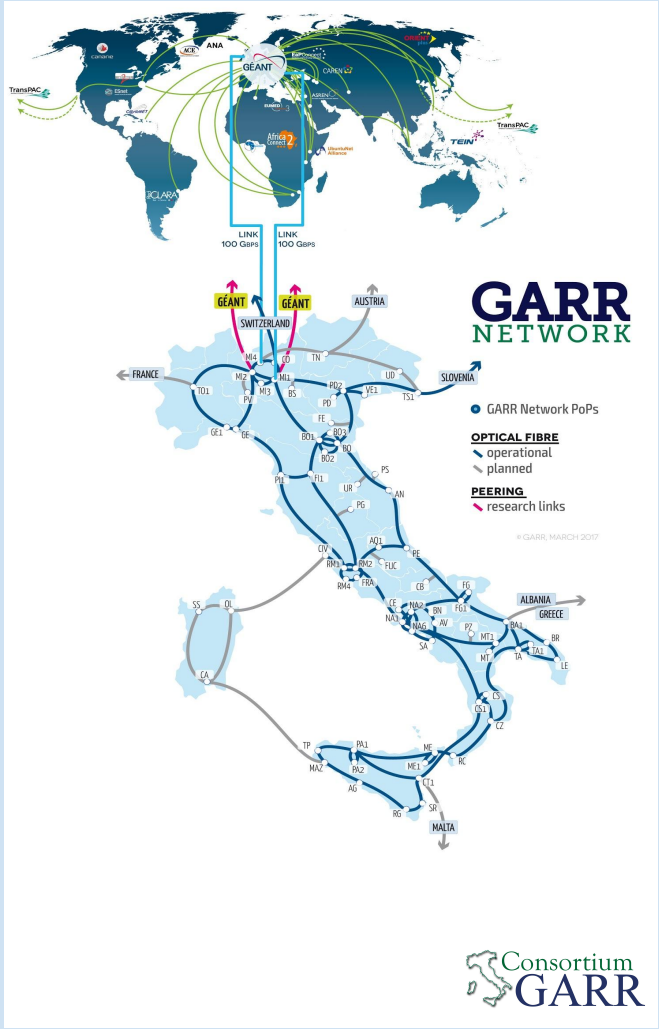
L’Identity Provider in the Cloud
GARR: servizio IdP in the Cloud

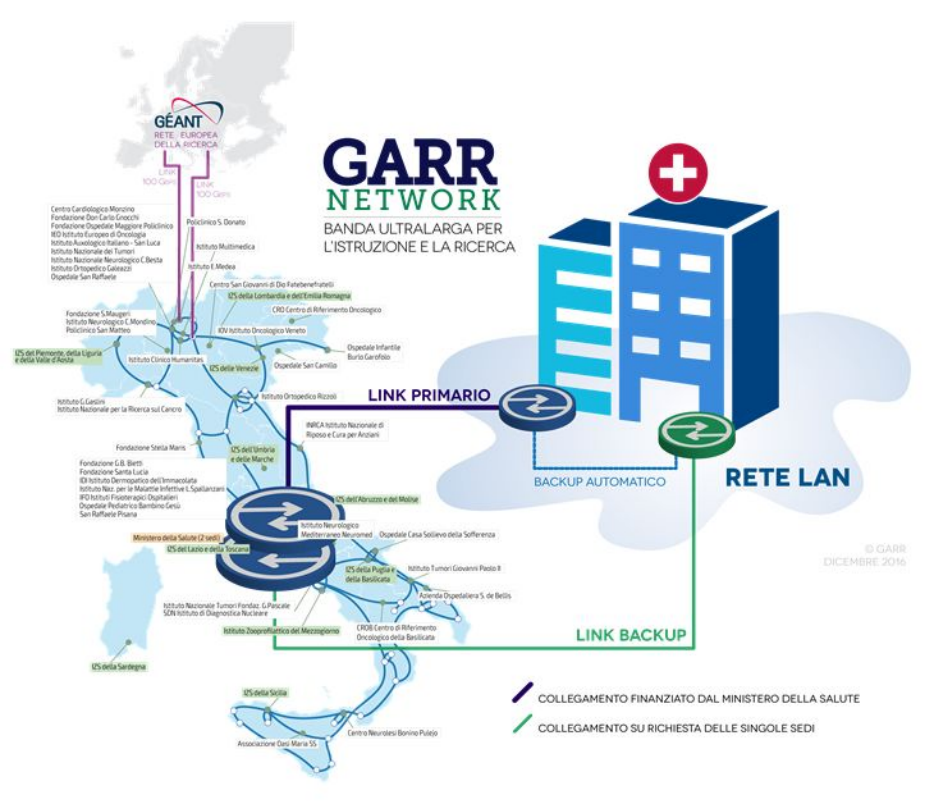
Webinar per gli IRCCS dedicato al servizio GARR Identity Provider in the Cloud

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



Distribuzione nazionale degli istituti del Ministero della Salute



Infrastruttura è caratterizzata da:

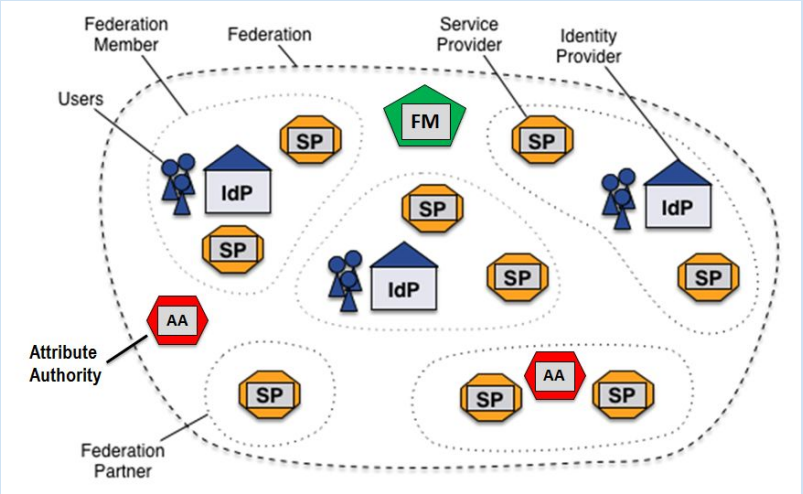
- un **circuito di accesso** di ampia capacità di banda
- **un apparato (tipo router)** utile per l'attestazione del collegamento di accesso primario

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

IdP 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 **interfederazione,** permettono l'accesso ad analoghe federazioni di altre nazioni, ampliando di molto il numero di utenti e di servizi disponibili

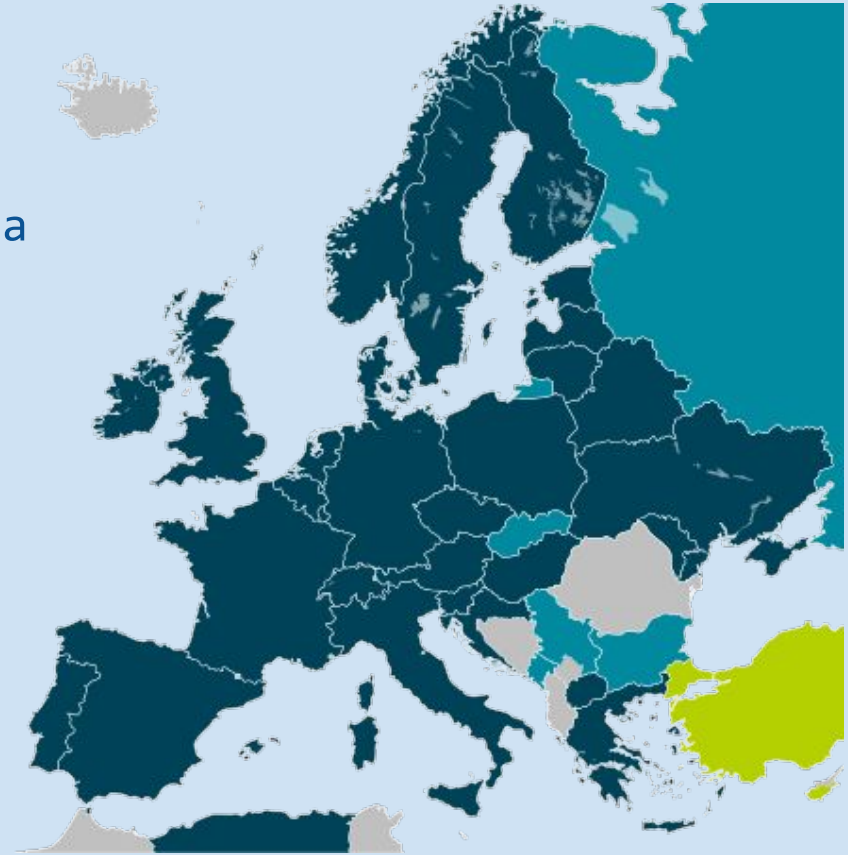


La Federazione Nazionale di Identità IDEM

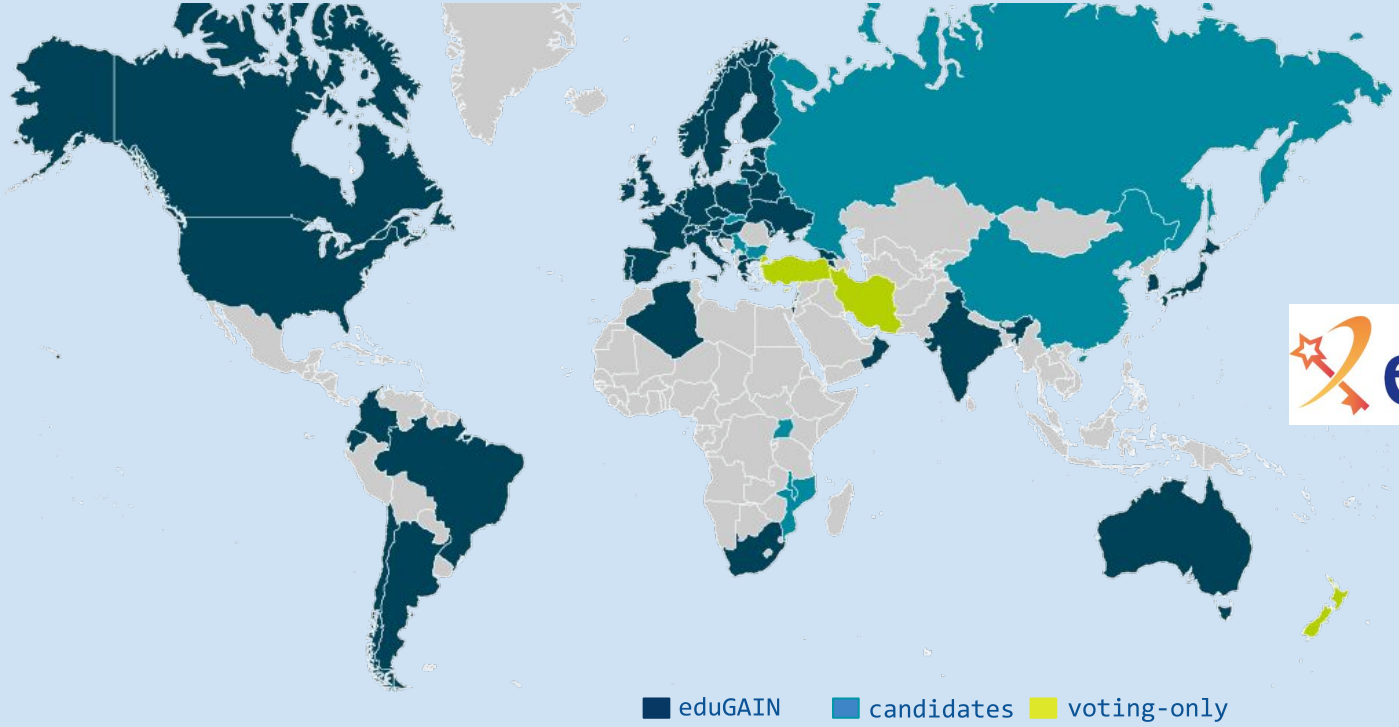
- IDEM (www.idem.garr.it) è la Federazione Nazionale di Identità per l'istruzione e la ricerca
  - Permette il **Single Sign On** degli utenti su servizi federati (soprattutto web, ma non solo web)
  - Consente di condividere Servizi ed Utenti in un contesto federato di reciproca fiducia
  - Si basa su standard aperti e condivisi (soprattutto SAML)
- Fa parte dell'inter-federazione **mondiale eduGAIN (56 federazioni)**
- Attualmente (Ottobre 2018) gestisce
  - 96 Identity Providers
  - 119 Service Providers
  - 1 Attribute Authority

La Federazione Nazionale di Identità IDEM

eduGAIN in Europa



La Federazione Nazionale di Identità IDEM



eduGAIN nel mondo:2897 IdPs,2207 SPs,5 AAs (Ottobre 2018)

Servizio per il Ministero della Salute

Ministero della Salute ha promosso con GARR una sperimentazione che ha permesso di dare il via al servizio ***IdP in the Cloud***

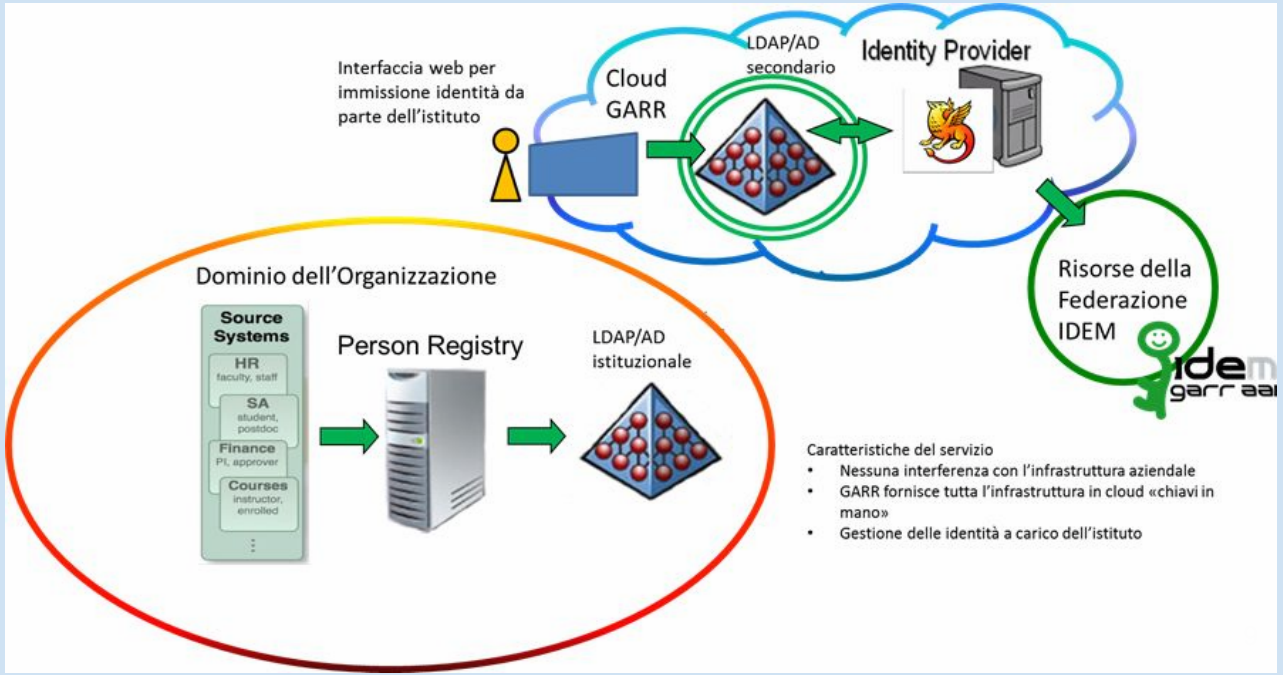
Istituti coinvolti:

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

Per ciascuno di questi istituti è prevista l'attivazione del servizio ***IdP in the Cloud***
Gli *IdP in the Cloud* attualmente in produzione sulla GARR Cloud sono 27 (Ottobre 2018)

Identity Provider = identità digitale senza confini

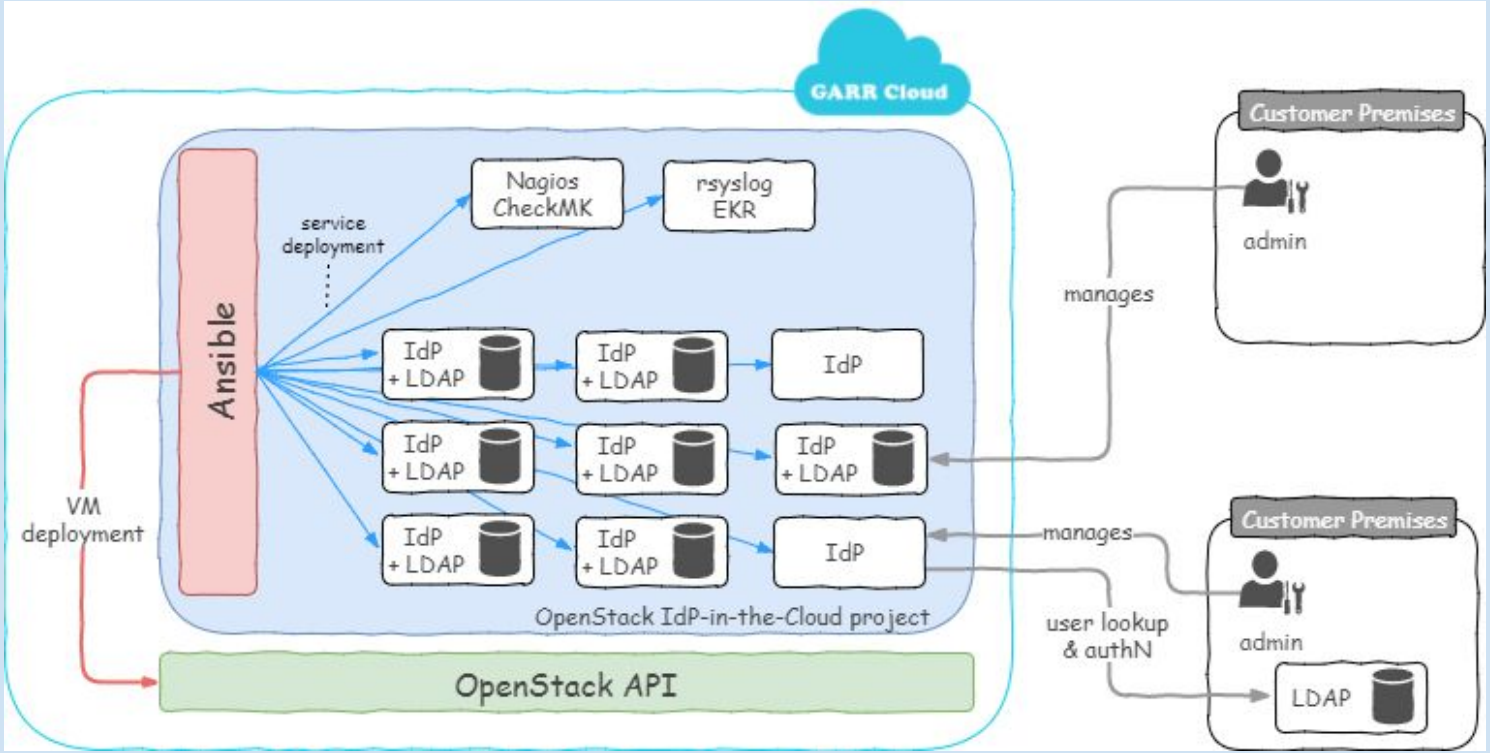
- un Identity **Provider dedicato** e residente nella cloud GARR
- soluzione *chiavi in mano* e pronta all'uso da parte dell'organizzazione
- garantisce la sicurezza del processo di autenticazione anche da dispositivi mobili e su applicazioni esterne



Punti di forza di GARR come Cloud IdP provider

- GARR gestirà l'istanza IDP in maniera conforme alle norme EU GDPR
- GARR implementerà 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

Architettura *IdP in the Cloud*



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
- *Opzionale*: LDAP Interno con gestione password
- *Opzionale*: Sistema di gestione delle identità

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 anonimizzati 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 o senza un servizio di Directory integrato), collegato a una o più federazioni di identità (IDEM & eduGAIN).

Requisiti di Progettazione	**Vantaggi conseguiti**
• Semplicità di utilizzo	• Semplice interfaccia utente
• Conformità ai più comuni standard di sicurezza e riservatezza dei dati	• Sicuro (manutenzione ed aggiornamenti)
• Interoperabilità con le risorse federate interne e/o esterne all’istituzione	• Affidabile (backup e disaster recovery)
• Accessibilità ovunque in quanto erogato su una cloud	• Monitorato, Non necessita di deployment locale
• Interconnessione alla Federazione IDEM e all’interfederazione eduGAIN per usufruire di migliaia di risorse web.	• Universale (accesso da ogni device: PC, smartphone, tablet)

Il ciclo di vita delle identità digitali

Operazioni principali:

- Identificazione dell'utente
- Creazione dell'identità digitale
- Assegnazione delle credenziali di autenticazione
- Assegnazione delle autorizzazioni
- Aggiornamento dei dati dei profili utente
- Gestione recupero password
- 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, tecnici specialistici.

Cosa farà GARR durante le attivazioni degli IdP (1/2)
Aspetti Logistico-Amministrativi

- Ha chiesto agli admin degli IdP Cloud degli enti di fornire informazioni sull' IdP (logo istituzione, etc)
- Ha inviato documenti per la richiesta di adesione ad IDEM e la pubblicazione dell'IdP in Federazione
- Registrerá l'IdP nella federazione di test **IDEM TEST**
- Invierà ai referenti amministrativi degli IdP una specifica versione del Documento Descrittivo del processo di Accreditamento degli Utenti della Federazione, affinché sia sottoscritto
- Dopo un collaudo definitivo, lo **registrerà in Federazione IDEM**
  - Rendendolo parte dell'**interfederazione eduGAIN**
- Formerà l' admin del IdP di IRCCS sulle operazioni di gestione IdP ed utenti

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

- Preparerà i certificati server per SSL per gli IdP
- Si occuperà della corretta registrazione in DNS delle istanze
- Preparerà gli scripts (**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 dell' IRCCS)
- Installerà e configurerà l' IdP, lo collauderà e lo registrerà nella federazione di test con delle utenze GARR di test
- Dopo un collaudo definitivo, lo **registrerà in Federazione IDEM**
  - Rendendolo parte dell'**interfederazione eduGAIN**
- Formerà l' admin del IdP di IRCCS sulle operazioni di gestione IdP ed utenti

Attivazione degli account utente

Ogni UTENTE accede autonomamente al SISTEMA di registrazione:

- inserisce il proprio CODICE_FISCALE
- inserisce la email personale
- il SISTEMA invia un messaggio alla email inserita con url per impostare la password
- l'UTENTE segue la url, imposta la password e attiva l'account

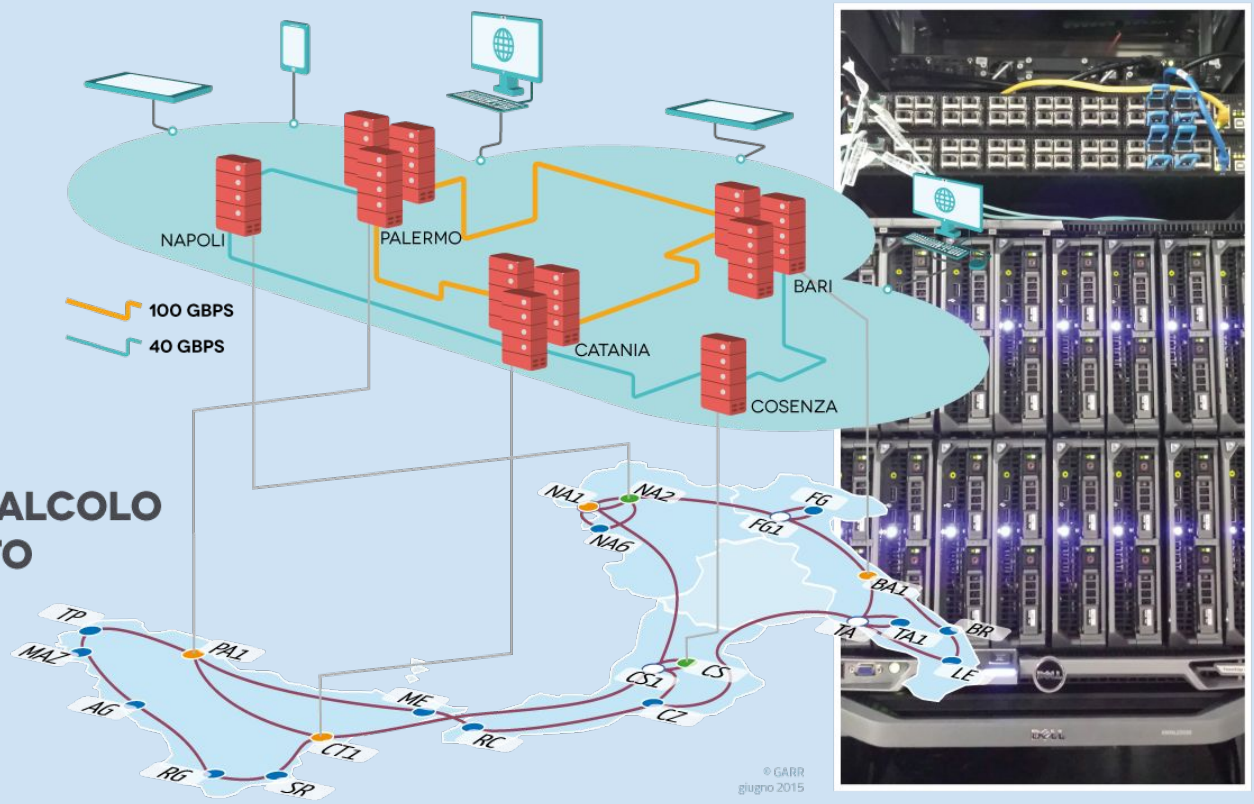
Cosa farà GARR durante la gestione dell’ IdP

- Il personale GARR CSD collaborerà direttamente con gli operatori di federazione (IDEM Fed Ops) per monitorare lo stato di salute dell’ istanza IdP
- Gli aspetti che verranno costantemente monitorati sono i seguenti
  - **Test funzionali** periodici dell’ IdP
  - **Monitoring completo dell'istanza** attraverso Check_MK monitoring
  - **Monitoring interno all’ infrastruttura Cloud GARR** sulla VM e sullo storage

Cosa farà l’IRCCS IdP Admin durante le attivazioni

- Fornirà preliminarmente a GARR le informazioni necessarie all'installazione e alla configurazione (favicon e logo, Identity management base DN…) dell’IdP.
- Parteciperà ai Webinar formativi per comprendere procedure e strumento(IdP) ottenuto
- Gestirà gli utenti con l’interfaccia di amministrazione di IdP (phpLDAPadmin) e monitorerà le sue statistiche.

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

Conclusioni

- *IdP in the Cloud* è una soluzione che risponde ai requisiti di semplicità di provisioning ed utilizzo di molte istituzioni, inclusi gli IRCCS
- GARR ha progettato e realizzato una soluzione scalabile e gestibile e l'ha sperimentata con il Ministero della Salute
  - E si appresta adesso all'implementazione della nuova fase di deployment
- Il progetto con il Ministero della Salute si è trasformato in un Servizio offerto da GARR
- Nei prossimi giorni collaborando con voi passeremo alla fase di installazione e configurazione

Riferimenti Bibliografici

- IDEM - IDP IN THE CLOUD: https://www.idem.garr.it/casi-duso/idp-in-the-cloud

- FARINA F., BIANCINI A., MANTOVANI M.L., MALAVOLTI M., MANDATO P., VALLI C., PRETE L., TOMASSINI S. (2014), IDP IN THE CLOUD: IDENTITY MANAGEMENT AS A SERVICE AT GARR, TNC 2014, DUBLINO, 19-22 MAGGIO 2014, https://tnc2014.terena.org/core/presentation/31

- MANTOVANI M.L. (2015), GESTIONE FEDERATA DELL'IDENTITÀ DALL'UNIVERSITÀ ALLA SCUOLA DIGITALE E ACCESSO UNICO A RISORSE E SERVIZI, TEACH DIFFERENT! PROCEEDING DELLA MULTICONFERENZA EMEMITALIA2015, GENOVA, 9-11 SETTEMBRE 2015, GENOVA UNIVERSITY PRESS, ISBN: 978-88-97752-60-8, p. 151-154, http://www.ememitalia.org/phocadownload/Atti_EMEM2015.pdf

- MALAVOLTI M.,MANTOVANI M.L. (2015), BYOD - QUANTE RISORSE CON UN'UNICA PASSWORD - IDEM DAY 2015: http://www.garr.tv/hwdvideos/uploads/v3thk4mmcwqja0.mp4

- REALE M. (2017) - "SUPPORTING THE PROVISIONING OF CAMPUS IDPS " REFEDS 34 https://goo.gl/R6fNE5

GRAZIE

Domande ?