ITALY
OpenInfra Days

OPENINFRA DAYS
ITALY

# OpenStack for Government Cloud: the Italian Experience

**25-Settembre-2019**

Franco Fiorese - DXC.technology
franco.fiorese@dxc.com

Organized by

IRIDEOS

Binario Etico

Under the patronage of

AGID | Agenzia per l'Italia Digitale

Sponsored by

Mellanox TECHNOLOGIES

MESOSPHERE

gci SERVICE FACTORY

# DXC Technology

DXC.technology è oggi, in Italia, un attore rilevante nel settore dell'IT per la pubblica amministrazione ed offre un catalogo di servizi in rapida espansione per consentire ai clienti della P.A. Italiana di accelerare il loro processo di trasformazione digitale.

**$20+B**
global IT services leader

**200+**
partner network with best-of-breed partners
15 strategic partners

**~6,000**
clients
200+ Fortune 500 companies

**60+**
years of innovation

**~138,000**
employees worldwide

**#122**
in the 2019 Fortune 500

**#19**
of *CR Magazine*'s 100 Best Corporate Citizens for 2018

**70+**
countries

**10,000+**
Agile/DevOps professionals


Insurance
Healthcare & Life Sciences
Travel, Transportation & Hospitality
Banking & Capital Markets
Aerospace & Defense
Consumer & Retail
Energy, Utilities, Oil & Gas
Manufacturing & Auto
Public Sector
Technology, Media & Telecommunications

Build on the best of **innovation**

Align with customer **preferences**

Provide **clarity** for clients

Analytics
Application Services
Business Process Services
Cloud & Platform Services
Consulting
Enterprise & Cloud Apps
Industry Software & Solutions
Security
Workplace & Mobility

# Agenda

1. **SPC-Cloud Lotto 1**
2. **Reference context**: the SPC-Cloud public tender, the offered services, the user landscape
3. **The technology platform:** the evolution in the last 3 years
4. **The new services introduces in 2018**: Container DevOps Platform (ECaaS)
5. **QA**

# SPC Cloud – Lot 1

- **The contract**: assigned in 2016 after a tender issued in 2014 with a budget of 500€, to the TJV composed by **TIM**, **DXC** e **Poste Italiane** e **Postel**
- **Goal**: the service included in Lot 1 are geated to accelerate the consolidation of Data Centers in the PS space by using enabling service, with cloud based hw and sw resources. The physical infrastructure of this community cloud platform must be fully dedicated to the public sector clients.
- **Clients:** all the entities that are part of the local and central Public Sector domain in Italy
- **Offered services**: IaaS, PaaS, SaaS, Cloud enabling (professional services)
- **New services introduced in2017**: DRaaS, ECaaS, Managed Services, H24 Managed
- **Duration of the framework contract**: 5 years (ends July 2021)
- **Official internet site**: https://www.cloudspc.it/ where all the documentation (technical, contracts, pricing, guidelines on reversibility) and the evidence of the management comittee meetings
- **Locations of delivery center in Italy**: Milan and Rome
- **SLA and guarantee on deliverted services:** the contracts include penalty of service failures and moreover there is the need to guarantee delivery of service in case of any delay in payments or missing payments (art. 340 p.c.)

TIM

DXC.technology

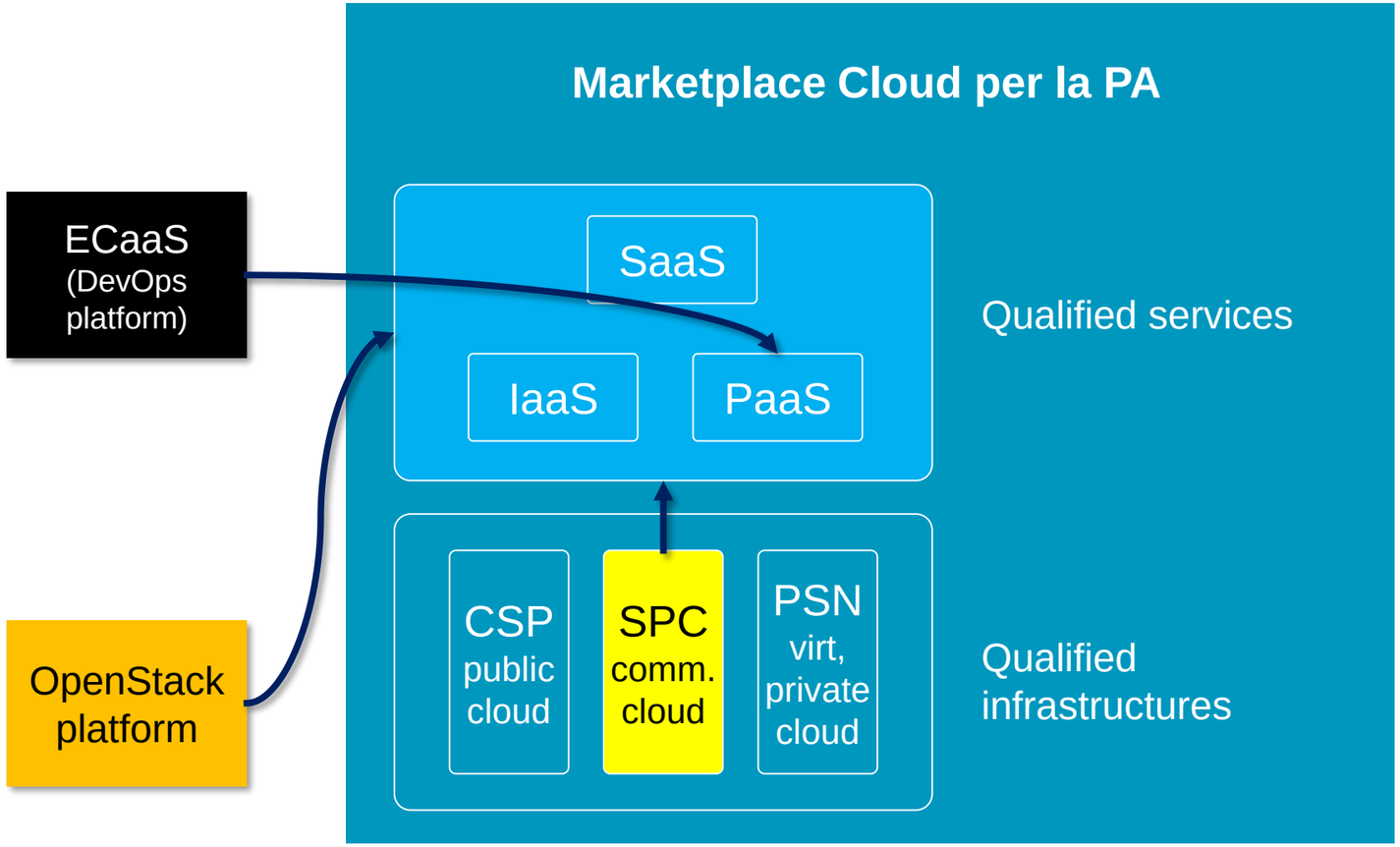
Posteitaliane

Postel

# Reference context

## The cloud for the Public Sector and SPC Cloud Lot 1

- Consistent model with a marketplace that offer multiple choices, all qualified by AgID.
- Compliance with ISO 17888 6.6 standard for cloud service governance.
- Categorization based on the service level,delivered support in relation to the qualified infrastructures.
- Easiness of contract activation: SPC-Cloud allow allow a quick contract activation for all the offered services.



# The technology platform

## The original proposal to use of OpenStack for SPC-Cloud Lot 1

### Initial requirements

The proposal made by the TJV for SPC-Cloud Lot 1, formalized at the end of 2014, that won the tender is based on the use of OpenStack. To be fully compliant with the requirements of the public tender RFP some customizations were developed – the most relevants are:

- Allow the creation of VDC (Virtual Data Center) where elementary resources (CPU, RAM, storage, network) can be aggregated. This allow also the creation of custom VM flavors.
- Management of VM images with ownership a multiple levels and sharing across internal and external organizations.
- Hierarchical acess to tenant administration functionality
- Two storage tiers: standard and high performance
- Resize of VM

### The project and the implementation

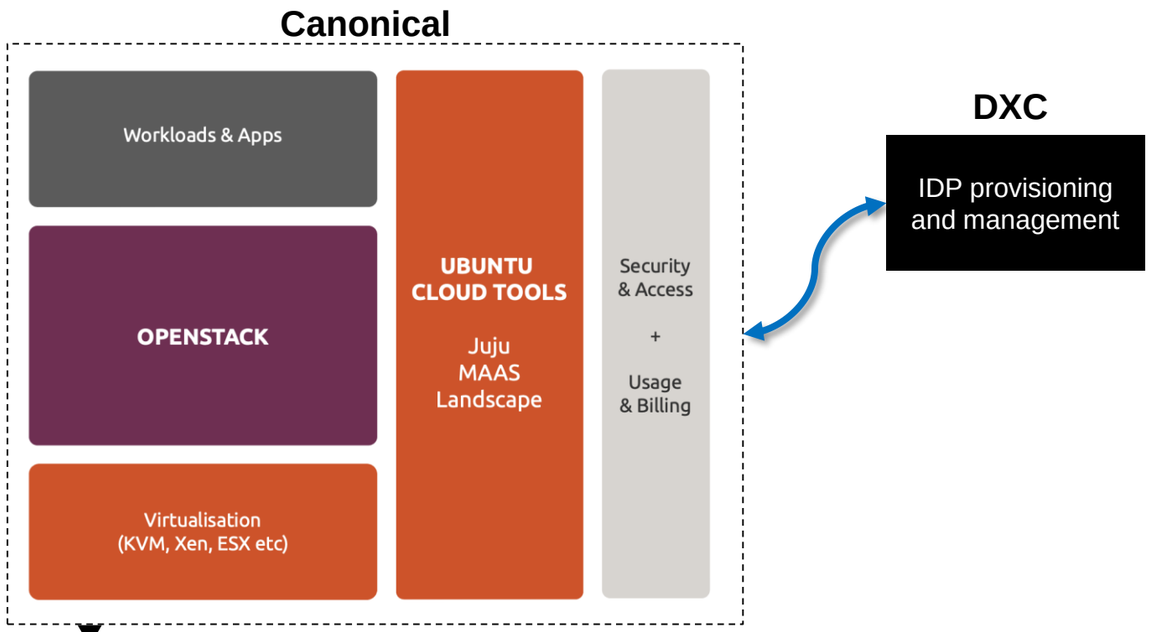
- The initial choice was to select HPE Helion OpenStack distribution on top of which there were developed custom functionalities – focused mostly on the Horizon component.
- The initial release – deployed early in 2015 has been Mitaka – the tender was awarded in May 2016.
- The hardware infrastructure was based on HPE Proliant blade servers.
- The block storage was based on HPE 3PAR while the object storage on HPE Apollo.
- The platform lifecycle management, very crucial aspect, was initially based on TripleO and after that on Helion Lifecycle Manager
- Some customizations were selected for upstream contribution (OpenStack Freezer project)

# The technology platform

## The evolution: moving from Helion OpenStack to Canonical OpenStack

The nice choice to use an open soruce solution like OpenStack allowed for a facilitated transition towards a different solution, without changing architecture and software components.

The migrations of the client's resources has been tenant driven.




**Production grade OpenStack (Queens release) with:**

- Compute based on KVM, LXD (containers) used for internal services
- Networking based su OpenVSwitch

**Cloud machine**:

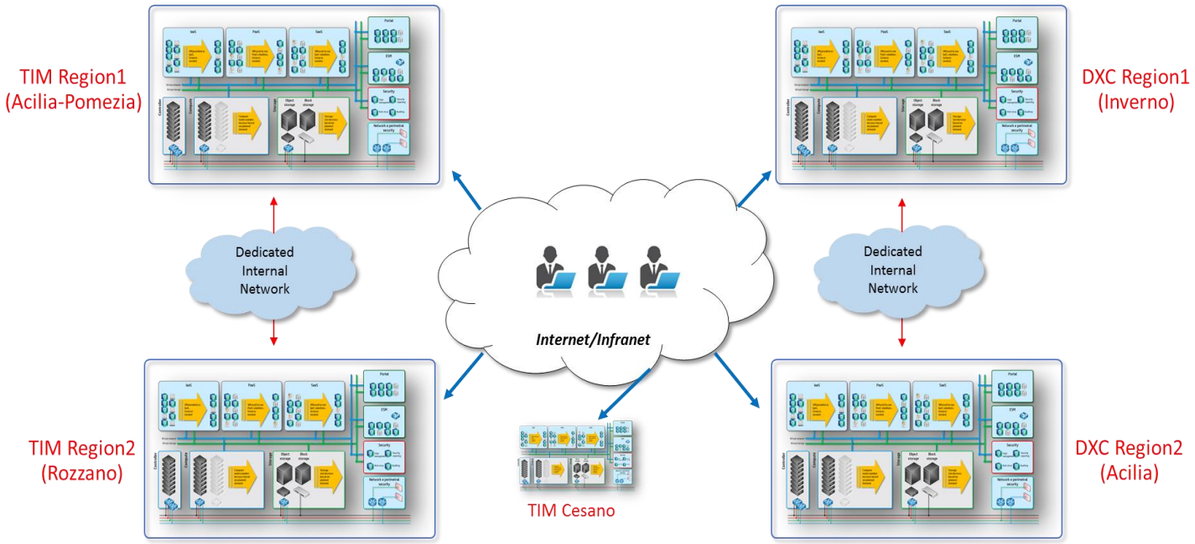
- Use of rack servers with converged tecnology (compute+storage nodes)
- MaaS physical automation (bare metal provisioning)
- Service modeling based su Juju
- Control plane with services using containers (LXD)
- Nodes updated using Canonical Landscape
- DXC designed and developed an application to manage the federated domains and the SAML2 + 2FA authentication (it can be integrated with SPID: Italy's PS Identity Management)
- Creation of private flavor for end users (domain + ad hoc policies)
- Private visibility of VM images
- Ceph for block storage and Swift for object storage
- Platform configuration backup (using Juju)

# The technology platform

## Architecture and functionality: multi-region

The new architecture improve the availabity of services and through the use of the following solutions:

- **Multi-region**: allowing native cloud IT services based on mutiple active regions
- **Re-design and re-engineering** of the **Disaster Recovery** functions, no more based on the whole platform DR, instead it provides a tenant based recovery of the services.
- Introduction of the *Fast Recovery* e *Always-on* concepts

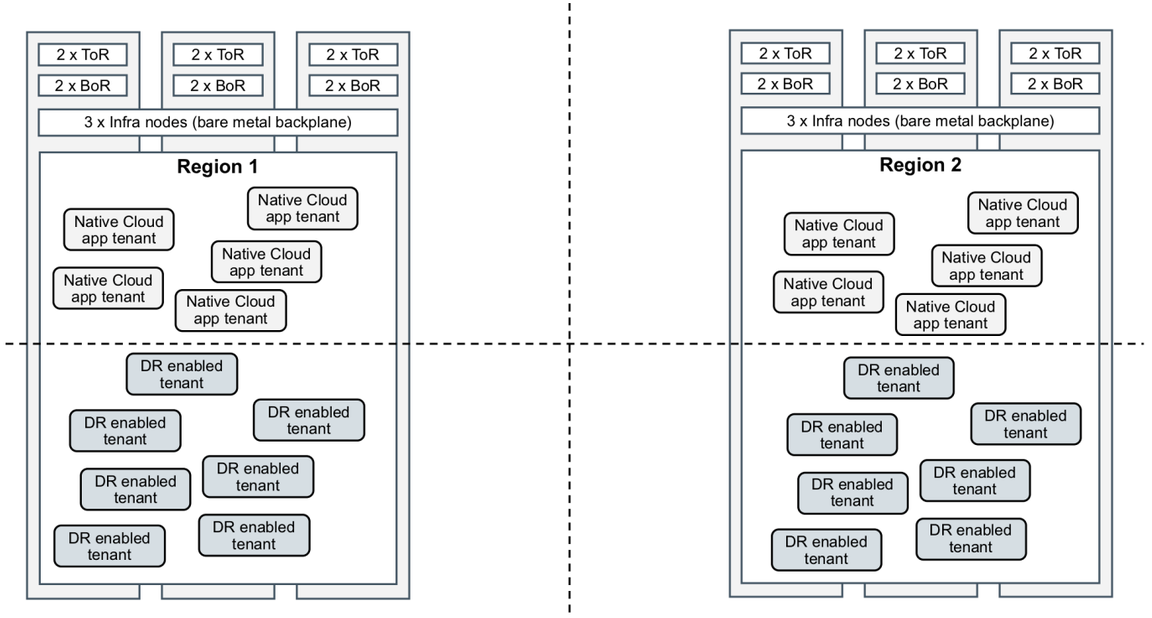



- **Fast Recovery**: a functionality fullu equivalent to traditional DR but implemented at tenant level.
- **Always On**: a functionality that is equivalent to traditional BC (Business Continuity) based on the use of multi-region and available to cloud native application services.

# The technology platform

## Use of the regions: workloads post-legacy and native cloud applications

- Each region is created by using an automated consistent deployment based on Juju and LXD
- From an end user perspective the OpenStack regions have equivalent functionality of the same kind of regions used in most of the public cloud service providers platforms
- The availability of multiple regions allow the users to place applications in disparate geographical locations with the benefit to get access to the services even on case of failures on a single region. The best resiliency can be obtained with the *Always-on* functionality by developing cloud native applications.
- The users get access to the different region with the same account identity (integrated with the 2FA access, as per AgID's request).



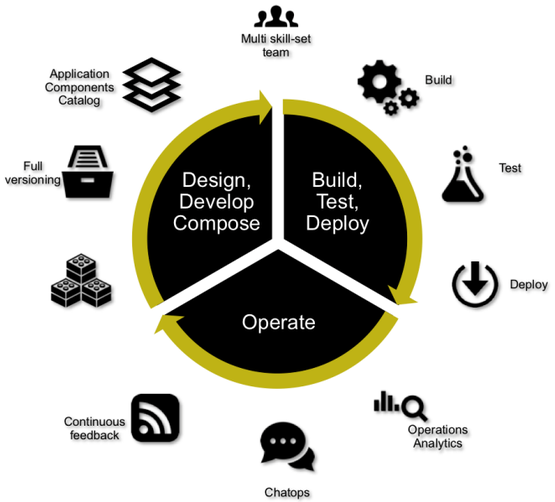

- During the tenant activation the type of resiliency support required must be specified: *fast-recovery* o *always-on.*

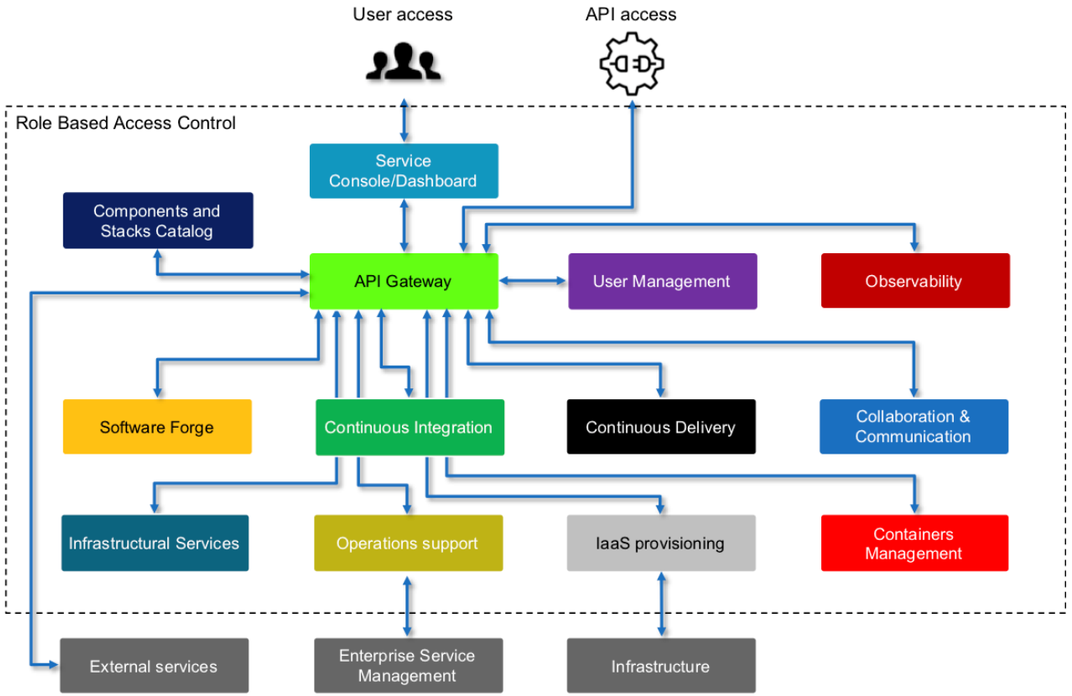
# Container DevOps Platform (ECaaS)

## Enablement of DevOps and microservices using  containers technology

The CDP service has been defined at beginning of 2017 and a specific process was started to set model, technology approach and price, as a new SPC-Cloud Lot 1 PaaS service: **Enterprise Container as a Service**

ECaaS is a fully managed service. that provide a fully fledged DevOps platform dedicated to each specific client.
Using this solution it is possible to manage the whole lifecycle of an IT service with a DevOps model, fully exploiting the Docker and Kubernetes technology.

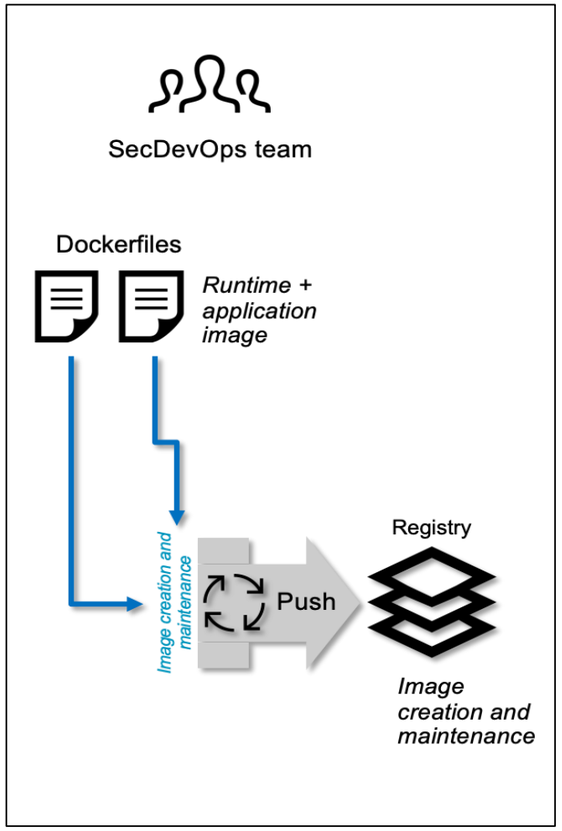


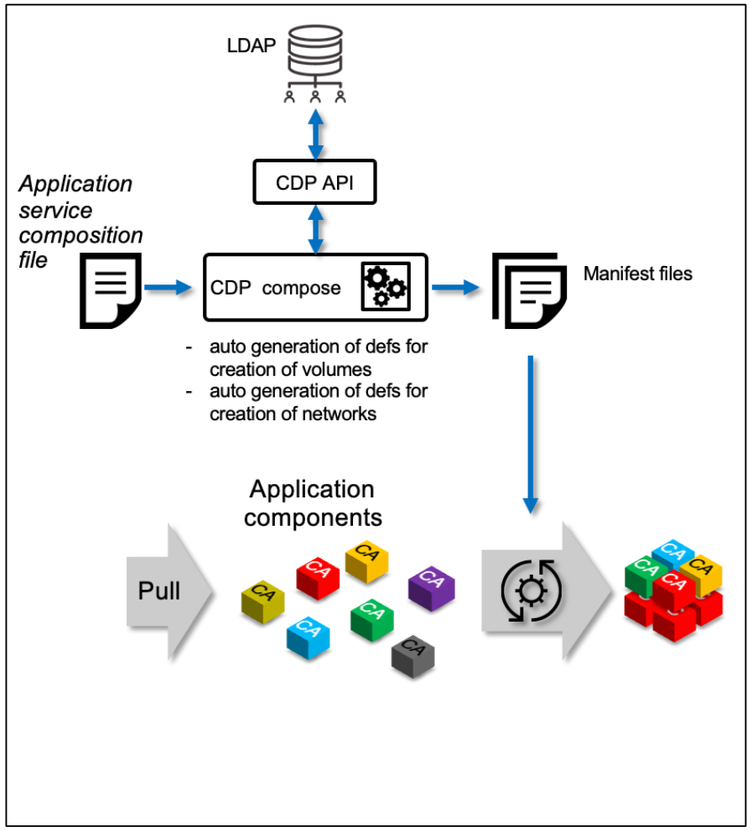

There are already several PS cliants that are using it: AgID, DFP, MIUR, ANPAL, INDIRE, Comune di Roma, Comune di Milano.

# Lifecyle of stateful application services

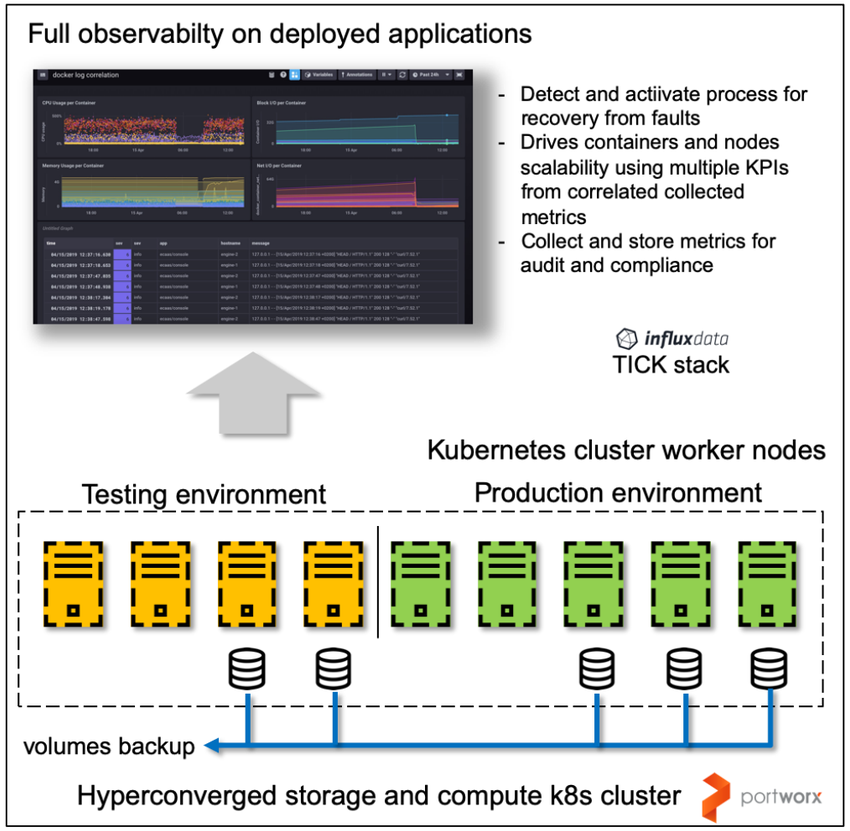
## Design, Develop Compose




## Build, Test, Deploy




## Operate (Monitor and Diagnose)




**Every software assets (config, definitions, scripts) stored in 'git' repos**

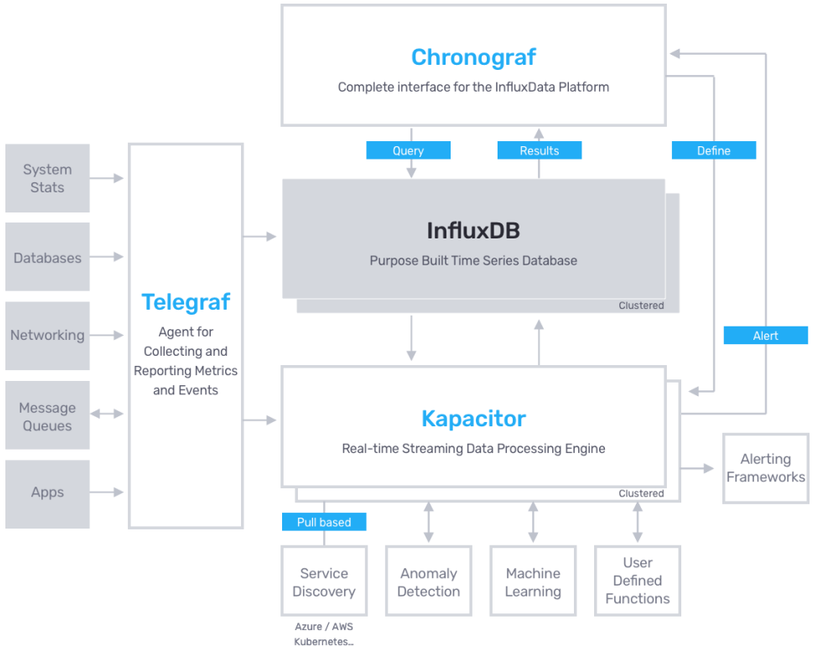
git

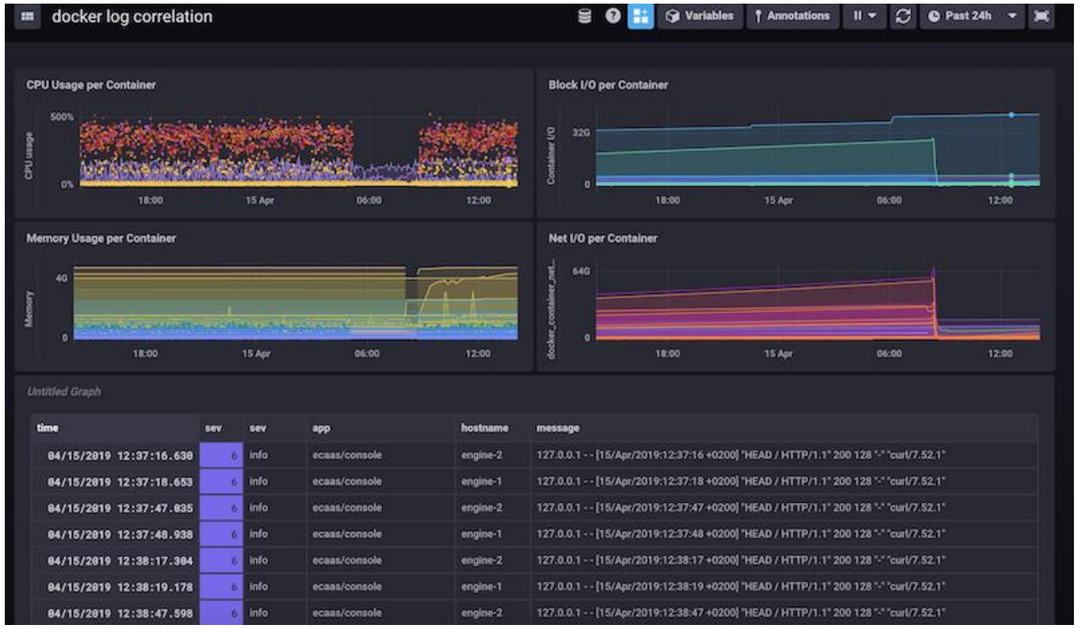
# Upcoming functionality on CDP (ECaaS)

## Observability

**Goal**: determine the health state of a system [distributed and complex] by inferring from the knowledge of its output

**Approach:** use of open source solutions:  Influxdata TICK stack (Telegraf, InfluxDB, Chronograf and Kapacitor), Jaeger (distributed tracing) to correlate different metrics, events, logs, etc. all indexes on a time scale (time-series DB), fully managed and exploitable through dashboard, CLI and API.



# QA

# Agenda

1. **SPC-Cloud Lotto 1**
2. **Contesto di riferimento**: la gara SPC-Cloud, i servizi offerti, il bacino di utenza
3. **La piattaforma tecnologica:** l'evoluzione negli ultimi 3 anni
4. **I nuovi servizi introdotti nel 2018**: Container DevOps Platform (ECaaS)
5. **QA**

# SPC Cloud – Lotto 1

- **Il contratto**: assegnato nel 2016 dopo una gara indetta nel 2014 con un budget di 500M€ al Raggruppamento Temporaneo d'Impresa costituito da **TIM**, **DXC** e **Poste Italiane** e **Postel**
- **Obiettivo**: i servizi del Lotto 1 sono finalizzati ad incentivare il consolidamento dei CED delle PA mediante servizi abilitanti quali la fruizione di risorse hardware e software in logica di "Cloud Computing" rese fruibili mediante infrastrutture fisiche, dedicate esclusivamente alla P.A., centralizzate e basate su un modello di cndivisione tra le PA di tipo "Community Cloud".
- **Clienti:** rivolto tutte le entità della pubblica amminstrazione centrale e locale
- **Servizi previsti ed offerti**: IaaS, PaaS, SaaS, Cloud enabling (servizi professionali a supporto di attività progettuali di virtualizzazione di infrastrutture delle PA)
- **Nuovi servizi introdotti sucessivamente (2017)**: DRaaS, ECaaS, Managed Services, H24 Managed
- **Durata del contratto**: 5 anni (scadenza Luglio 2021)
- **Sito ufficiale**: https://www.cloudspc.it/ dove sono pubblicati, in piena trasparenza, tutta la documentazione relativa al contratto quadro, i servizi, prezzi, modalità di fruizione, atti del Comitato di Direzione Tecnica, linee guida sulla reversibilità, ecc.
- **Centri di delivery e data center localizzati in Italia**: Milano e Roma
- **I servizi sono garantiti con specifici SLA** con penali dovute su eventuali disservizi, i clienti inoltre hanno la garanzia di erogazione della fornitura del servizio anche in caso di esaurimento del budget economico attivato inizialmente (art. 340 c.p.)

TIM

DXC.technology

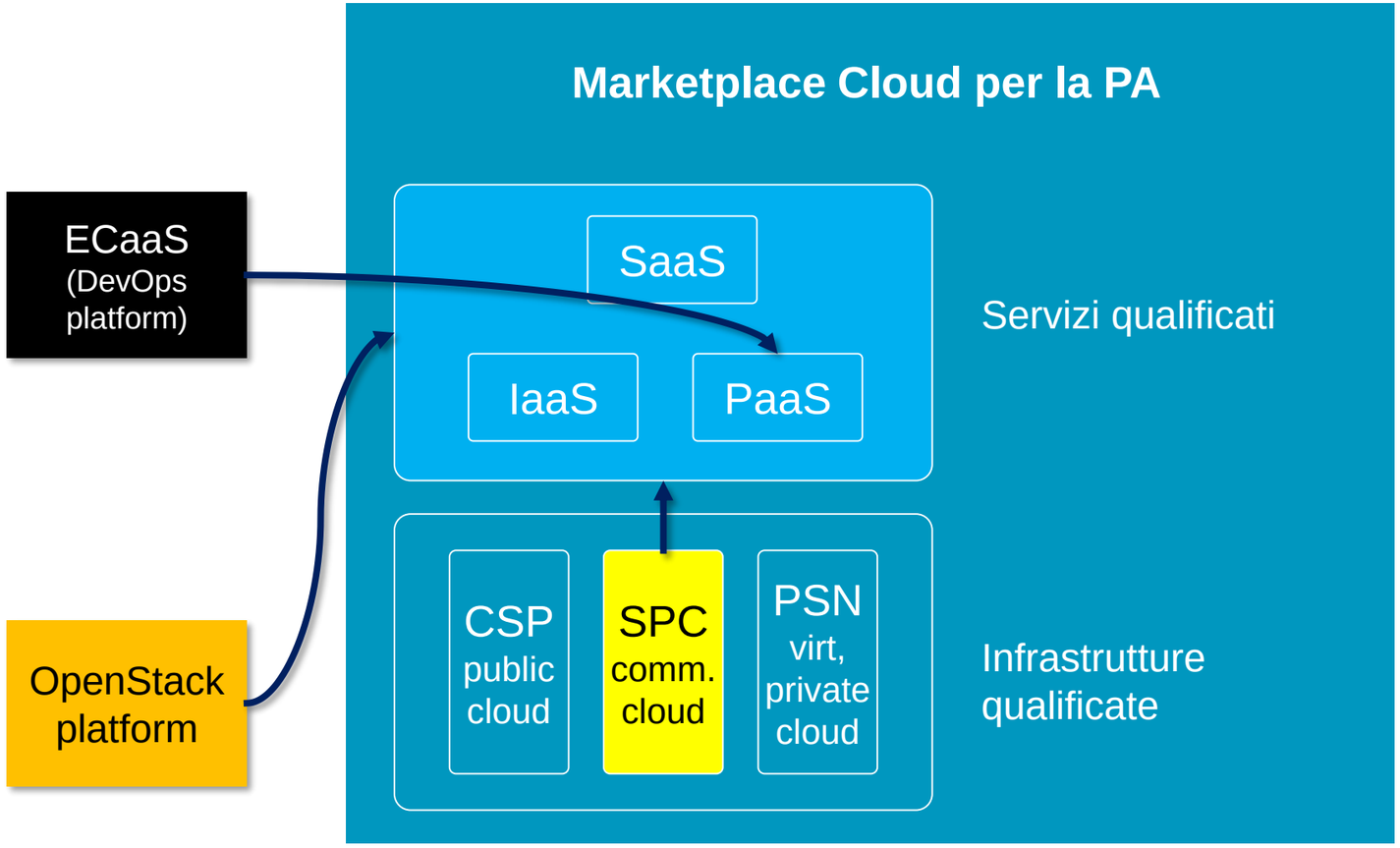
Posteitaliane

Postel

# Il contesto di riferimento

## Il cloud per la P.A. e SPC Cloud Lotto 1

- Modello consistente con un markeplace che favorisce più scelte, tutte qualificate da AgID
- Conformità allo standard ISO 17888 6.6 standard per la Cloud Governance
- Caratterizzazione sulla base del livello di servizio (SLA, supporto, ecc.) erogato in relazione a servizi e infrastrutture qualificate
- Facilità di attivazione dei contratti. SPC-Cloud permette una contrattualizzazione rapida per tutti i servizi erogati.



# La piattaforma tecnologica

## La proposta di usare OpenStack per SPC-Cloud Lotto 1

### I requisiti iniziali

La proposta iniziale del RTI per la gara SPC- Cloud Lotto 1, formalizzata a fine 2014 e risultata vincitrice dell'appalto, è basata sull'uso di OpenStack. Per poter ottemperare ai requisiti del capitolato di gara è stato necessario prevedere delle personalizzazioni, in particolare tra le più rilevanti:

- La possibilità di fornire ambienti VDC (Virtual Data Center) con risorse elementari (cpu, ram, storage e network) aggregabili liberamente – in pratica la possibilità di creare flavor personalizzati di VM
- Gestione delle immagini VM con funzionalità di condivisione tra gruppi e utenti
- Accesso gerarchico all'amministrazione di un tenant
- Tier differenziati per block storage: standard e alte prestazioni
- Resize delle immagini VM

### Il progetto e l'implementazione

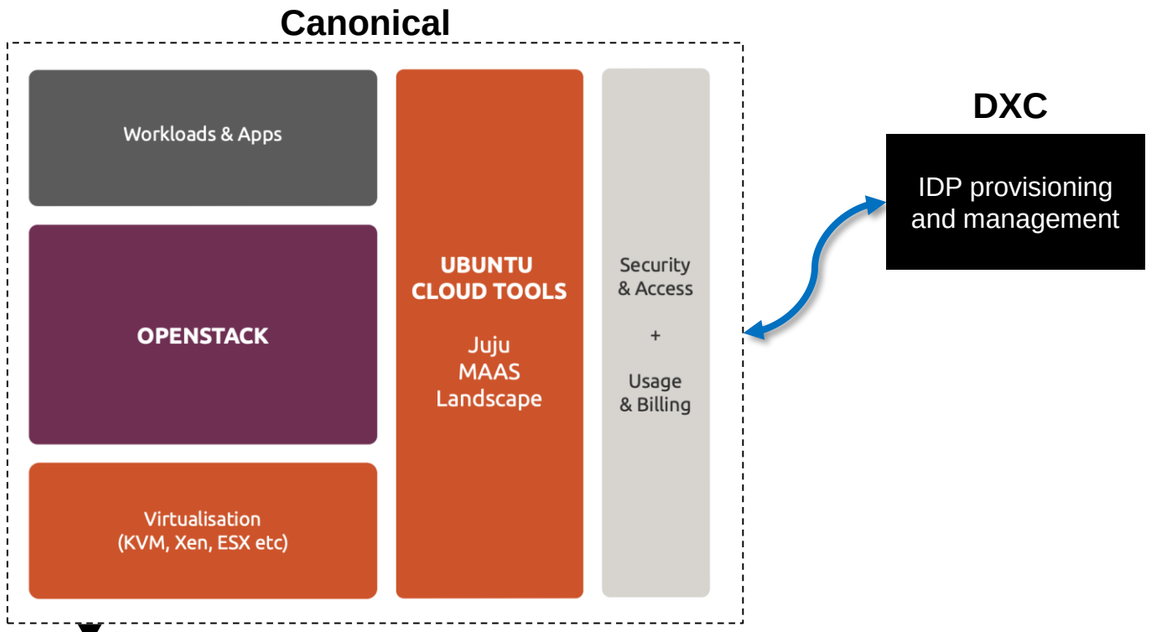
- La scelta iniziale è stata basate sulla distribuzione Helion OpenStack di HPE su cui sono state create delle personalizzazioni concentrate prevalentemente sulla console Horizon. Sebbene si sia cominciata l'attività di implementazione da Gennaio 2015 la release iniziale è stata la Mitaka (aggiudicazione gara: 19-maggio-2016)
- L'infrastruttura  hardware è stata inizialmente basata su server HPE Proliant nella versione blade
- Lo storage è stato implementato su piattaforma HPE 3PAR per il block storage e HPE Apollo per l'object storage
- Il lifecycle management della piattaforma, aspetto molto critico per un community o public cloud, era basato su TripleO, poi successivamente con Helion Lifecycle Manager
- Alcune personalizzazioni hanno avuto un percorso di contribuzione al progetto upstream OpenStack (Freezer)

# La piattaforma tecnologica

## L’evoluzione: il passaggio da Helion OpenStack a Canonical OpenStack

La bontà della scelta iniziale di una piattaforma cloud open source come OpenStack ha permesso di affrontare una migrazione da una distribuzione ad un’altra senza alterare l’architettura ed i componenti software della piattaforma stessa.

La migrazione è stata attivata su base dei singoli tenant di ogni cliente già presente sulla precedente edizione di OpenStack.




**Production grade OpenStack (Queens release) con:**

- Compute basato su KVM e supporto LXD (containers) per servizi interni OpenStack
- Networking basato su OpenVSwitch

**Cloud machine**:

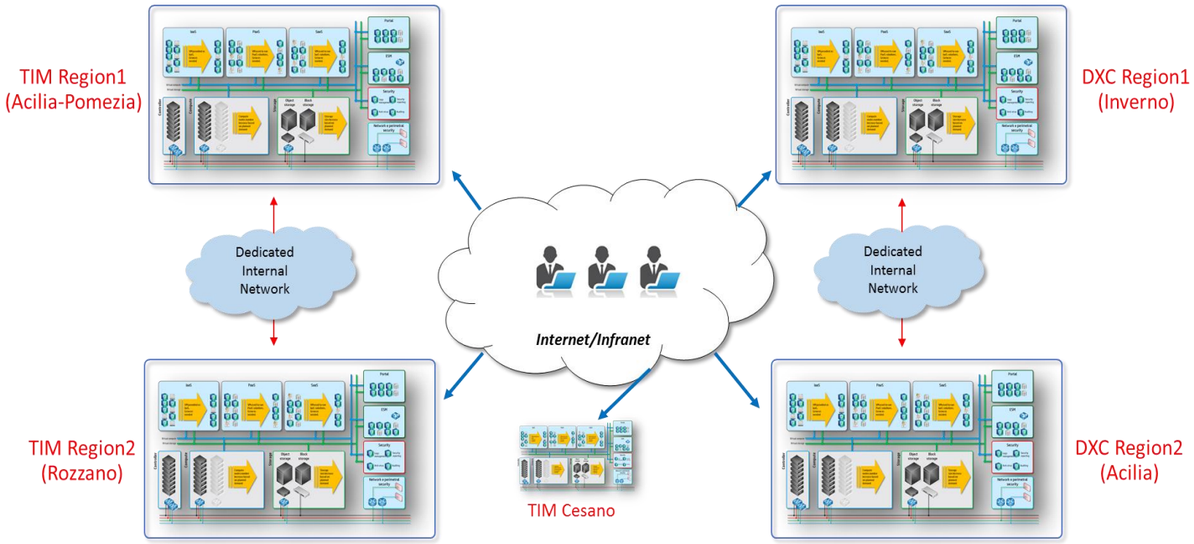
- Utilizzo di server rack con tecnologia convergente (compute+storage nodes)
- MaaS physical automation (bare metal provisioning)
- Service modeling basato su Juju
- Control plane con servizi incapsulati in Containers (LXD)
- Update nodi mediante Canonical Landscape
- DXC ha sviluppato una soluzione applicativa per gestire domini federati con autenticazione SAML2 e 2FA (integrabile con SPID)
- Creazione flavor privati da parte degli end user (domini + ad hoc policies)
- Visibilità privata delle immagini (domini + ad hoc policies)
- Supporto Ceph per block storage e Swift per object storage
- Backup configurazione piattaforma (tramite Juju)

# La piattaforma tecnologica

## Architettura e funzionalità della nuova piattaforma: multi-region

La nuova soluzione architetturale identificata aumenta l'affidabilità dei servizi e la continuità operativa mediante i seguenti elementi fondanti:

- abilitazione all'erogazione dei servizi SPC Cloud in **modalità multi-Region** che supportano servizi "Cloud nativi" con la predisposizione di Region **contemporaneamente attive**.
- re-ingegnerizzazione ed **evoluzione del Disaster Recovery** che per gli ambienti legacy non sarà più basato sull'intera piattaforma ma circoscritto ad ogni singolo progetto/tenant per scongiurare anche fault parziali
- Funzioni di *Fast Recovery* e *Always-on* dei servizi

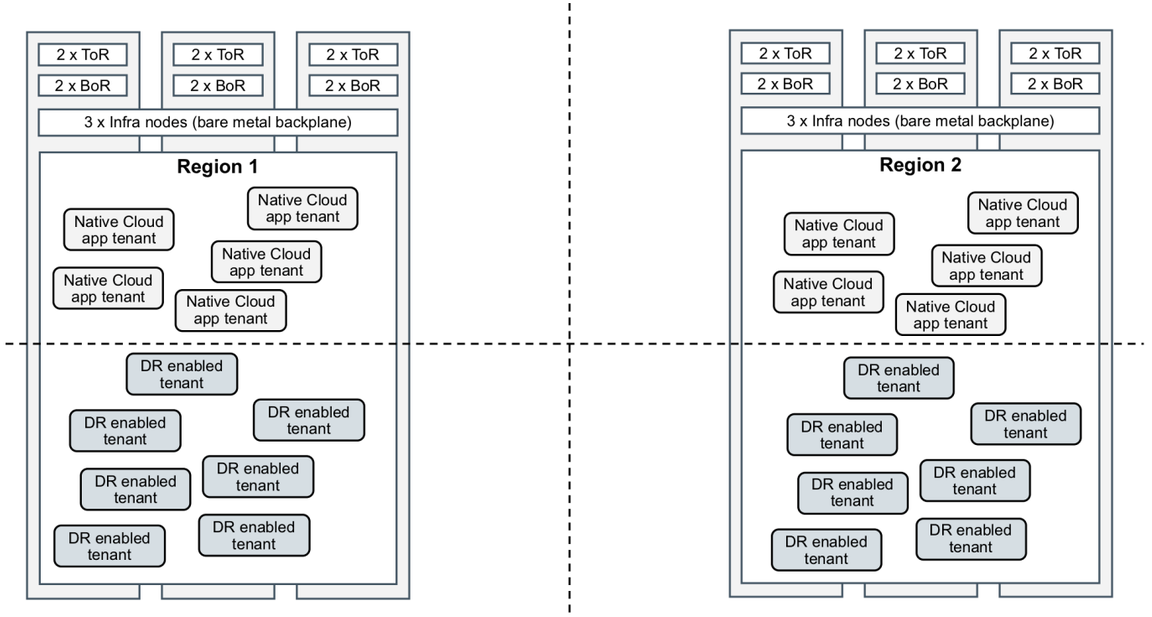



- **Fast Recovery**: funzionalità pienamente equivalente al DR ma realizzato a livello di tenant.
- **Always On**: funzionalità che è pienamente equivalente al BC (Business Continuity) ma che richiede una predisposizione delle applicazioni (applicazioni cloud native)

# La piattaforma tecnologica

## Utilizzo delle region: workloads post-legacy e applicazioni cloud native

- Ogni region è realizzata mediante un deployment auto consistente della piattaforma Canonical OpenStack attraverso le funzionalità fornite da Juju e LXD
- Dal punto di vista dell'utente finale le region OpenStack hanno funzionalità equivalenti a quelle dei principali Cloud Service Providers pubblici.
- L'implementazione delle region consente agli utenti di dislocare geograficamente i propri workload e di conseguenza avere la garanzia, in caso di problemi in una region, di poter accedere ai servizi ancora attivi sull'altra region; ovviamente per sfruttare appieno le funzionalità delle Region i servizi applicativi devono essere concepiti in modalità cloud nativa.
- Gli utenti usano le stesse credenziali di accesso alla piattaforma Cloud integrate con il two factor authentication system recentemente implementato (su richiesta AgID)



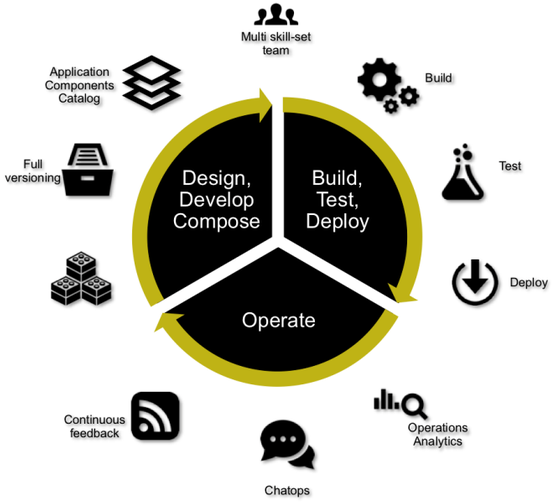

- In fase di attivazione di un tenant va definito il tipo di supporto in termini di recovery dei servizi: *fast-recovery* o *always-on* ed i tenant creati**,** nelle specifiche region, saranno predisposti adeguatamente.

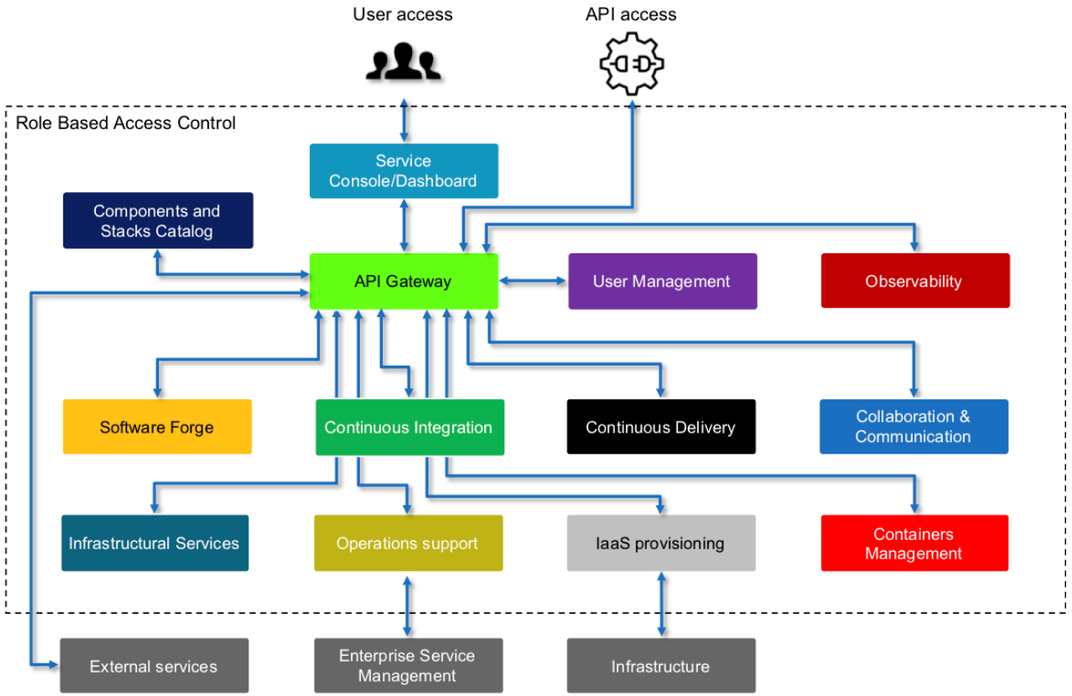
# Container DevOps Platform (ECaaS)

## Abilitazione al DevOps e microservizi con la tecnologia containers

Ad inizio 2017, insieme ad AgID e CONSIP è stato avviato il processo di ampliamento dei servizi disponibili (previsto dal capitolato) che ha portato a rendere disponibili ulteriori servizi tra cui, **Enterprise Container as a Service**

ECaaS è il servizio che fornisce una piattaforma DevOps completamente dedicata ad ogni cliente. Con questa soluzione è possibile gestire l'intero ciclo di vita di un servizio IT in modalità DevOps e sfruttando appieno la tecnologia container basta su Docker ee Kubernetes.

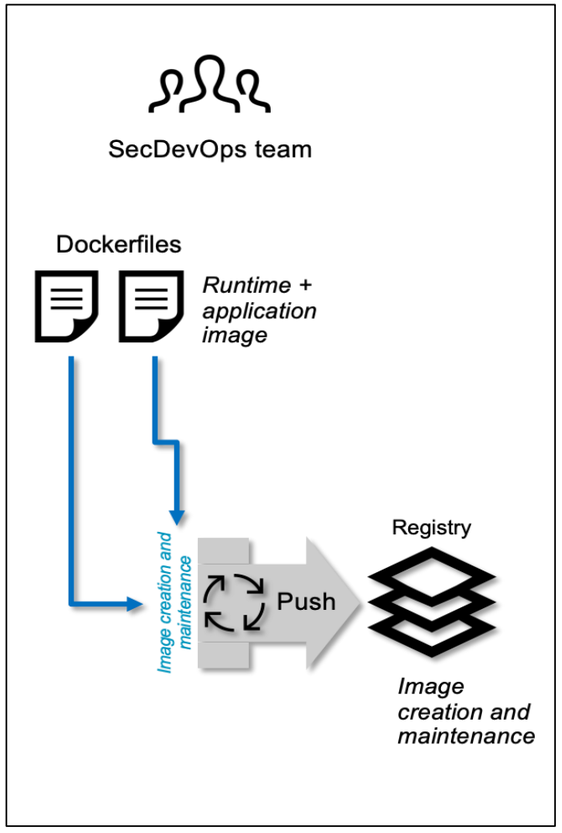


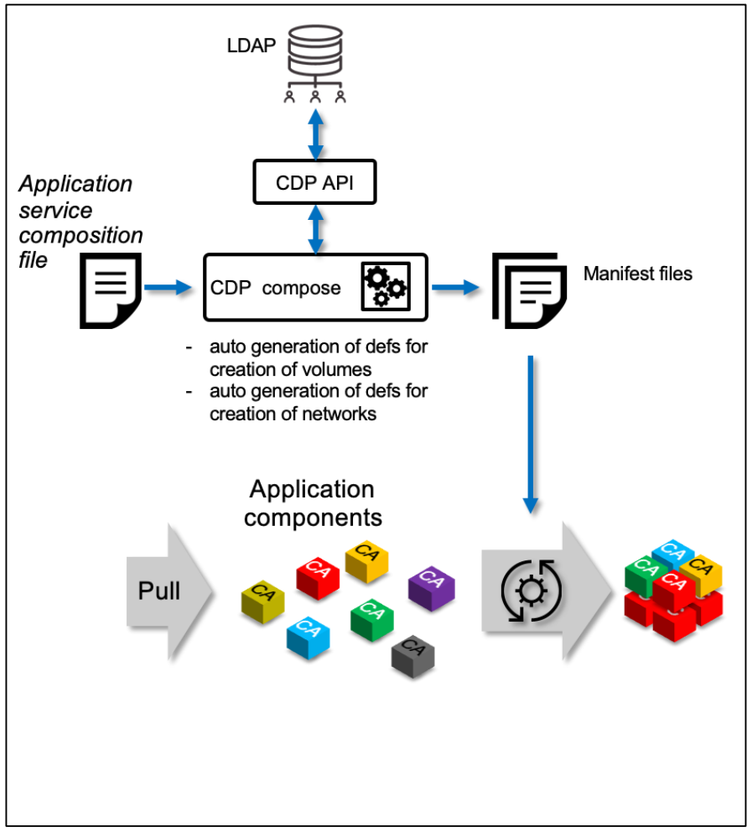

Ci sono già diverse entità della P.A. che usano questa soluzione tra cui: AgID, DFP, MIUR, ANPAL, INDIRE, Comune di Roma, Comune di Milano.

# Ciclo di vita di servizi IT stateful su cluster k8s

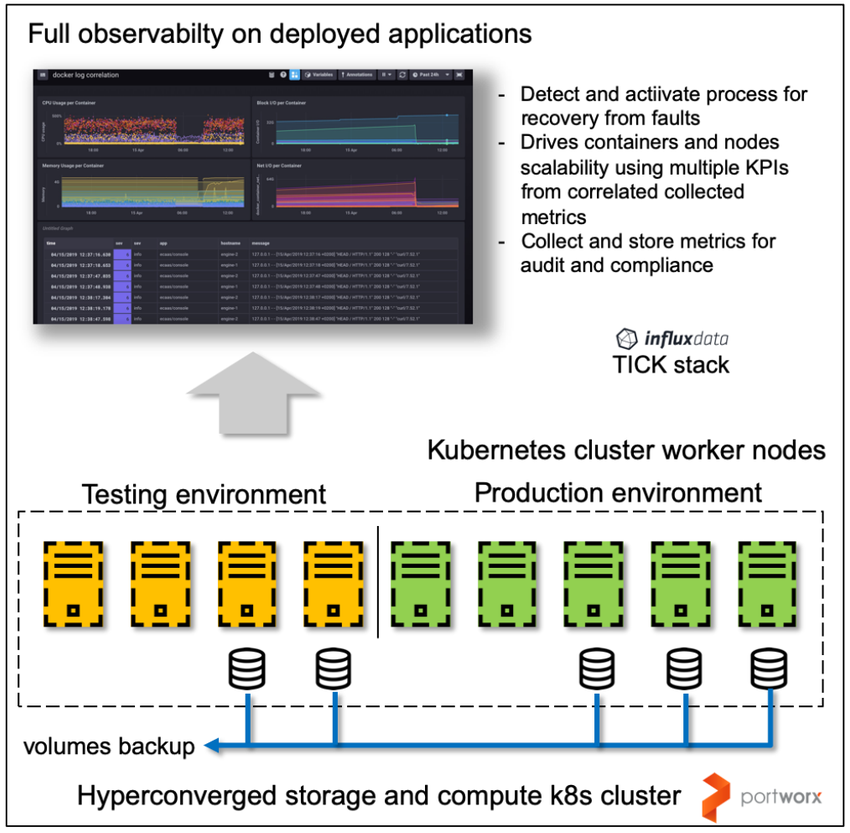
## Design, Develop Compose




## Build, Test, Deploy




## Operate (Monitor and Diagnose)




**Every software assets (config, definitions, scripts) stored in 'git' repos**

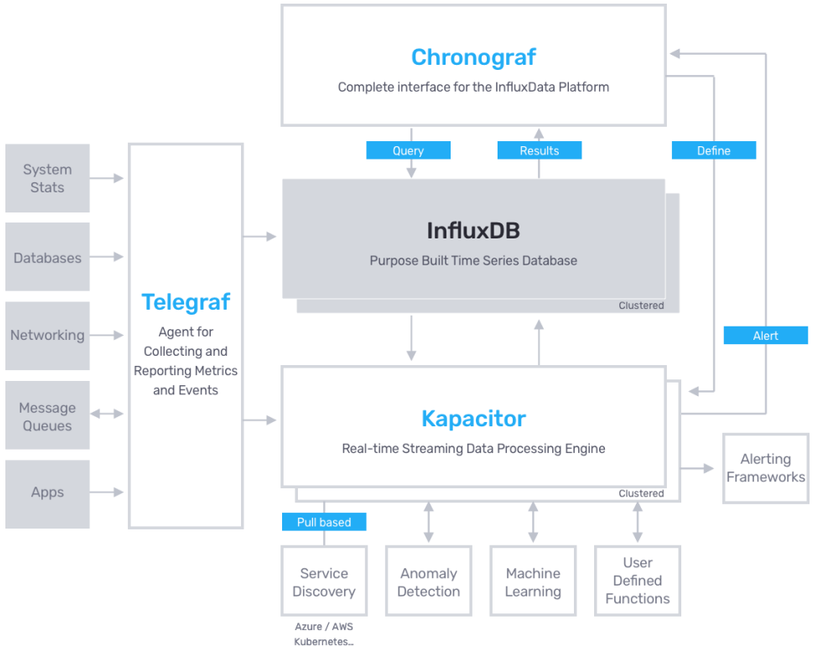
git

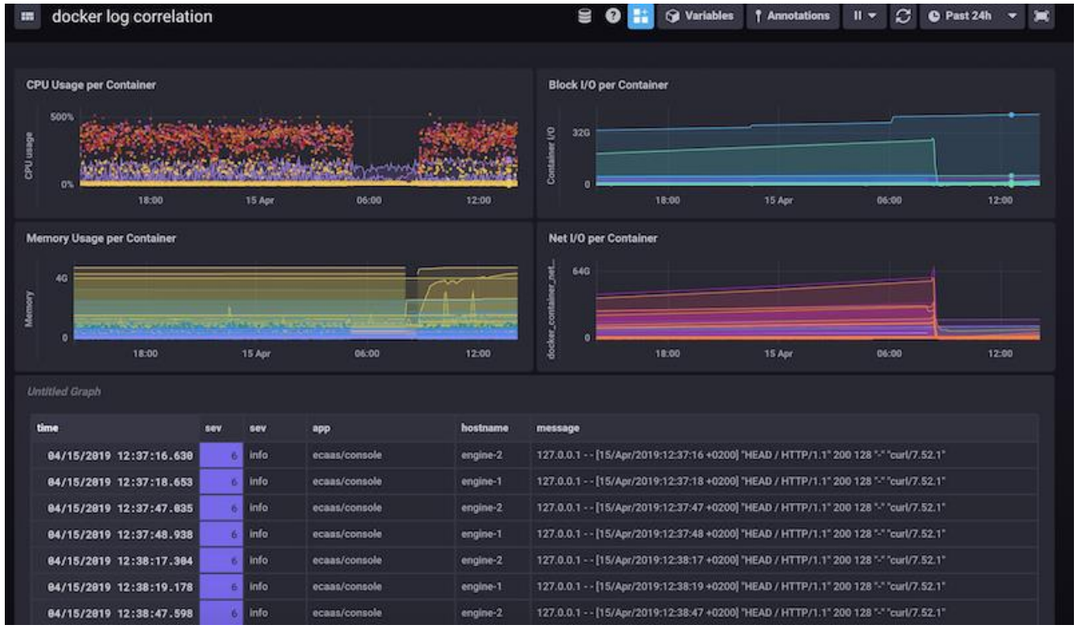
# Nuove funzionalità su CDP (ECaaS)

## Observability

**Obiettivo**: determinare lo stato di salute di un sistema [distribuito e complesso] dalla conoscenza di ciò che produce (output)

**Approccio**:  utilizzo di una soluzione open source, Influxdata TICK stack (Telegraf, InfluxDB, Chronograf and Kapacitor) + Jaeger (distributed tracing) che effettua correlazione disparate metriche, eventi, logs, ecc. indicizzati su base temporale (time-series DB), il tutto controllabile e fruibile tramite dashboard, CLI o API.



# QA