Introduzione alla sicurezza in INFN Cloud

Vincenzo Ciaschini
INFN CNAF

Sommario

- Regole di accesso
- AUP
- Terms of Use
- PaaS o IaaS
- Amministratore di Sistema
- Ownership
- Security Recommendations

Regole di accesso

- INFN Cloud e’ parte della rete INFN
  - Per accedere occorre rispettare tutte le regole di accesso alle risorse dell’INFN
  - E qualcuna in piu’.
  - Esse sono dettagliate in una AUP e nei Terms of Use
  - https://www.cloud.infn.it/policies-procedures

Regole di accesso/2

- Leggere e spiegare la totalita’ di AUP e Terms of Use richiederebbe da solo l’intera giornata
  - Ne verra’ mostrato un estratto
  - La lettura integrale e’ un “compito per casa.”

AUP

- Definisce chi puo’ accedere al servizio:
  - Dipendenti o associati INFN
  - Membri di progetti, contratti o convenzioni di cui e’ parte l’INFN
  - Identificati tramite INFN-AAI

AUP/2

- Ogni macchina ha un Amministratore di Servizio che ne e’ responsabile
  - Puo’ aggiungere altri utenti, ma dovranno venire registrati in INFN-AAI e dovra’ accettare AUP e Terms of Use
- Ogni macchina e’ soggetta a periodiche scansioni di sicurezza e ogni problema dovra’ venire risolto in fretta.

AUP/3

- Non ci sono garanzie sulla disponibilita’
- Per il supporto potra’ venire richiesto l’accesso alle machine
- L’INFN conserva i log dell’utilizzo di INFN-Cloud

Terms of Use

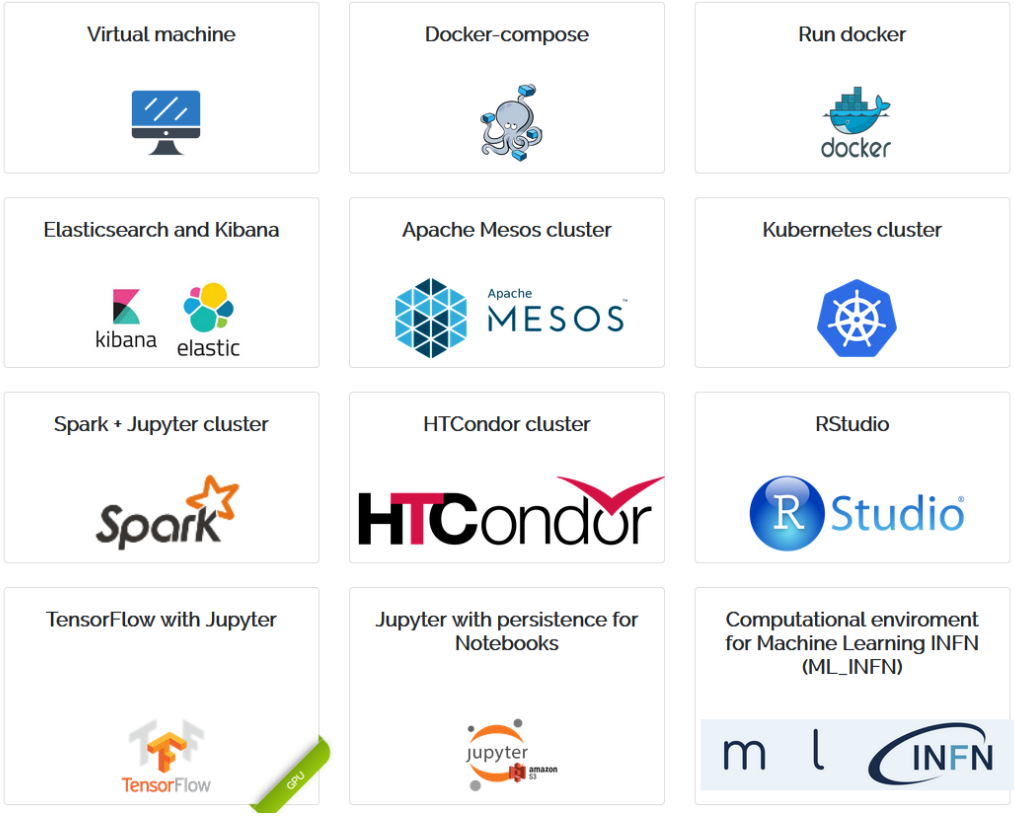
- Integrano per riferimento le AUP GARR, le AUP di INFN-Cloud ed il Disciplinare per l'utilizzo delle risorse infromatiche.
- Specificano che l'Amministratore di Sistema e' responsabile della macchin.
- Elencano utilizzi vietati
  - Attivita' commerciali, spamming, mining, etc...

Terms of Use/2

- Vincola l’amministratore di servizio ad usare le macchine solo per lo scopo per cui gli sono state assegnate.
- Garantisce all’INFN il diritto di sospendere il servizio o bloccarne l’utilizzo

PaaS o IaaS

- La INFN-Cloud ha come interfaccia principale la paas
  - https://paas.cloud.infn.it
- Ci sono svariati servizi gia' preconfigurati da far partire



PaaS o IaaS/2

- Ma INFN-Cloud e’ basata su OpenStack
  - E’ possible far partire vm “lisce” direttamente da OepnStack?
- Risposta breve: no
- Risposta lunga: si, ma…

PaaS o IaaS/3

- L’interfaccia di INFN-Cloud e’ la PaaS, ed e’ questa l’interfaccia che tutti devono usare.
- Si riconosce che per alcuni casi d’uso questa non e’ adeguata.
- Gli amministratori possono richiedere l’accesso diretto a OpenStack, ma esso verra’ concesso solo dietro approvazione del PMB di INFN-Cloud

Amministratore di Sistema

- L’Amministratore di Sistema e’ una persona nominata da un direttore per amministrare risorse informatiche
- Presuppone il possesso di tutte le conoscenze necessarie per amministrare una macchina
- E’ quindi in possesso delle credenziali amministrative
- E’ responsabile di quello che accade sulle risorse da lui amministrate

Amministratore di Sistema/2

- L’INFN richiede che ogni servizio abbia un (o piu’) Amministratore di Sistema che lo prenda in carico
- INFN-Cloud richiede che per far partire un servizio si debba necessariamente aver ricevuto la nomina ad Amministratore di Sistema
  - Altrimenti si e’ Utenti, ovvero si utilizzano servizi gestiti da altri

Come diventare Amministratori di Sistema

- Procedura (semi)automatica tramite il libro firma dell'INFN
  - https://librofirma.dsl.infn.it
- Seguire le istruzioni in:
  - https://www.cloud.infn.it/policies-procedures
- Aprire un ticket su ServiceDesk allegando il pdf firmato e rinominato secondo lo schema <CognomeNome>-<email>.pdf

Servizi su rete privata

- In corso di discussione con Harmony una procedura per permettere agli Utenti di far partire servizi
  - Che saranno pero’ su una rete parzialmente isolata, ovvero NON raggiungibile dall’esterno.

Ownership e Amministrazione di servizi

- Come detto sopra, ogni servizio DEVE avere un amministratore
- Un servizio senza amministratore non puo’ esistere e verra’ chiuso d’ufficio da INFN-Cloud

Ownership e Amministrazione di Servizi/2

- Cosa succede quando l'amministratore di servizio se ne va?
  - Cambia lavoro, passa ad un altro gruppo di lavoro od esperimento, va in pensione, etc…
  - Il servizio rimane senza amministratore
  - Dovrebbe essere chiuso
  - Ma se serve ancora?

Ownership e Amministrazione di servizi/3

- Se serve ancora, la soluzione migliore e' distruggerlo e farlo ripartire con un nuovo amministratore
  - L'istanza su OpenStack e' legata all'account che la ha fatta partire
- Ci rendiamo conto che non e' sempre praticabile
  - In questo caso si deve contattare il supporto utenti di INFN Cloud che cerchera' (ma senza offrire garanzie) strade alternative
- Rimane pero' il punto fisso: servizi senza amministratore non possono esistere

Security Recommendations

- Poter avere macchine virtuali a disposizione NON significa essere nel far west.
- Ci sono un set di raccomandazioni MINIMO che DEVE essere rispettato da ogni servizio implementato su INFN-Cloud e da ogni amministratore:
  - https://www.cloud.infn.it/policies-procedures/

Security Recommendations/2

- Esempi:
  - Mantenere sempre aggiornato il Sistema Operativo
  - Effettuare sempre autenticazione ed autorizzazione degli utenti
  - Non usare credenziali di default
  - Crittare tutte le comunicazioni

Security Recommendations/3

- Ma io non posso implementarla perche'...
- Le recommendation non sono facoltative.
  - Esse VANNO implementate
- Se proprio non si capisce come farlo, si deve contattare il WP4 di INFN-Cloud, che discutera' del problema e potra':
  - 1) suggerire una implementazione funzionante del requisito
  - 2) suggerire una implementazione alternativa che fornisca la stessa garanzia di sicurezza

Domande?