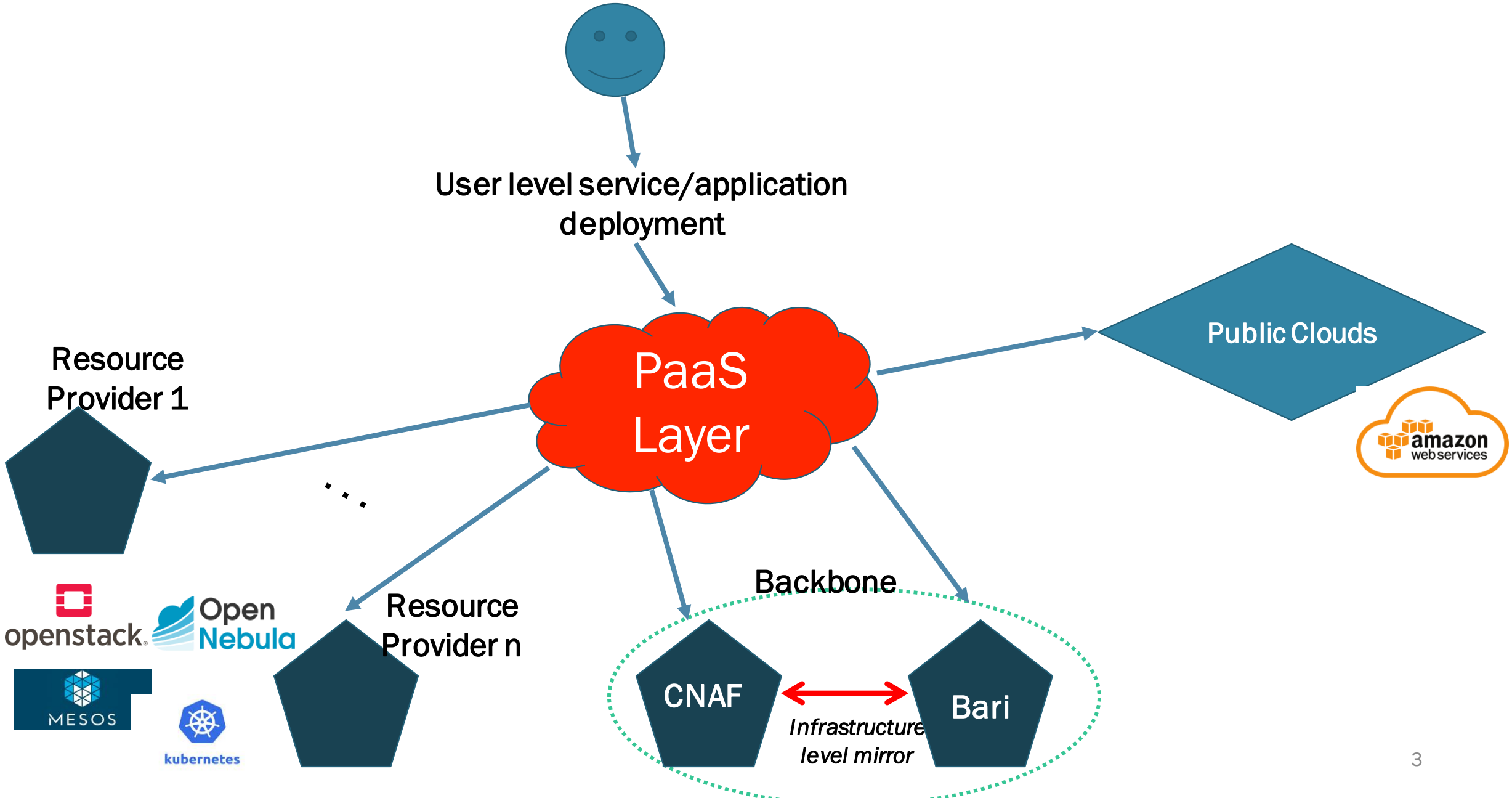
INFN Cloud

- Progetto partito a inizio 2020
- Goal: offrire servizi Cloud alle comunità di utenti INFN
  - Servizi configurati per le loro specifiche esigenze
  - Focus in particolare su servizi di alto livello
- Goal: infrastruttura distribuita con impatto limitato sui siti che decidono di federarsi

- INFN Cloud è una federazione di:
  - un backbone: 2 siti (CNAF e BARI) "tightly coupled"
  - un insieme di siti "loosely coupled"
    - al momento:
      - RECAS-BARI
      - Cloud@CNAF
      - CloudVeneto

Architettura



Fattori abilitanti

- Layer uniforme e consistente per gestire autenticazione e autorizzazione, implementato attraverso INDIGO-IAM
- Orchestrazione dinamica delle risorse implementata attraverso l'INDIGO PaaS Orchestrator
- Set di policy e regole di partecipazione consistenti

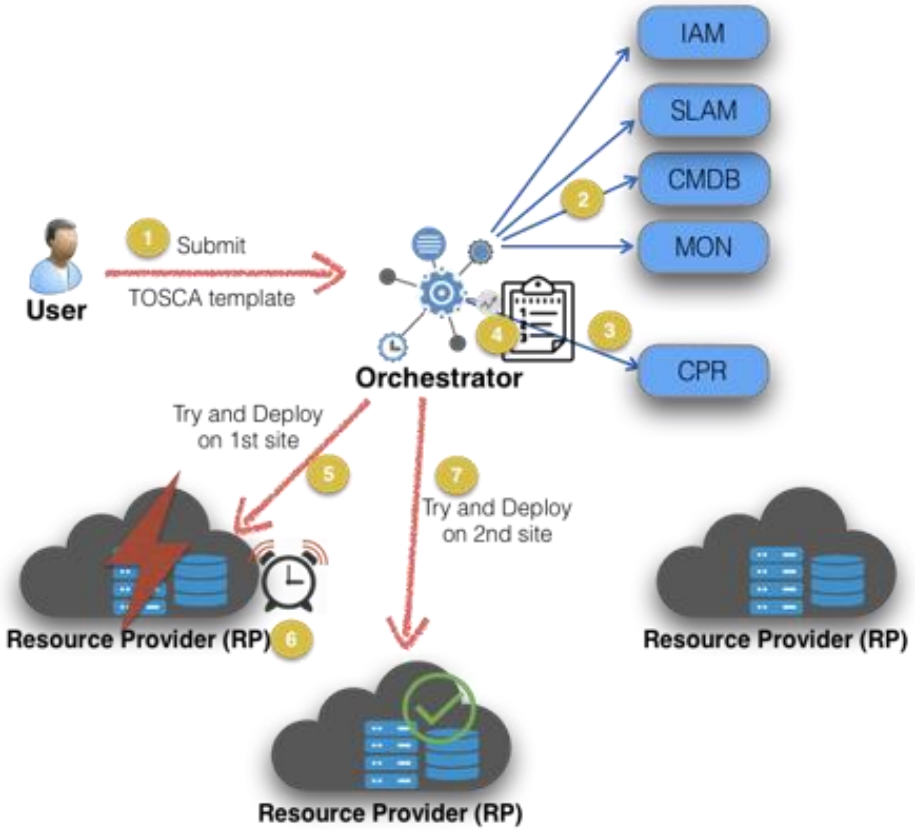
INDIGO IAM

- Provides a layer where identities, enrollment, group membership and other attributes and authorization policies on distributed resources can be managed in an homogeneous way
- Compliant with OAuth and OpenID-Connect standards and therefore easily integrable with many off-the-shelf components (Openstack, Kubernetes, …)
- Support SAML IdPs or identity federations, OpenID Connect providers and X.509 certificates for authentication
- Chosen as token based AuthN/Authz framework by WLCG
- Supported for the foreseeable future by INFN

INDIGO IAM in INFN Cloud

- Viene utilizzato per definire chi può istanziare servizi su INFN Cloud
- Molti servizi istanziati su INFN Cloud usano IAM anche per gestire chi può accedere al servizio
- Gli utenti in IAM sono organizzati in gruppi, che definiscono la Virtual Organization di appartenenza

INDIGO-PaaS Orchestrator



Orchestrator: responsabili di orchestrare le risorse distribuite e fare il deployment dei servizi su richiesta degli utenti

I servizi sono descritti attraverso TOSCA* template

* TOSCA (Topology and Orchestration Specification for Cloud Applications): OASIS standard language to describe a topology of cloud-based services, their components, relationships, and the processes that manage them.

User interfaces

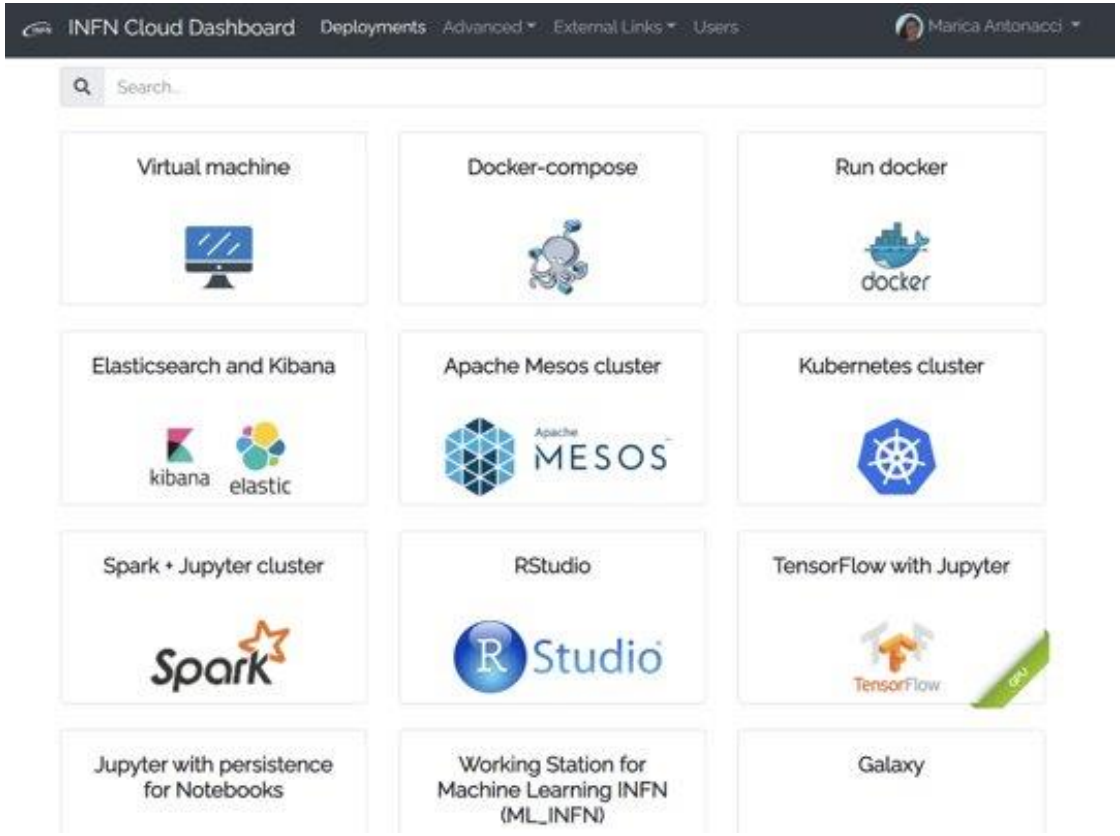
- *PaaS REST APIs*
- *Orchestrator CLI*
- *Orchestrator bindings (go, python)*

Richiede una conoscenza di TOSCA, almeno minima

- *Orchestrator Dashboard*

- Non serve conoscere TOSCA
- Accesso via web (facile e intuitivo)

Service Catalogue



Fornisce servizi di diverso tipo (IaaS, PaaS, Saas)

Viene costantamente espanso, per soddisfare nuovi use case

I servizi sono facilmente customizzabili

Approccio **lego-like:** componenti riusabili che possono essere usate per costruire nuovi servizi

Perché federarsi in INFN Cloud ?

- Per poter fornire agli utenti risorse in modo consistente e uniforme
- Per poter fornire ai proprio utenti servizi “di alto livello” senza la necessità di doverli implementare e gestire localmente
- Per essere allineati con le best practice in termini di gestione di una infrastruttura (incluse le tematiche legate alla sicurezza)
- …

Federazione con INFN Cloud

- Il sito federato mantiene controllo delle sue risorse
  - Il sito continua a usare i tool che preferisce
  - Decide il sito quante e quali risorse federare
  - Decide il sito che comunità di utenti autorizzare
  - Decide il sito come configurare gli utenti autorizzati

Posso federarmi ?

- Per accedere alla federazione INFN-Cloud
  - Bisogna rispettare i requisiti tecnici, regole e procedure specificati nelle Rules of Participation (RoP) di INFN-Cloud
  - Bisogna superare un processo di certificazione
- L'integrazione di un nuovo sito nella federazione deve inoltre essere approvata dal Project Management Board di INFN-Cloud

Cosa serve per federarsi ?

- Sostanzialmente è solo necessario:
  - Usare un Cloud/Container stack supportato dal layer PaaS di INFN-Cloud
    - OpenStack e` tra questi
  - Configurare lo IAM di INFN-Cloud come identity provider e abilitare gli utenti federati desiderati
  - Mandare gli usage record al server centrale di accounting di INFN-Cloud
  - Essere compliant con le policy specificate nelle “Rules of Participation”

Rules of Participation

- Definiscono i requisiti tecnici necessari, e le policy e procedure a cui attenersi

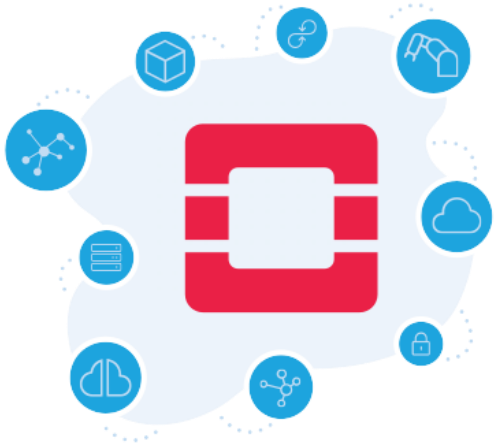
- Obiettivo: fornire in maniera efficiente e più possibile sicura servizi e risorse agli utenti, in modalità uniforme e consistente

Rules of Participation

- Why joining the INFN Cloud federation?
- Compliance for resource access
- Authentication and Authorization
- Resource allocation
- Resource configuration
- Supported end users' services
- Networking
- Support
- Service level targets
- Security
- Management of security incidents
- Traceability and logging
- Accounting
- Certification
- Withdrawals
- Violations

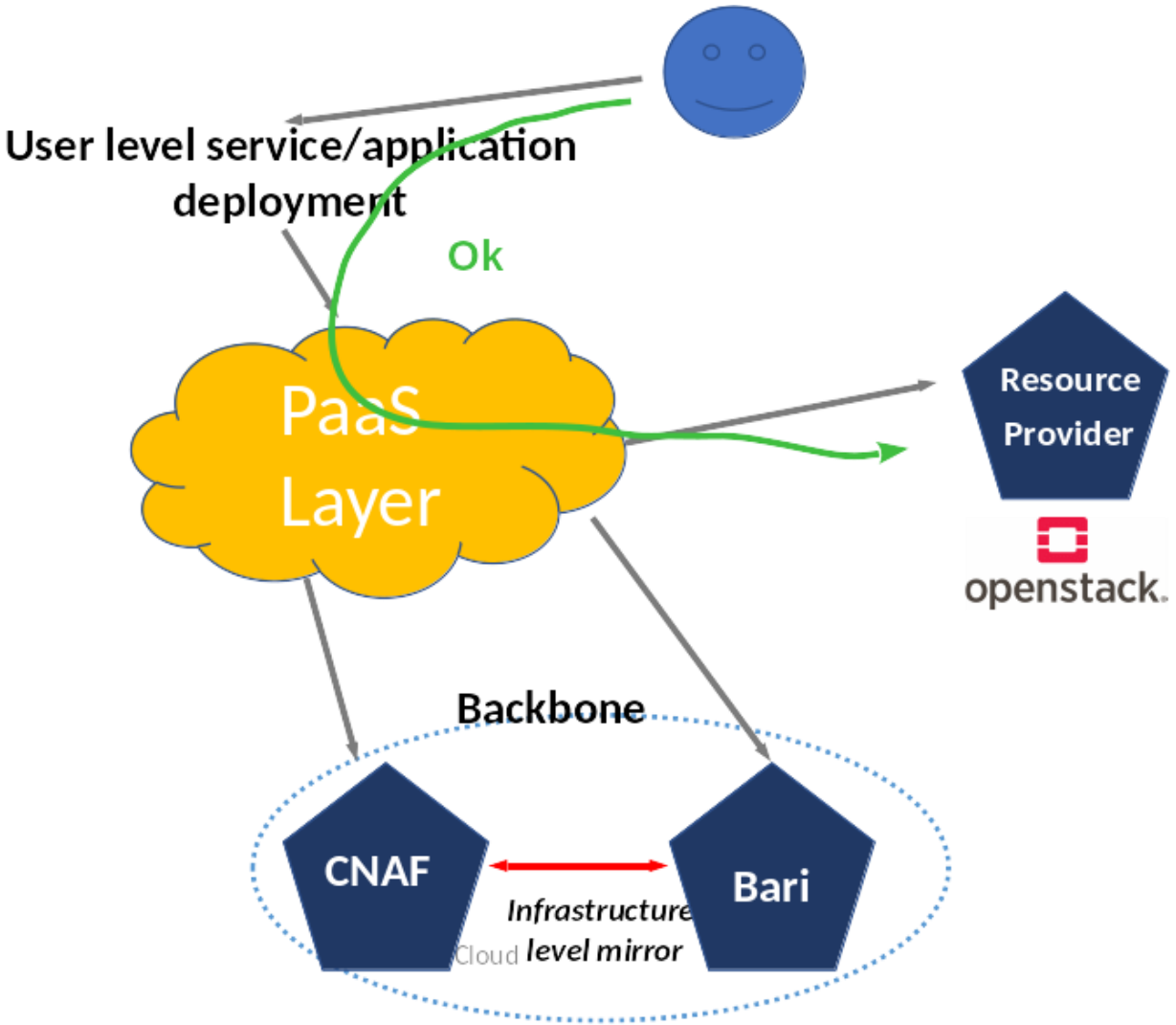
Integrazione con OpenStack

- Serve che siano configurati almeno i seguenti servizi:
  - Keystone (Identity)
  - Glance (Image)
  - Nova (compute)
  - Cinder (Block storage)
  - Neutron (Networking)
- Non serve una particolare versione di OpenStack



Accesso alle risorse

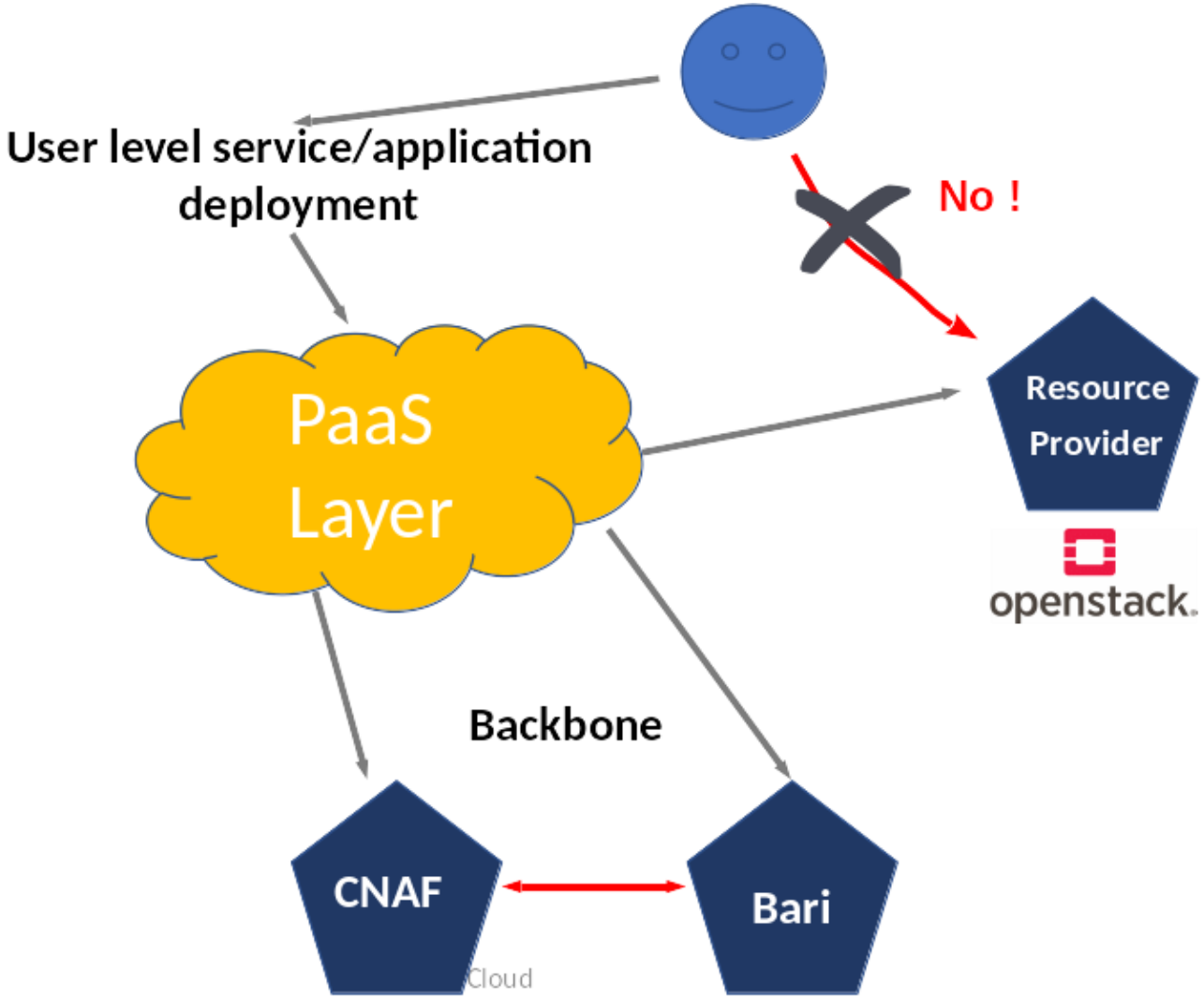
L'instanziazione di servizi attraverso il layer PaaS di INFN-Cloud è il modo "blessed" per accedere alle risorse



Accesso alle risorse

L'accesso alla IaaS bypassando il layer PaaS è consentito solo in casi particolari (servizi calcolo)

... anche se tecnicamente non si può impedirlo negli altri casi



Istanziazione di un servizio INFN Cloud (su OpenStack)

1. L'utente sceglie un servizio del Service Catalogue
2. Il layer PaaS di INFN Cloud sceglie un sito della federazione di INFN Cloud dove fare il deployment del servizio
3. Il layer PaaS crea una (o più) macchine virtuali sull'OpenStack di questo sito
4. Il layer PaaS configura (via ansible) il servizio su queste macchine virtuali

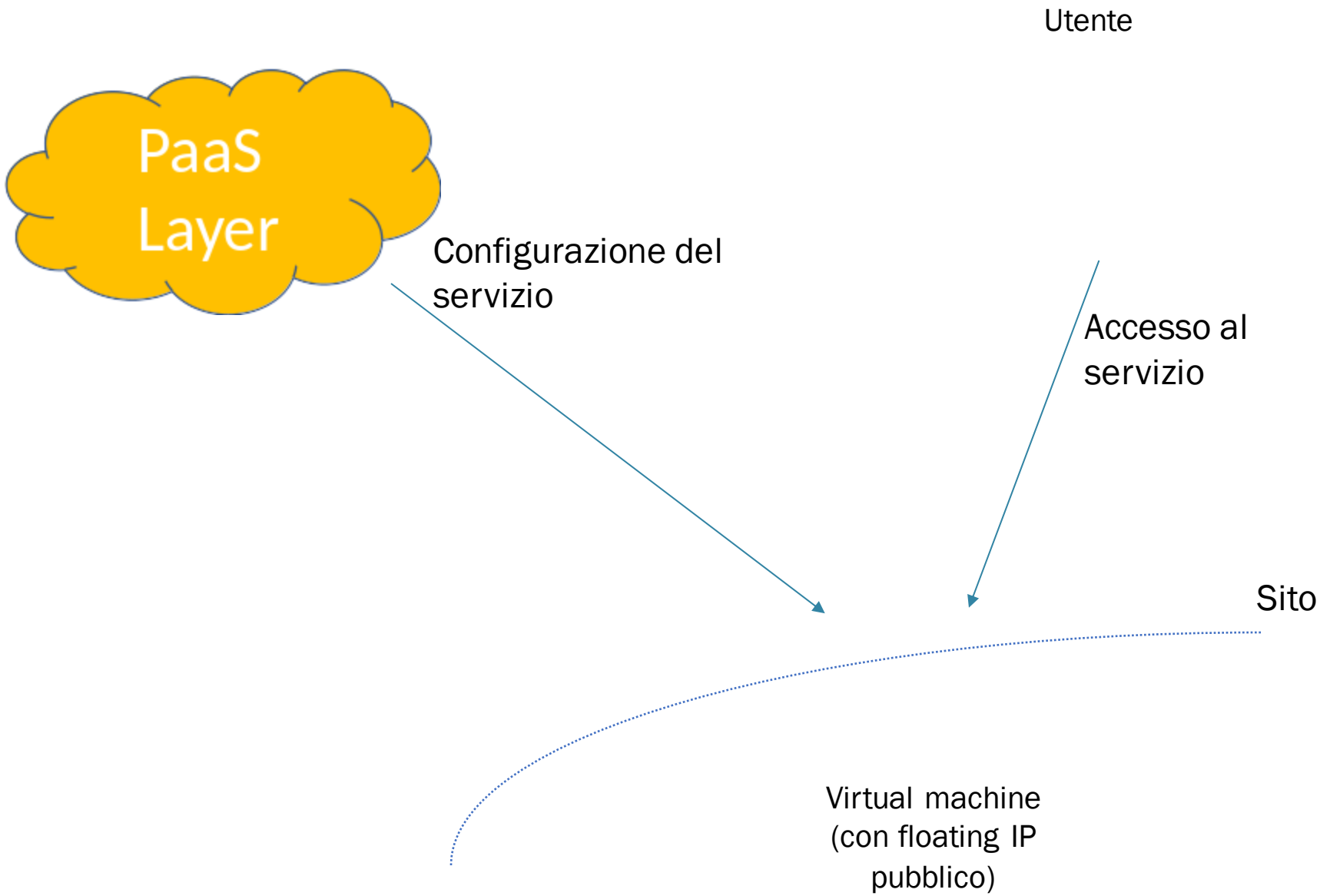
Servizi

- 2 categorie di servizi INFN Cloud istanziabili dall'utente:

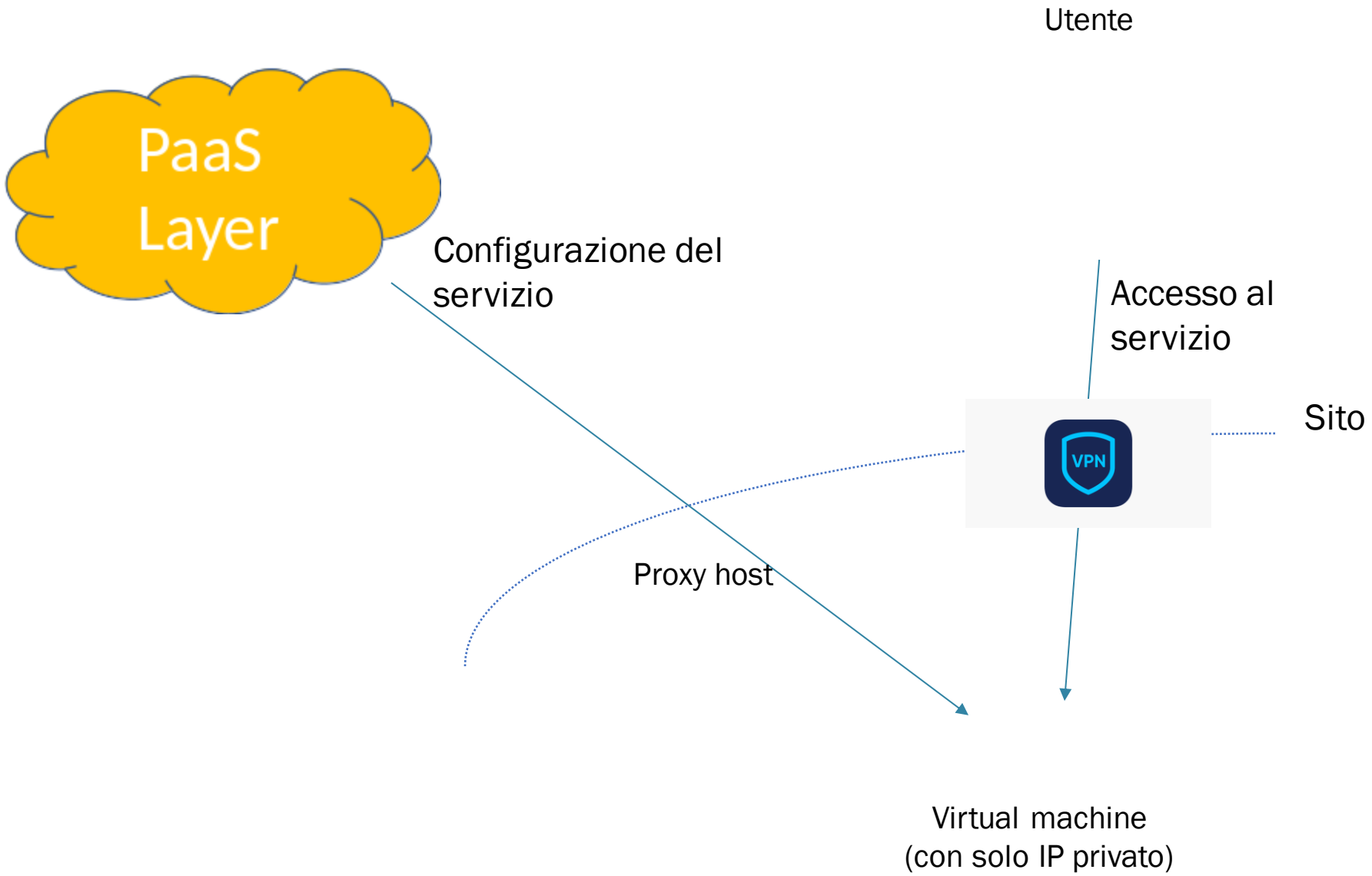
    A. Servizi su rete pubblica
    B. Servizi su rete privata (work in progress)

- Un sito della federazione di INFN Cloud può abilitare solo una di queste 2 categorie o entrambe

Servizi su rete pubblica



Servizi su rete privata



Servizi

- Per abilitare l'istanziazione di servizi da parte degli utenti INFN Cloud il sito deve:
  - Fornire e tenere aggiornate le immagini necessarie (v. prossima slide)
  - Fornire i flavor necessari
- Per il servizi su rete pubblica il sito deve inoltre:
  - fornire gli IP pubblici necessari (in genere uno per istanza di servizio)
  - Abilitarne l'accesso in rete
- Per I servizi su rete privata il sito deve inoltre:
  - Configurare i proxy-host e VPN server

Immagini

Sistema operativo	os_distro	os_version
Ubuntu 18.04	ubuntu	18.04
Ubuntu 20.04	ubuntu	20.04
CentOS 7	centos	7

Oltre ai metadati os_distro e os_version, le immagini devono avere il tag 'infn_cloud'

$ openstack image set --property os_distro=<distro> --property os_version=<version> <image-id>
$ openstack image set --tag infn-cloud <image-id>

Le immagini devono permettere accesso solo via chiave SSH (non via username-password)
Il fingerprint della chiave deve essere loggato

Gestione utenti

- Deve esssere abilitato lo IAM di INFN Cloud
- Gli utenti nello IAM di INFN-Cloud sono organizzati in user group
  - Gruppo /admins/<VO>: utenti che possono istanziare servizi su rete pubblica
  - Gruppo /PrivateResourceAdmins/<VO>: utenti che possono istanziare servizi su rete privata
- Il sito decide quali gruppi di utenti IAM vuole abilitare
- User group IAM diversi devono essere mappati nel sito in progetti OpenStack diversi

Abilitazione IAM di INFN Cloud

1. Registrazione di uno IAM client ("self service client registration" della istanza https://iam.cloud.infn.it)
2. Installazione e configurazione mod_auth_openidc (inserendo I dettagli del client prima registrato)
3. Modifica configurazione keystone per abilitare openid come metodo di autenticazione
4. Definizione di mapping tra gruppi IAM e progetti OpenStack locali

Ref: https://agenda.infn.it/event/23774/contributions/122401/attachments/76818/98889/Keystone_Auth_Federazione.pdf

Gestione utenti

- Deve essere sempre abilitato lo user group IAM "ops" (usato per monitoring) mappandolo su un progetto specifico

- È necessario garantire un isolamento tra utenti, anche dello stesso progetto
  - Un utente non deve essere in grado di cancellare la VM/il volume di un altro utente
    - Quindi è necessario modificare le default policy di nova e cinder

- Le risorse vanno assegnate (via quota) al progetto
  - Non c'è necessità di definire quote per utenti

Progetti per servizi su rete pubblica

- Dovranno avere a disposizione floating IP pubblici
- Per questi IP nel firewall di sito dovranno essere aperte le seguenti porte:
  - Porte basse: 22, 80, 443
  - Tutte le porte > 1024 tranne alcune "pericolose":
    - 1080 (socks proxy)
    - 1191 (gpfs) (udp+tcp)
    - 2049, 4045, 4046, 4049, 20048, 20049 (nfs) (udp+tcp)
    - 3260 (iscsi)
    - 3389 (rdp)
    - 5900 (vnc)
    - 5800 (jvr)
    - 10000 (webmin)
    - 6000 to 6023 (X11)

Progetti per servizi su rete privata

- In questi progetti una VM dovra` essere configurata dal site admin configurandola con:
  - Proxy host
    - Una macchina acceduta via chiave SSH dal "layer PaaS", e in grado di "parlare" con le VM su rete privata
  - OpenVPN server
    - Integrato via IAM
    - Abilitato ad essere usato solo dagli utenti di quel gruppo IAM
- Questa deve essere l'unica istanza nel progetto con IP pubblico

Service level target

What	Meaning	Minimun
Monthly availability	Ability to fulfil the intended function over a calendar month	90 %
Monthly reliability	Ability to fulfil the intended function over a calendar month, excluding scheduled maintenance periods	95 %

Supporto

- Utilizzo dell'INFN-Cloud service desk
- La priorità è specificata nel ticket (settata dall'utente ma modificabile dal team di supporto di I livello)
- Per gli incidenti di sicurezza sono previsti diversi tempi di risposta

Request priority	Ack. Time	Target solution time
Low	5 working days	3 months
Normal	3 working days	2 weeks
High	1 working day	5 working days
Critical	1 working day	2 working days

Gestione vulnerabilità

- Vengono fatte regolarmente scansioni di sicurezza sui servizi istanziati su INFN Cloud
- La vulnerabilità in una istanza deve essere curata dall'utente-ammministratore che ha istanziato e gestisce quel servizio
  - Il site admin viene comunque avvisato
- All'amministratore del sito viene chiesto di isolare l'istanza, se la vulnerabilità non viene risolta nei tempi stabiliti

Date	Status	Task	Severity	Scan Results	Actions
Thu Jan 9 03:05:08 2020	Done	Immediate scan of IP 192.168.11.137	N/A	0 0 0 0 0	

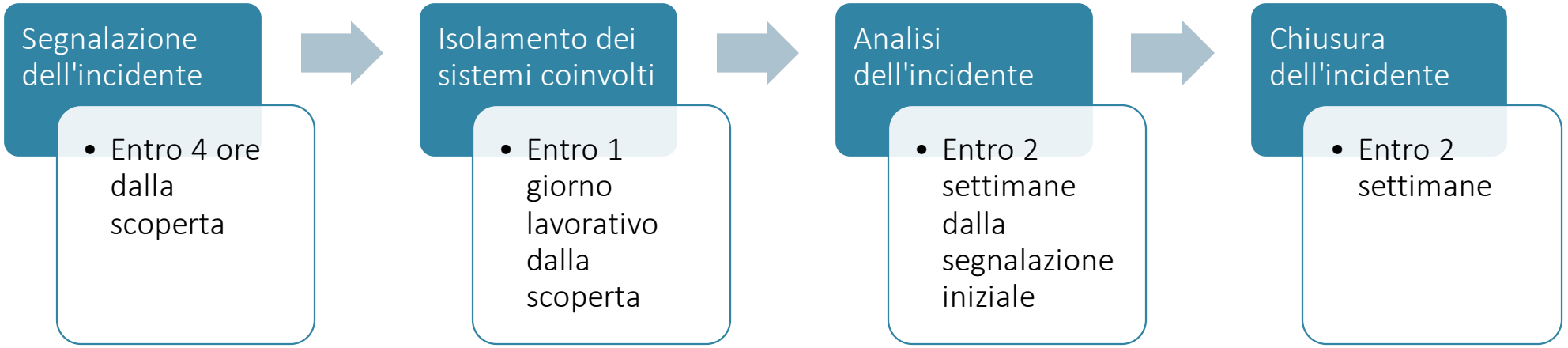
Report: Results (312 of 734)

ID: 97cc63d0-65d7-45ee-8ca8-711df1baa7dd
Modified:
Created:
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	75%	192.168.11.137	512/tcp	
Samba End Of Life Detection	10.0 (High)	75%	192.168.11.137	445/tcp	
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10.0 (High)	75%	192.168.11.137	445/tcp	
PHP Multiple Vulnerabilities - Aug08	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP Version < 5.2.7 Multiple Vulnerabilities	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	80/tcp	
MySQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	3306/tcp	
PostgreSQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	5432/tcp	

Gestione incidenti di sicurezza

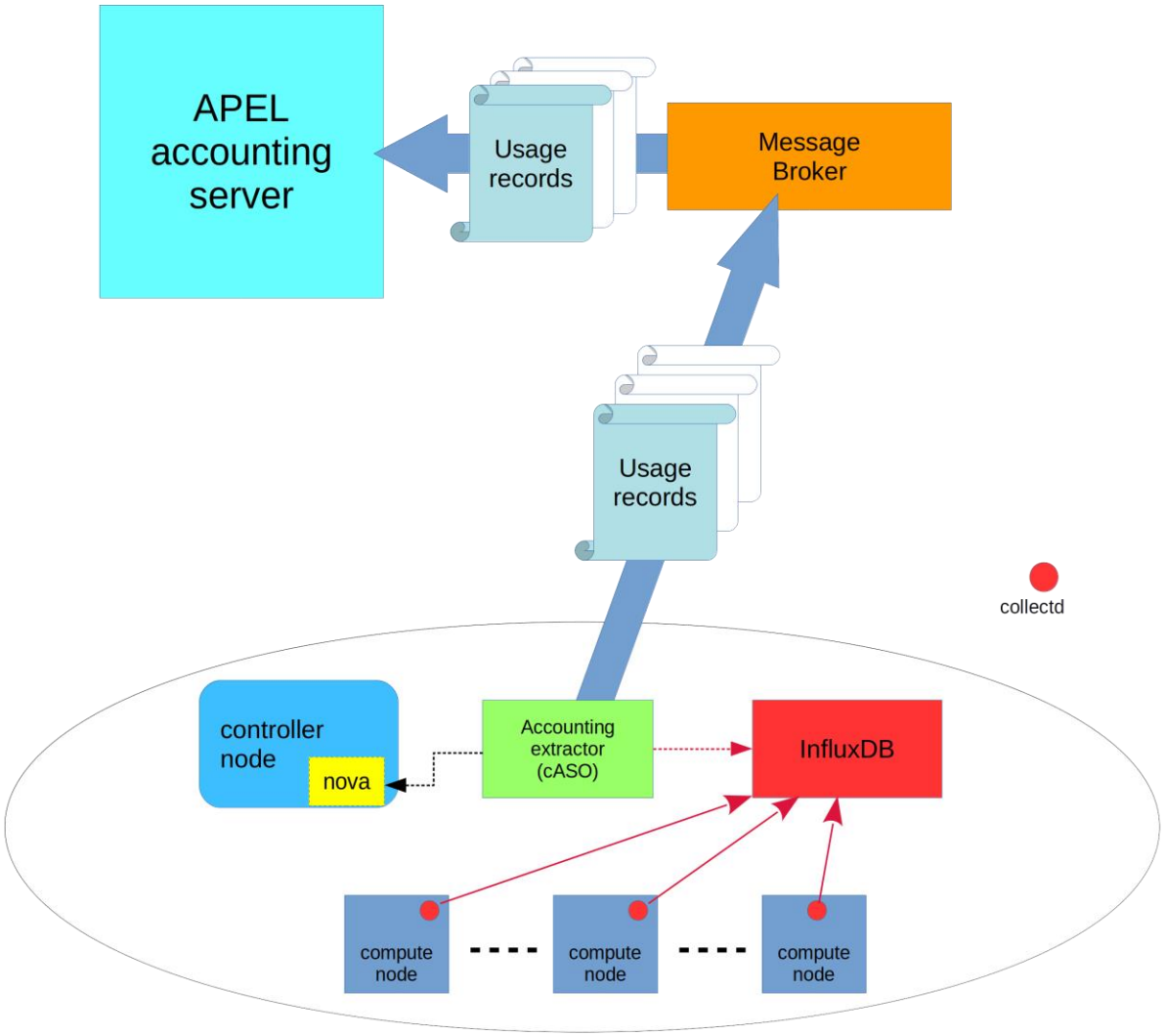
- Nel caso di incidente di sicurezza in una istanza di INFN Cloud al site admin viene chiesto:
  - Di isolare l'istanza
  - Di analizzare (assieme all'amministratore responsabile di quella istanza) l'incidente e di produrre un report



Accounting

- Obiettivo: misurare l'uso delle risorse su base temporale
  - Quante risorse usa un utente?
  - Quante risorse usa un gruppo di utenti?
  - Quante risorse fornisce un sito?
  - Un sito fornisce almeno le risorse «promesse» (pledged)?
  - Un sito fornisce più delle risorse promesse?

INFN Cloud Accounting Architecture



Openstack site

Accounting: responsabilità del sito

- Il sito deve inviare gli usage record (solo quelli relativi ai progetti federati con INFN Cloud)

- Per fare questo il sito deve configurare opportunamente i servizi richiesti lato "resource provider":
  - cASO
  - Collectd
  - Influxdb
  - Apel-ssm

- V. https://confluence.infn.it/x/xQLdAg

Logging

- I log dei servizi OpenStack devono essere mantenuti per almeno 90 giorni e non più di 1 anno

- Non è richiesto (ma è consigliato) di raccogliere e centralizzare i log delle singole istanze
  - La cosa può essere implementata nelle immagini, o via vendor-data

Riferimenti

- INFN Cloud Federated cloud site admin Guide (https://guides.cloud.infn.it/docs/admins-guides/en/latest/admins_guides/index.html)
  - Under construction

- INFN Cloud Policies & Procedures (https://www.cloud.infn.it/policies-procedures/)
  - Scansioni di sicurezza e gestione degli incidenti su INFN CLOUD
  - Rules of Participation