Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Una nuova architettura per IdP in the Cloud: da Puppet ad Ansible sulla Cloud GARR Federata

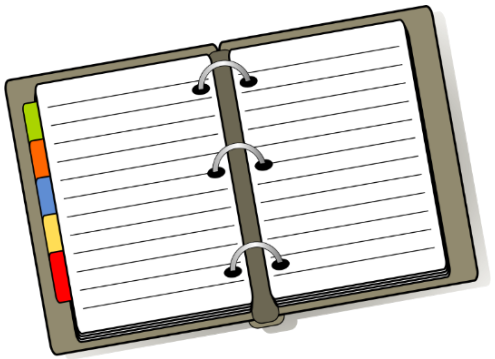
MARCO MALAVOLTI

Roma, 30 Maggio 2018

Workshop GARR 2018 - #wsgarr

Agenda

1. Introduzione
2. Confronto Puppet VS Ansible per IdP-in-the Cloud
3. Architettura IdP-in-the-Cloud (Ansible version)
4. Cosa riusciamo a fare oggi con Ansible
5. Bello! Posso riuscirci anche io?
6. Risultati ottenuti
7. Conclusioni



Alzi la mano chi sa cos'è un Identity Provider (IdP) e lo ha installato

Perché è importante avere un Identity Provider?

Avere un Identity Provider è importante per:

1. **Centralizzare**:
   la gestione delle identità digitali nella tua organizzazione
2. **Controllare:**
   il rilascio degli attributi utente verso le risorse (esterne/interne)
3. **Interagire:**
   con realtà federate come IDEM ed eduGAIN

IMPORTANTE !

IdP in the Cloud – Perché (La parola agli utenti)

Massimo Del Sarto (IRCCS Fondazione Stella Maris) :

L'adesione alla Federazione IDEM si è resa necessaria al fine di facilitare la fruizione dei servizi messi a disposizione dal Ministero della Salute e dagli altri enti aderenti ad IDEM. Fin dall'inizio l'IRCCS Stella Maris è stato molto interessato al progetto IDEM, ma problematiche di risorse interne non ci avevano consentito di aderire. Finalmente con il nuovo progetto IdP in the Cloud siamo riusciti in tempi molto brevi ad implementare il servizio di IdP.

IDEM facilita il lavoro dei nostri ricercatori, per esempio consentendo loro l'accesso ai servizi bibliografici (Nilde, riviste online, etc) e al workflow della ricerca, ma anche l'accesso a servizi più generali come le reti WiFi. Così il nostro IRCCS potrà semplificare la gestione dell'accesso dei ricercatori ospiti alla rete WiFi. Inoltre, pur essendo le collaborazioni di ricerca internazionali in numero minore rispetto alle nazionali, negli ultimi anni sono cresciute di numero e importanza, in questo caso l'adesione a eduGAIN rappresenta un grande valore aggiunto.

Il maggior lavoro è stato nell'aggiornare le procedure e le policy interne per renderle conformi a quanto richiesto dalla Federazione, mentre i piccoli problemi tecnici sono stati velocemente risolti.

IdP-in-the-Cloud: Da Puppet ad Ansible

PUPPET(2013-2016)	ANSIBLE(2017-2018)
Ruby	**Python**
Flusso di esecuzione governata dai **metaparametri** (before, after, subscribe, notify)	Flusso di esecuzione **Top-Down**: Così come lo leggi
Rischio cicli bloccanti **elevati**	Rischio cicli bloccanti **nullo** (per ora)
Linguaggio dichiarativo proprio	**YAML**
Software richiesto: Client: **puppet-agent** Server: **puppetserver**	Software richiesto: Client: **Python** Server: **Ansible**
Template: Embedded Ruby (**ERB**)	Template: **Python Jinja2**
I Puppet Agent devono essere approvati dalla **CA** del Puppet Server	Usa le **chiavi SSH**
Provisioning VM: **NO**	Provisioning VM: **SI**

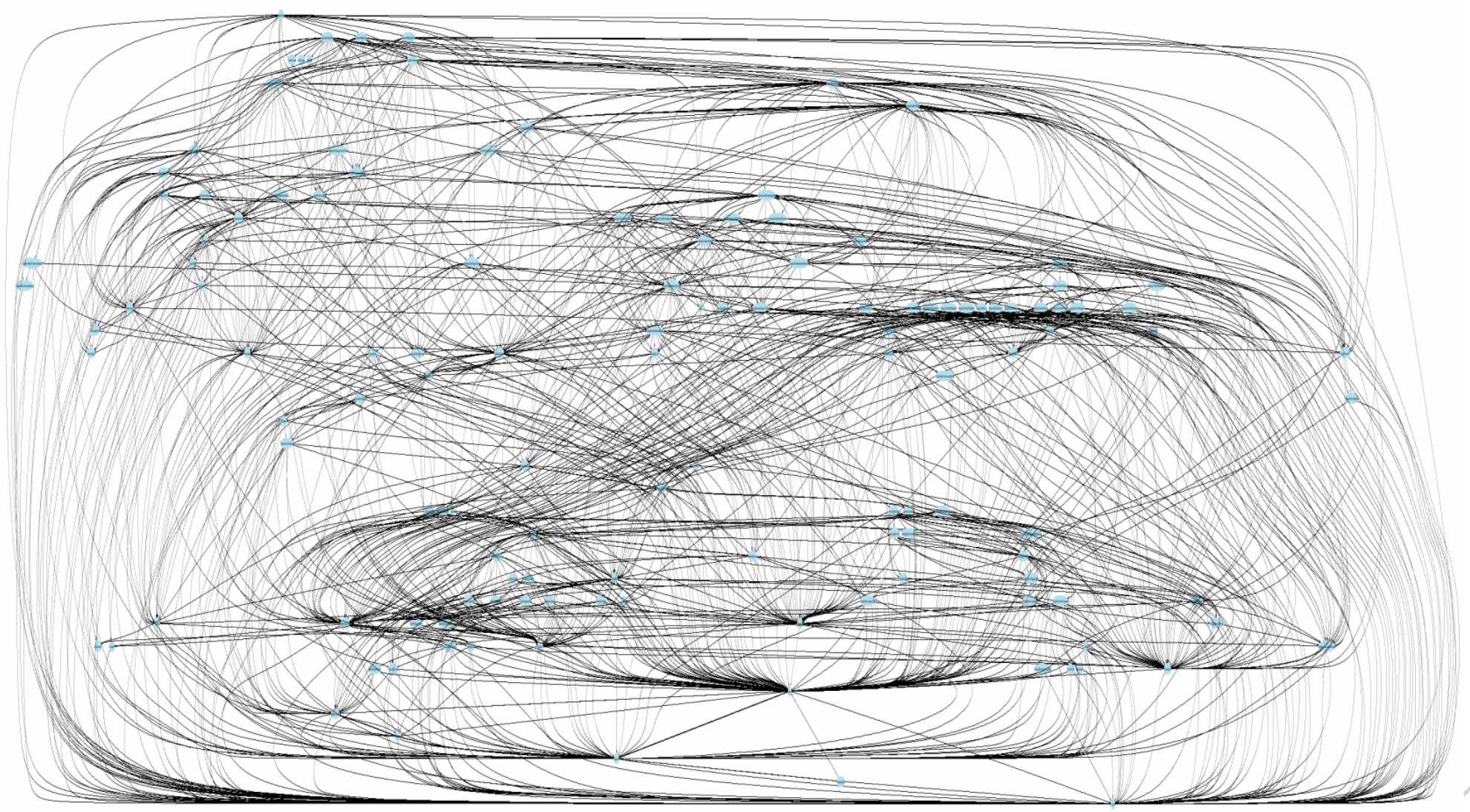
Storia di vita vissuta…

Error:
Could not apply complete catalog: Found 1 dependency cycle:

```
(Exec[pip install requirements] =>
File[change venv permissions] =>
File[enforce MinGW compiler]
=> Exec[pip install requirements])
```

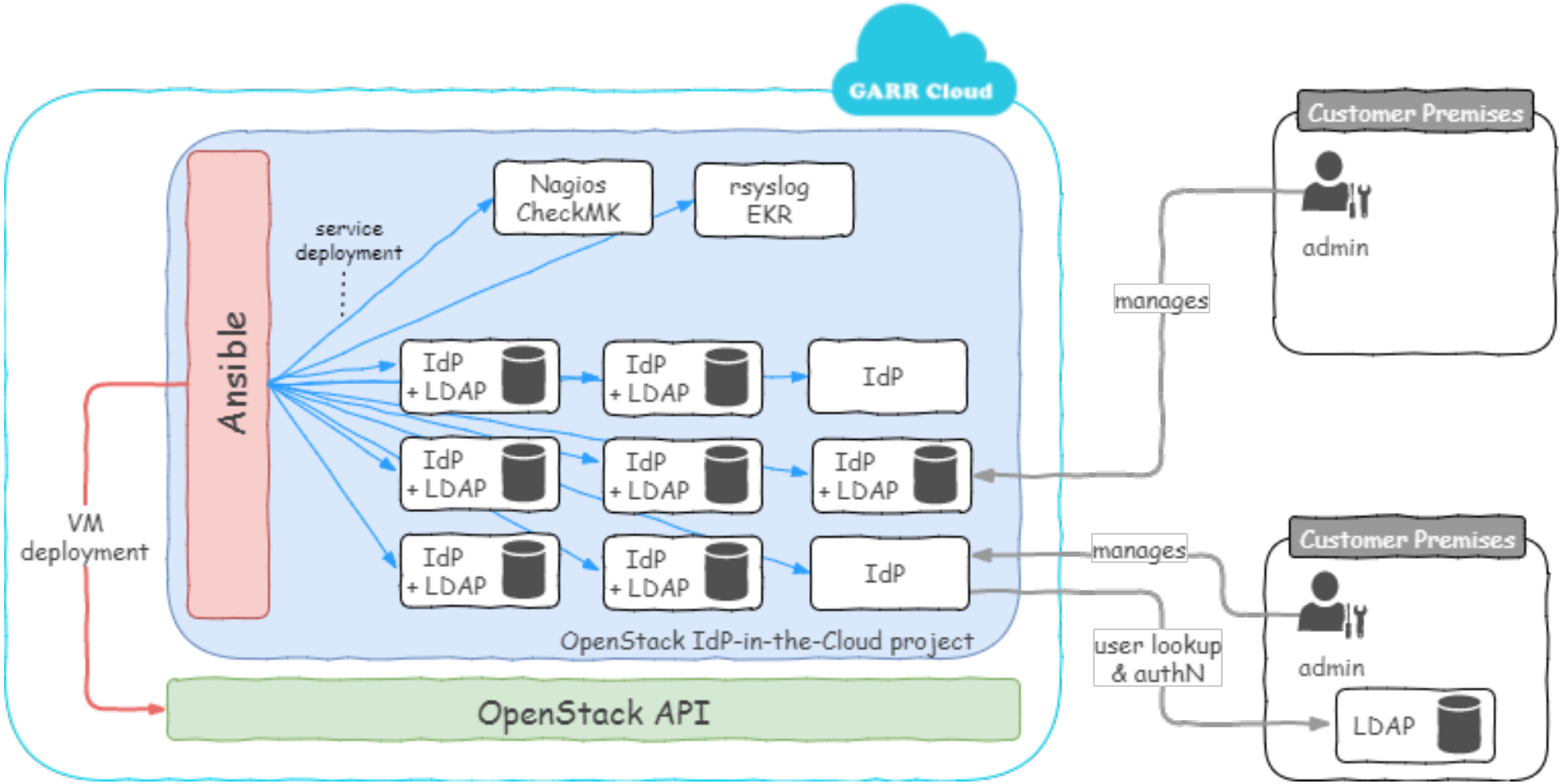
```
Try the '--graph' option and opening the resulting '.dot'
file in OmniGraffle or GraphViz
```

Storia di vita vissuta…



Dependency diagram (Geek Sublime, pg 111)

Architettura IdP-in-the-Cloud



Cosa riusciamo a fare con Ansible

1. Creare/Distruggere **macchine virtuali** sulla Cloud GARR (API)
2. Creare e collegare più nodi **elasticsearch** tra loro per collezionare ed elaborare i logs degli IdP
3. Creare un nodo **kibana** per la visualizzazione grafica dei logs collezionati
4. Installare/Configurare il servizio di monitoraggio **Check_MK**

Cosa riusciamo a fare con Ansible

5. Creare Identity Provider **Shibboleth** (<10 min):
   1. **Conformi** a IDEM e ad eduGAIN (non solo)
   2. **Multilingua**
   3. Orientati ai dispositivi mobili: **responsivi**
   4. Inclini a più comuni standard di sicurezza (**SSLLabs – A+**)
   5. Dodati di **IdM** (Identity Management) proprio:
      1. Capace di **bloccare gli utenti** mediante bottone o una data prestabilita
      2. Facile da utilizzare con **phpLDAPadmin**
      3. Rispettoso delle misure minime di **sicurezza** sulle **password** (NIST SP 800-63-3)
   6. Muniti di app per la **gestione autonoma** dell'account da parte dell'utente (password & mail)
   7. In grado di raccogliere alcune **statistiche** di utilizzo dell'IdP
   8. **Aggiornati** e **aggiornabili** rapidamente
   9. Conforme alle **raccomandazioni** del Consortium Shibboleth (Jetty 9 – JDK open/ oracle)

Bello! Posso riuscirci anche io?

- **ansible-master.aai.garr.it**
  - ansible-openstack:
    Crea le macchine virtuali(VM) necessarie

  - ansible-monitoring:
    Configura l'ambiente di monitoraggio e di stoccaggio dei dati:
    - **elasticsearch[1…N].aai.garr.it** (ricevono i logs dagli IdP)
    - **kibana.aai.garr.it** (visualizza i logs raccolti sui server elasticsearch)
    - **checkmk.aai.garr.it** (monitora il funzionamento degli IdP)
    - **logs.aai.garr.it** (punto di stoccaggio dei logs degli IdP)
    - **data-backups.aai.garr.it** (punto di stoccaggio dei backup LDAP & MySQL DB)

  - ansible-shibboleth:
    Configura un Identity Provider Shibboleth v3.3.2 su Linux Debian 8
    - **idp-[1…N].irccs.garr.it** (our IdPs)

Risultati Raggiunti

1. Abbiamo sviluppato un servizio in grado di essere ripristinato rapidamente su di una nuova architettura dalle medesime caratteristiche

2. Abbiamo erogato più di 24 nuovi IdP-in-the-Cloud v3.3.2 conformi agli standard di IDEM e di eduGAIN.

3. Abbiamo ottenuto un ottimo grado di personalizzazione degli IdP installati (multilingua, colori, icone, pagine web, …)

4. Abbiamo velocizzato l'erogazione di un nuovo IdP ben formato.

5. Abbiamo semplificato l'adesione alla Federazione IDEM ed eduGAIN

Conclusioni

Ansible, e l'automazione, hanno permesso di:

1. Raggiungere un buon grado di successo: sviluppi 1 volta, ripeti per N.
2. Correggere velocemente gli errori su tutte le VM.
3. Generare una documentazione di base attraverso il codice.
4. Ripristinare il servizio da zero con rapidità e precisione.
5. Guadagnare tempo per nuovi sviluppi.

Ringraziamenti

- Fabio Farina (moderatore di questa sessione)
- Davide Vaghetti, Sabrina Tomassini, Laura Pirelli, Mario Reale e Lalla (IdP-in-the-Cloud Team)
- Barbara Monticini (IDEM GARR AAI)

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Grazie per l'ascolto!

Marco Malavolti – Servizio IDEM GARR AAI
marco.malavolti@garr.it