

|  |
| --- |
|  |
| **Crédit Agricole Group Solutions** |
| **Disegno Architetturale**  **Progetti Applicativi** |
|  |
| ***Applicazione: Openshift Container Platform***  ***Progetto: FREE***  ***RGP:* 4462** |
|  |

# Indice

[1 Indice 2](#_Toc163473576)

[2 Panoramica 4](#_Toc163473577)

[2.1 Ambito 4](#_Toc163473578)

[2.2 Versione 5](#_Toc163473579)

[2.3 Acronimi 7](#_Toc163473580)

[3 Architettura AS-IS 8](#_Toc163473581)

[3.1 Disegno Logico 8](#_Toc163473582)

[3.2 Descrizione Funzionale 8](#_Toc163473583)

[4 Architettura TO-BE, High level view 9](#_Toc163473584)

[4.1 Scopo del Progetto 9](#_Toc163473585)

[4.2 Obiettivi 9](#_Toc163473586)

[4.3 Assunzioni 9](#_Toc163473587)

[4.4 Vincoli 9](#_Toc163473588)

[4.5 Decisioni Architetturali 9](#_Toc163473589)

[4.6 Disegno Cartografico – INFO SU CMDB 11](#_Toc163473590)

[4.7 Disegno Logico 11](#_Toc163473591)

[5 Architettura TO-BE, Low level view 12](#_Toc163473592)

[5.1 Disegno Tecnologico 12](#_Toc163473593)

[5.1.1 Microservizi ambiente Sviluppo e Collaudo 12](#_Toc163473594)

[5.1.2 Microservizi ambiente Parallelo 13](#_Toc163473595)

[5.2 Microservizi ambiente Produzione 16](#_Toc163473596)

[5.3 Componenti Applicativi/Tecnologici 19](#_Toc163473597)

[5.3.1 Nodo Bastion 19](#_Toc163473598)

[5.3.2 Nodi Master 19](#_Toc163473599)

[5.3.1 Nodi Infra 20](#_Toc163473600)

[5.3.2 Nodi Storage (ODF) 20](#_Toc163473601)

[5.3.3 Nodi Worker 21](#_Toc163473602)

[5.3.4 REPO esterno Autorizzato 22](#_Toc163473603)

[5.4 API & Web Service 23](#_Toc163473604)

[5.5 Requisiti Infrastrutturali 23](#_Toc163473605)

[5.5.1 Ambiente di Sviluppo & Test 23](#_Toc163473606)

[5.5.2 Ambiente di Pre-Produzione 23](#_Toc163473607)

[5.5.3 Ambiente di Produzione 23](#_Toc163473608)

[5.5.4 Business Continuity - HA-Scalabilità-Resilienza 24](#_Toc163473609)

[5.6 Architettura Dati 25](#_Toc163473610)

[5.6.1 Note implementative 26](#_Toc163473611)

[5.6.2 Parametri di connessione 26](#_Toc163473612)

[5.7 Architettura di Rete 27](#_Toc163473613)

[5.7.1 Schema di rete 27](#_Toc163473614)

[5.7.2 Bilanciamento 27](#_Toc163473615)

[5.7.3 Note implementative 28](#_Toc163473616)

[5.8 Architettura di sicurezza 29](#_Toc163473617)

[5.8.1 Sistemi di protezione e autenticazione 29](#_Toc163473618)

[5.8.1 Utenze tecniche non nominative 30](#_Toc163473619)

[5.8.1 Protezione dati – INFO SU CMDB 31](#_Toc163473620)

[6 System Management 32](#_Toc163473621)

[6.1 Administration Console 32](#_Toc163473622)

[6.2 Change & Release Management 33](#_Toc163473623)

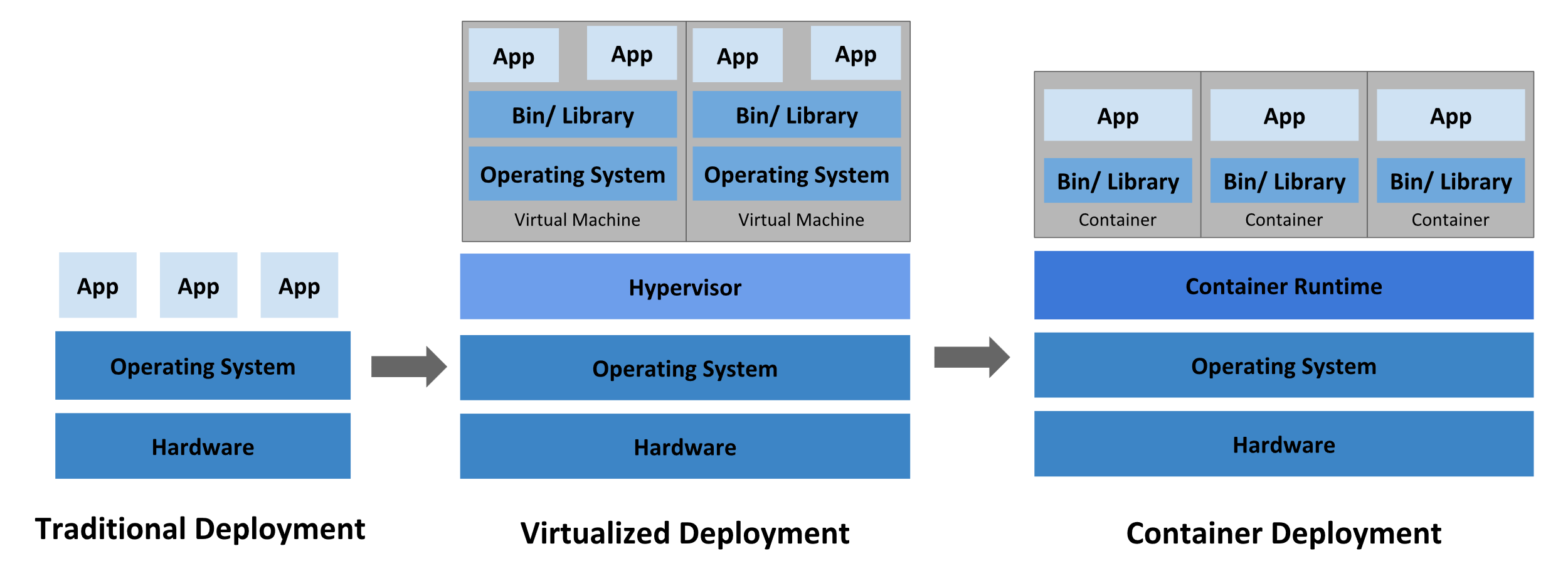
[6.3 Gestione dei Log 34](#_Toc163473624)

[7 Validazione 34](#_Toc163473625)

# Panoramica

## Ambito

Nel contesto dell’innovazione tecnologica e di una roadmap IT orientata alle architetture a microservizi e cloud native, CAGS ha individuato l’opportunità e la necessità di adottare una piattaforma tecnologica per il supporto di workload containerizzati. Tale necessità nasce dall’evoluzione del mondo IT verso un approccio a container e dalla tendenza a un maggiore utilizzo della virtualizzazione:



I container sono diventati popolari dal momento che offrono molteplici vantaggi, ad esempio:

* Creazione e distribuzione di applicazioni in modalità Agile: maggiore facilità ed efficienza nella creazione di immagini container rispetto all'uso di immagini VM.
* Adozione di pratiche per lo sviluppo/test/rilascio continuativo: consente la frequente creazione e la distribuzione di container image affidabili, dando la possibilità di fare rollback rapidi e semplici (grazie all'immutabilità dell'immagine stessa).
* Separazione delle fasi di Dev e Ops: le container image vengono prodotte al momento della compilazione dell'applicativo piuttosto che nel momento del rilascio, permettendo così di disaccoppiare le applicazioni dall'infrastruttura sottostante.
* L'osservabilità non riguarda solo le informazioni e le metriche del sistema operativo, ma anche lo stato di salute e altri segnali dalle applicazioni.
* Coerenza di ambiente tra sviluppo, test e produzione: i container funzionano allo stesso modo su un computer portatile come nel cloud.
* Portabilità tra cloud e sistemi operativi differenti: lo stesso container funziona su Ubuntu, RHEL, CoreOS, on-premise, nei più grandi cloud pubblici e da qualsiasi altra parte.
* Gestione incentrata sulle applicazioni: Aumenta il livello di astrazione dall'esecuzione di un sistema operativo su hardware virtualizzato all'esecuzione di un'applicazione su un sistema operativo utilizzando risorse logiche.
* Microservizi liberamente combinabili, distribuiti, ad alta scalabilità: le applicazioni sono suddivise in pezzi più piccoli e indipendenti che possono essere distribuite e gestite dinamicamente - niente stack monolitici che girano su una singola grande macchina.
* Isolamento delle risorse: le prestazioni delle applicazioni sono prevedibili.
* Utilizzo delle risorse: alta efficienza e densità

*OpenShift Container Platform* *con Kubernetes* è una soluzione completa per l'esecuzione di applicazioni containerizzate. È basato su Kubernetes, il sistema di orchestrazione dei container open source più popolare al mondo, e include una serie di funzionalità aggiuntive che semplificano lo sviluppo, la distribuzione e la gestione delle applicazioni containerizzate.

Alcune delle principali funzionalità di *OpenShift Container Platform con Kubernetes* sono:

* **Interfaccia utente web intuitiva**: la piattaforma fornisce un'interfaccia utente web intuitiva che consente agli sviluppatori e agli operatori di gestire le applicazioni containerizzate.
* **API RESTful**: la piattaforma fornisce un'API RESTful che consente agli sviluppatori di automatizzare le attività di gestione delle applicazioni containerizzate.

## Versione

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versione** | **Data** | **Autore** | **Progetto/PRJ** | **Modifiche** |
| 1.0 | 30/01/2024 | TA\_FREE\_ACN | FREE | Prima Stesura |
| 1.1 | 06/02/2024 | TA\_FREE\_ACN | FREE | Accesso a console amministrativa attraverso Cyberark |
| 1.2 | 29/02/2024 | TA\_FREE\_ACN | FREE | Integrazioni temi Sicurezza |
| 1.3 | 29/02/2024 | TA\_FREE\_ACN | FREE | Integrazioni temi sicurezza e Log |
| 1.4 | 29/02/2024 | TA\_FREE\_ACN | FREE | Modifica sessione Log per approfondimenti in corso |
| 1.5 | 14/03/2024 | TA\_FREE\_ACN | FREE | Integrazione DDS Parallelo |
| 1.6 | 19/03/2024 | TA\_FREE\_ACN | FREE | Integrazione DDS Parallelo con regole FW parallelo |
| 1.7 | 19/03/2024 | TA\_FREE\_ACN | FREE | Modifica disegno ACM Parallelo Temporaneo e integrazione nodi ODF in collaudo |
| 1.8 | 21/03/2024 | TA\_FREE\_ACN | FREE | Integrazione link alerta in conf proxy server |
| 1.9 | 05/04/2024 | TA\_FREE\_ACN | FREE | Integrazione Produzione |

Tabella 1, Elenco delle versioni del documento

## Acronimi

|  |  |
| --- | --- |
| **Acronimi** | **Descrizione** |
| RPC | Remote Procedure Call |
| RTO | Recovery Time Objective |
| RPO | Recovery Point Objective |
| AAA | Authentication, Authorization and Accounting |
| ACL | Access Control List |
| ACS | Access Control Server |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| IP | Internet Protocol |
| LAN | Local Area Network |
| BPM | Business process management |
| SDU | Sistema documentale unico |
| OCP | Openshift Container Platform |
| IPI | Installer Provisioned Infrastructure |
| ODF | OpenShift Data Foundation |

Tabella 2, Elenco acronimi utilizzati nel documento.

# Architettura AS-IS

## Disegno Logico

N.A.

## Descrizione Funzionale

N.A.

# Architettura TO-BE, High level view

## Scopo del Progetto

Nel contesto dell’innovazione tecnologica e di una roadmap IT orientata alle architetture a microservizi e cloud native, CAGS ha individuato l’opportunità e la necessità di adottare una piattaforma tecnologica per il supporto di workload containerizzati.

In prima fase, la piattaforma in questione è stata predisposta per tutte le attività legate al progetto FREE, a supporto delle applicazioni di FE.

--------------------------------------------------------------------------------------------------

Nuovo progetto/soluzione

Evoluzione progetto/soluzione esistente

--------------------------------------------------------------------------------------------------

## Obiettivi

Gli obiettivi dell’implementazione della piattaforma *Red Hat* *Openshift Container Platform con Kubernetes* (nel seguito OCP) sono:

* Adozione di paradigma a container per lo sviluppo di applicazioni di frontend, backend e micro-gateway;
* Implementazione di un approccio cloud-native allo sviluppo delle applicazioni di proprietà CAGS.

## Assunzioni

La piattaforma scelta per l’implementazione di architettura a microservizi containerizzati è *Red Hat* *Openshift Container Platform* con Kubernetes in quanto leader IT e di mercato, nonché piattaforma indicata dalla capogruppo quale preferenziale.

## Vincoli

N.A.

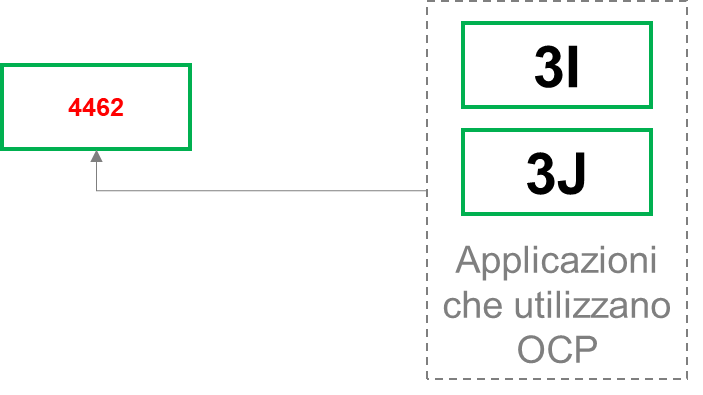
## Decisioni Architetturali

Le principali decisioni architetturali sono le seguenti:

* I change e le release degli applicativi che utilizzano la piattaforma OCP saranno effettuati tramite DevOps, per garantire agilità e una più semplice gestione operativa, che sarebbe altrimenti complicata data la natura distribuita dei sistemi in ambito;
* Utilizzo di Quay come Registry di OCP per ogni ambiente.
  + Per l’ambiente di sviluppo e collaudo, è utilizzato temporaneamente il DTR di Mirantis già presente in CAGS. In target per l’ambiente di sviluppo e collaudo esisterà componente Quay su cluster Openshift. La componente Quay sarà installata come Operator dedicato su nodi Infra. Come Backing Storage si utilizzerà l’ODF configurato sui Cluster Openshift di Collaudo.
  + Per gli ambienti di Parallelo e Produzione la componente Quay sarà installata come Operator sui nodi Infra per essere utilizzati solo per push/pull delle immagini. Come Backing Storage si utilizzerà l’ODF installato sui nodi “storage” del Cluster Openshift di Parallelo e Produzione, rispettivamente.
* Utilizzo di Hub Cluster (ACM) come gestione dei cluster OCP di tutti gli ambienti. In termini di Timeline l’installazione dei Cluster - per gestione di tutti gli ambienti - avverrà tra fine costruzione Parallelo e inizio predisposizione Produzione. Inoltre:
  + Per l’ambiente di Parallelo in via del tutto temporanea si installerà cluster ACM. L’ACM in questione sarà utilizzato per automatizzare e velocizzare l’installazione dei Cluster Openshift di Parallelo.
* I cluster OCP/Quay, Hub Cluster saranno installati con il metodo IPI.
* Per gli ambienti di Parallelo e Produzione il ruolo di DHCP non sarà configurato sul nodo Bastion. Dovranno essere rilasciati due nodi windows in HA e in configurazione di DHCP sulla subnet segregata di Openshift.
* Le versioni delle componenti infrastrutturali, qui considerate, sono le seguenti:

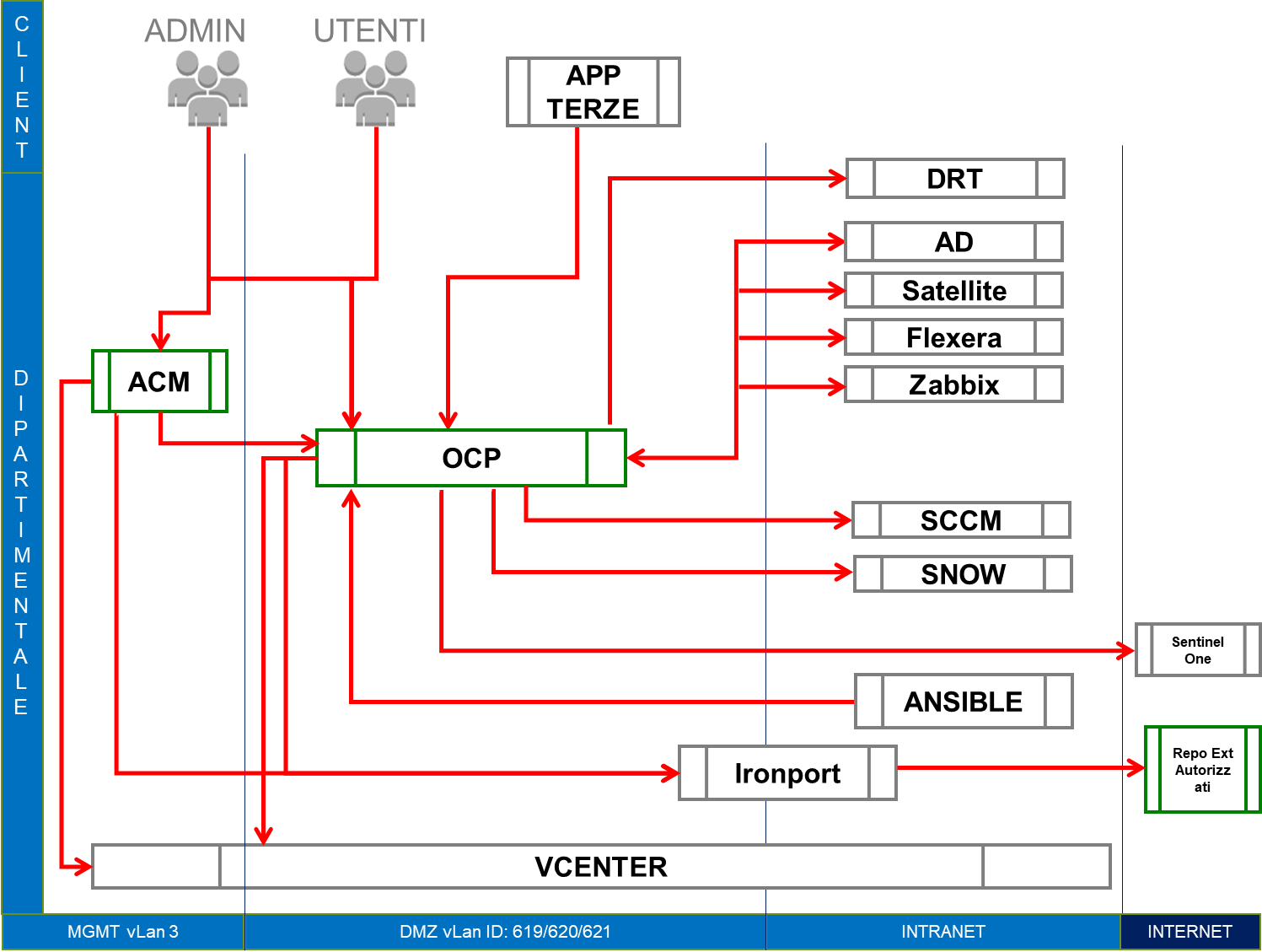
|  |  |
| --- | --- |
| ITEM | VERSIONE |
| Sistema Operativo | RHEL 8.6 |
| Cluster OCP | 4.14.2 |
| Kubernetes | 1.27.6+f67aeb3 |
| ServiceMesh | Red Hat Openshift Service Mesh 2.4.5 |

## Disegno Cartografico – INFO SU CMDB



La lista delle relazioni è ivi presente su CMDB.

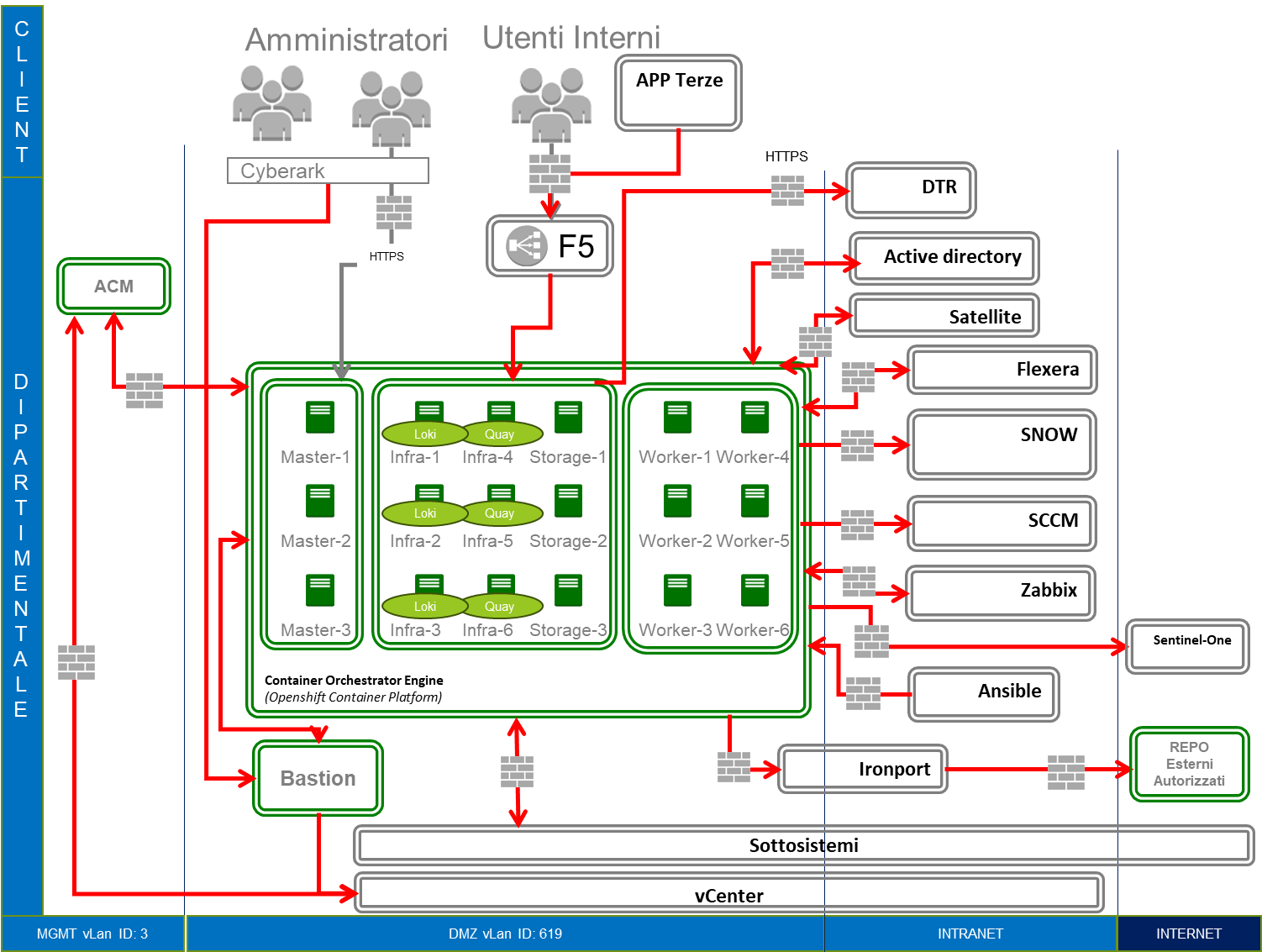
## Disegno Logico



# Architettura TO-BE, Low level view

## Disegno Tecnologico

### Microservizi ambiente Sviluppo e Collaudo

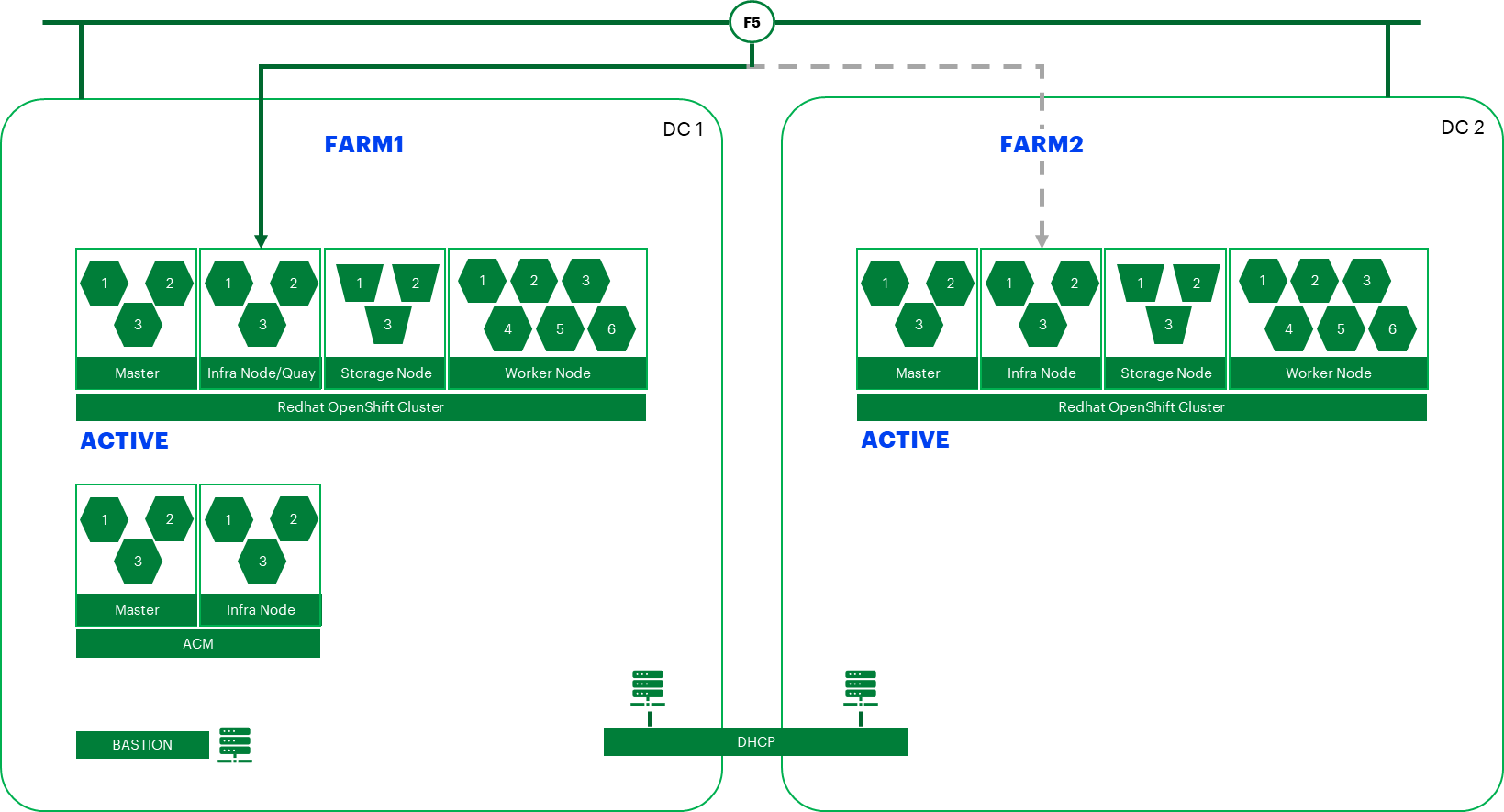


Qui di seguito uno schema dei nodi rappresentati nel diagramma:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HOSTNAME | Ruolo | S.O. | CPU | RAM | DISK | Dominio | vLan |
| grpi-ocp-kv00.cariprpccoll.it | Bastion Host | RHEL 8.6 | 4 | 4 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-master-0 | master | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-master-1 | master | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-master-2 | master | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-infra-0-2jxwk | infra | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-infra-0-czghd | infra | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-infra-0-gxb57 | infra | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-storage-0-7q264 | Infra ODF | RHEL CoreOS rel. 4.14 | 10 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-storage-0-bhlbp | Infra ODF | RHEL CoreOS rel. 4.14 | 10 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-storage-0-rqg69 | Infra ODF | RHEL CoreOS rel. 4.14 | 10 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-worker-0-8jkjr | worker | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-worker-0-gn5hn | worker | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-worker-0-q4mhl | worker | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-worker-0-q6q9j | worker | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-worker-0-vzt6w | worker | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |
| ocp-collaudo-jn6wt-worker-0-x9rlj | worker | RHEL CoreOS rel. 4.14 | 8 | 32 GB | 120 GB | .cariprpccoll.it | 619 |

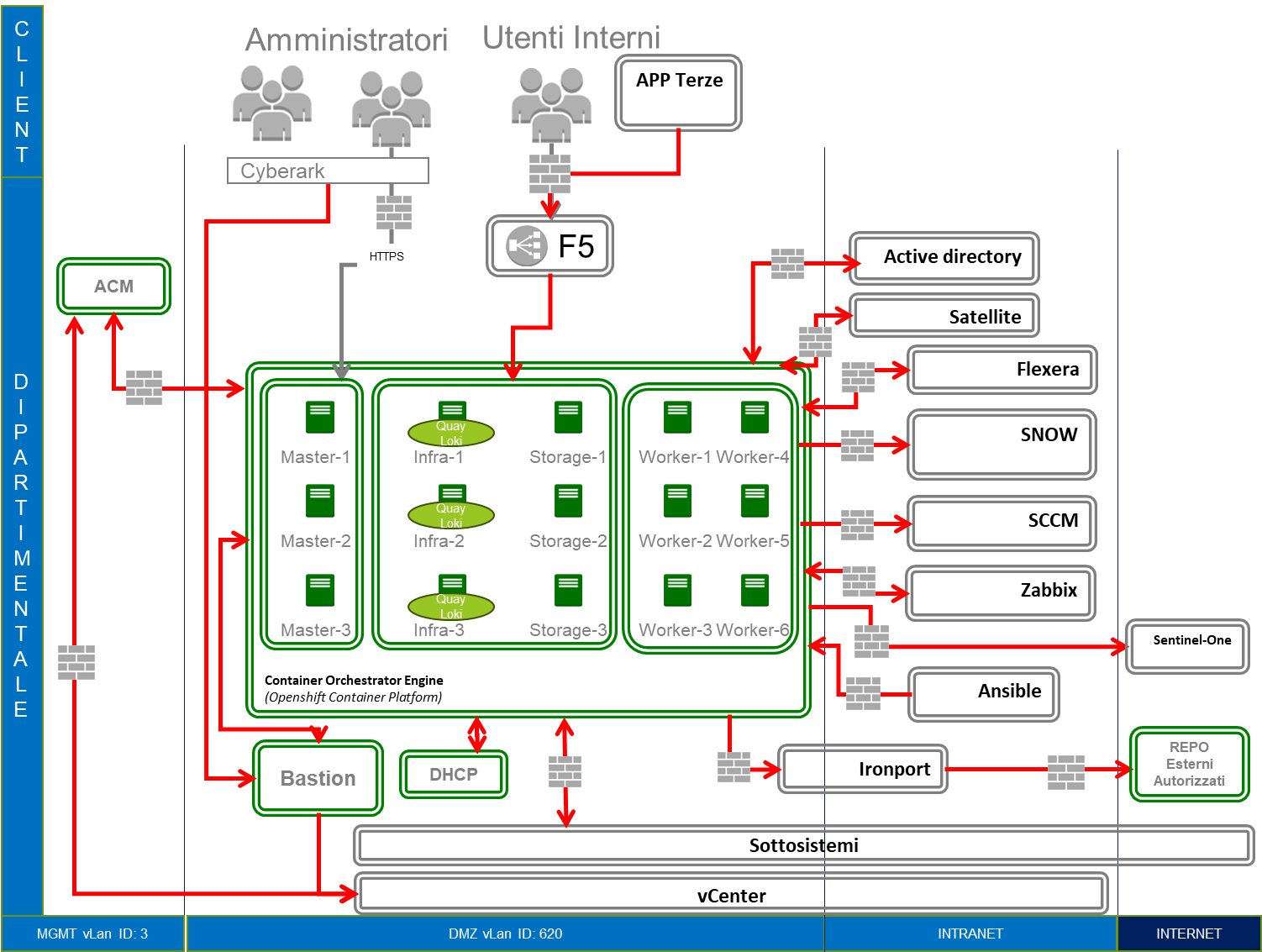
### Microservizi ambiente Parallelo

Su ambiente di Parallelo il Cluster Openshift è presente su doppio cluster: su data center di Acilia e su data center di Rozzano. Il cluster di ACM sarà installato su Datacenter Acilia.

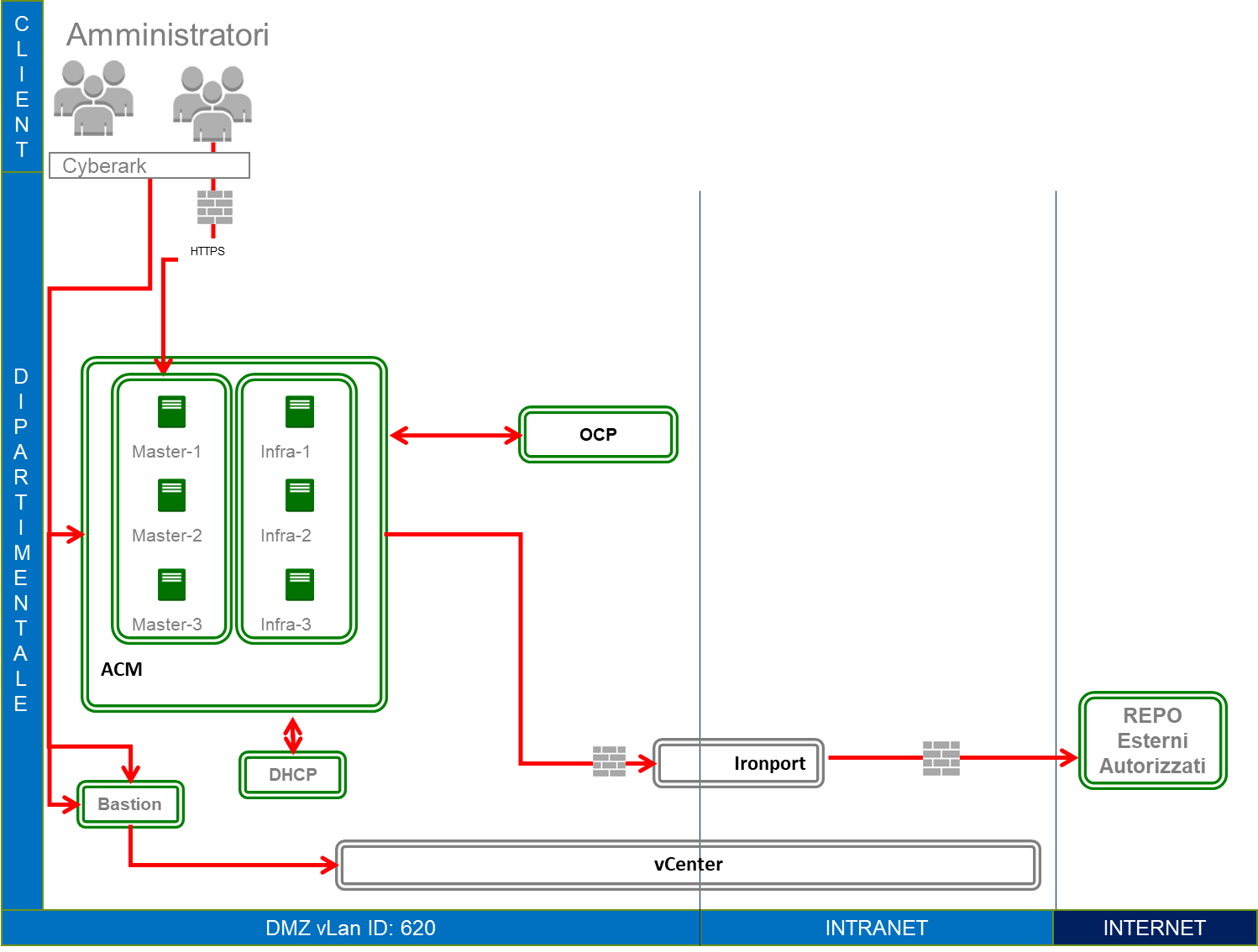


Le rappresentazioni qui di seguito illustrano rispettivamente solo uno dei due cluster Openshift, poiché essi sono speculari e identici, ma su farm diverse.

**Cluster Openshift Parallelo**

****

**Cluster ACM Parallelo (Temporaneo)**



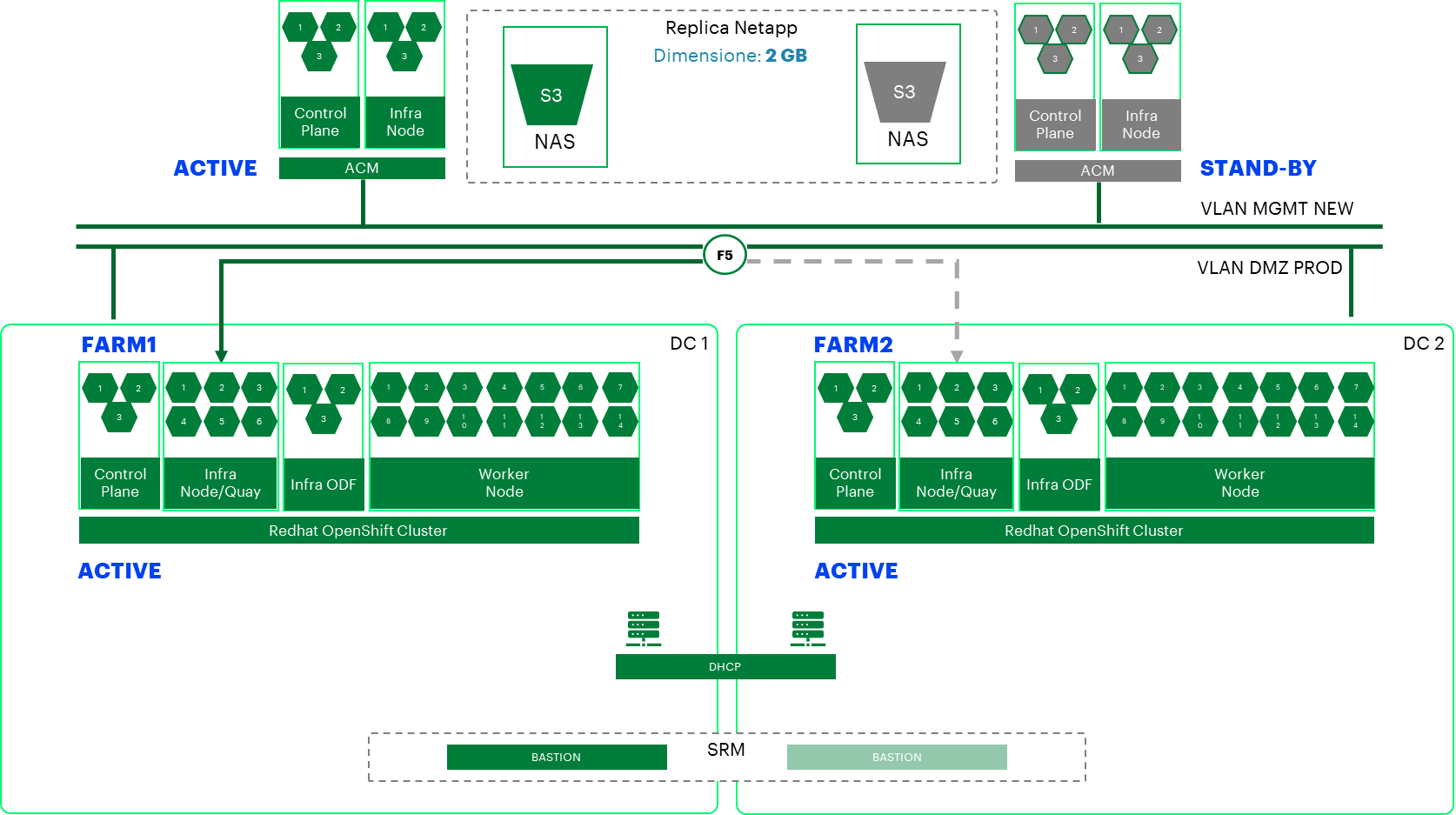
Qui di seguito uno schema dei nodi rappresentati nel diagramma:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HOSTNAME | Ruolo | S.O. | CPU | RAM | DISK | Dominio | vLan |
| GRPI-OCP-HV00.cariprpcpar.it | Bastion Host | RHEL 9.2 | 4 | 4 GB | 120 GB | cariprpcpar.it | 620 |
| GRPI-OCP-HV01.cariprpcpar.it | DHCP | Microsoft Windows Server 2022 | 4 | 8 | 120 | cariprpcpar.it |  |
| GRPI-OCP-HV02.cariprpcpar.it | DHCP | Microsoft Windows Server 2022 | 4 | 8 | 120 | cariprpcpar.it |  |
| ocp-parallelo-6lnrk-master-0 | Master-ACM | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp-parallelo-6lnrk-master-1 | Master-ACM | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp-parallelo-6lnrk-master-2 | Master-ACM | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp-parallelo-6lnrk-infra-0-vckgg.cariprpcpar.it | Infra-ACM | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp-parallelo-6lnrk-infra-0-k22pr.cariprpcpar.it | Infra-ACM | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp-parallelo-6lnrk-infra-0-2brpn.cariprpcpar.it | Infra-ACM | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-master-0 | Master | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-master-1 | Master | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-master-2 | Master | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-odf-0-5ptzd | ODF | RHEL CoreOS rel. 4.14 | 16 | 32 | 120  1000 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-odf-0-9kf59 | ODF | RHEL CoreOS rel. 4.14 | 16 | 32 | 120  1000 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-odf-0-q76tw | ODF | RHEL CoreOS rel. 4.14 | 16 | 32 | 120  1000 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-infra-0-cmr7g | Infra | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-infra-0-dbh5b | Infra | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-infra-0-xw5mb | Infra | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-worker-0-6n5kg | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-worker-0-74rd5 | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-worker-0-bjh8b | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-worker-0-lvkwt | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-worker-0-w6cgg | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp1-parallelo-6ldrf-worker-0-whwzp | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo-TBD-master-0 | Master | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -master-1 | Master | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -master-2 | Master | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -odf-0- TBD | ODF | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -odf-0- TBD | ODF | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -odf-0- TBD | ODF | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -infra-0- TBD | Infra | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -infra-0- TBD | Infra | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -infra-0- TBD | Infra | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -worker-0- TBD | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -worker-0- TBD | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -worker-0- TBD | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -worker-0- TBD | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -worker-0- TBD | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |
| ocp2-parallelo- TBD -worker-0- TBD | Worker | RHEL CoreOS rel. 4.14 | 16 | 32 | 120 | cariprpcpar.it | 620 |

## Microservizi ambiente Produzione

Nel seguente paragrafo si farà riferimento all’architettura dei Cluster Openshift di Produzione; in particolare in tale ambiente saranno presenti:

* Due Cluster Openshift, uno su data center di Acilia e uno su data center di Rozzano.
* Due Cluster di ACM, uno su data center di Acilia e uno su data center di Rozzano.

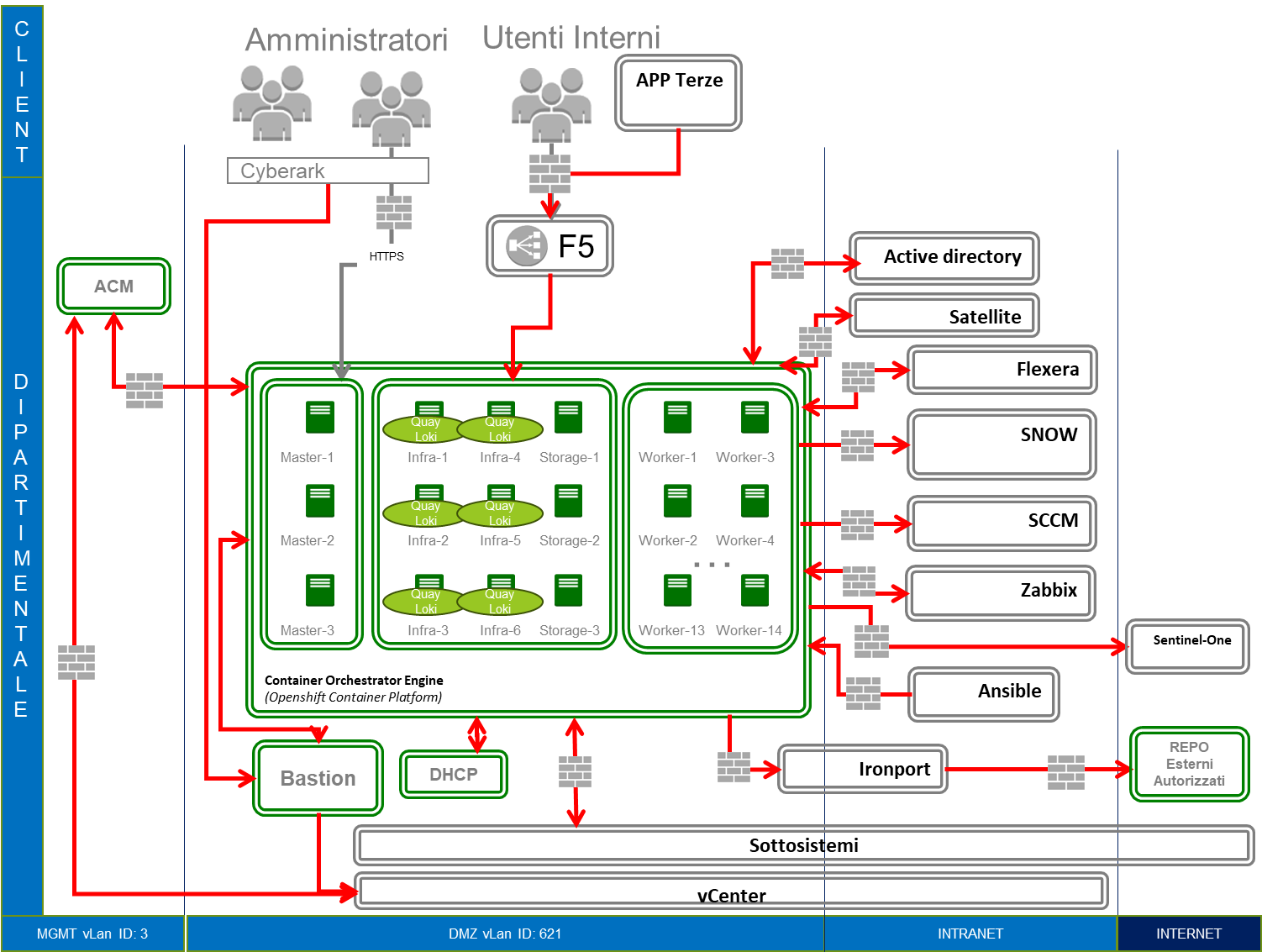


Le rappresentazioni qui di seguito illustrano rispettivamente solo uno dei due cluster Openshift, poiché essi sono speculari e identici, ma su farm diverse.

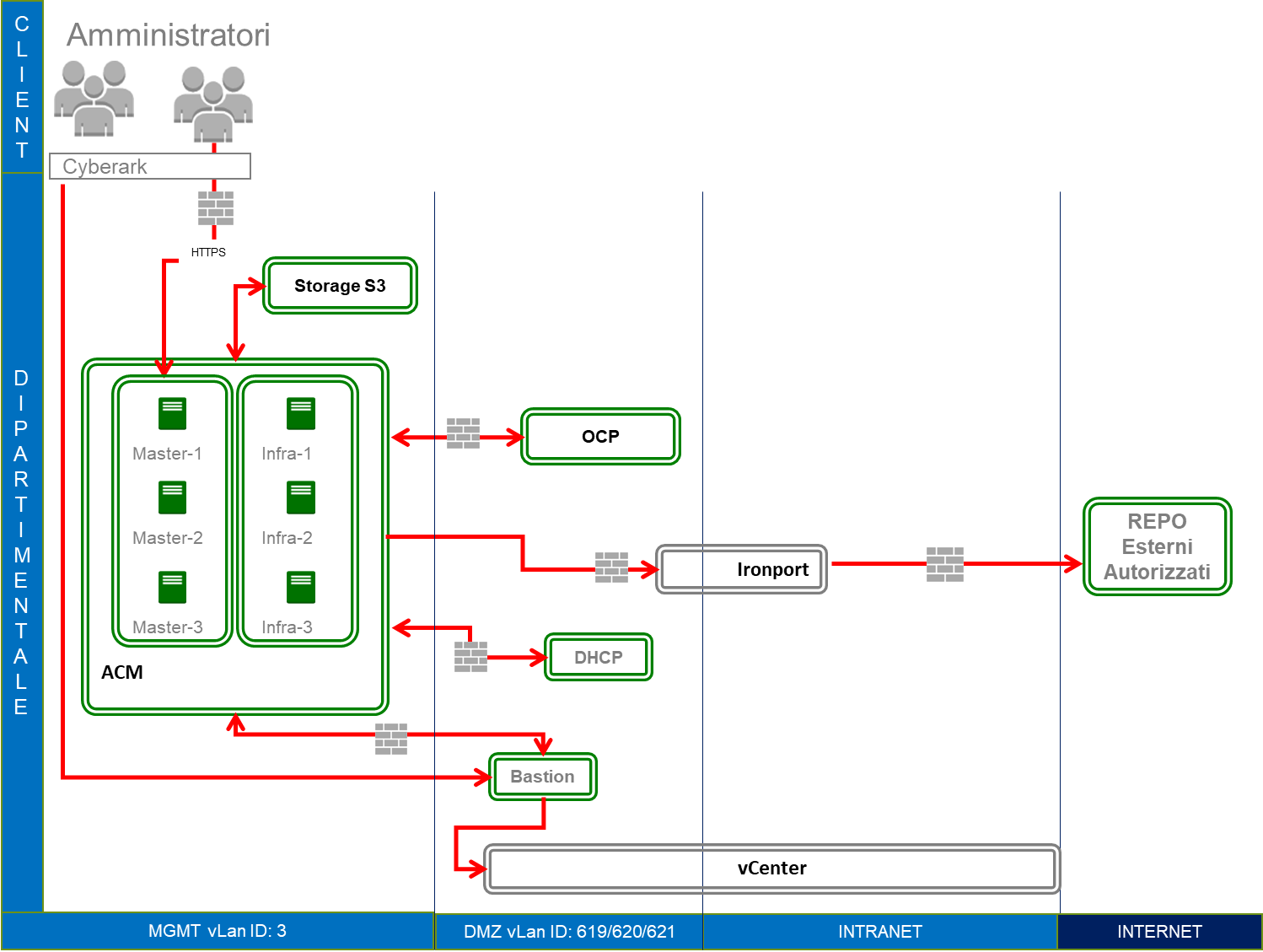
Rispettivamente le vLan di MGMT NEW e vLan di erogazione saranno:

* *vLan 3* - 192.168.248.0/22
* *vLan 621* - 10.215.88.0/24

**Cluster Openshift Produzione**



**Cluster ACM**



## Componenti Applicativi/Tecnologici

I componenti tecnologici riportati in questa sezione fanno riferimento ai componenti cluster della piattaforma OCP.

### Nodo Bastion

Il nodo bastion host assume il ruolo di punto di ingresso per l'autenticazione agli altri nodi presenti all'interno del cluster OCP.

Gli amministratori e gli operatori, attraverso la connessione al nodo bastion host, ottengono l'accesso autorizzato per la gestione e l'amministrazione degli altri nodi del cluster.

In collaudo il nodo Bastion assume anche il ruolo di DHCP, diversamente negli altri ambienti di Parallelo e Produzione ci saranno due VM presenti sulle nuove vLan e configurate in HA.

### Nodi Master

I nodi master all’interno della piattaforma di OCP svolgono il ruolo di control plane, gestendo il cluster.

In particolare, di seguito una breve descrizione delle principali responsabilità dei master node:

* **Gestione del Cluster:**

I master node sono responsabili della gestione complessiva del cluster OpenShift. Coordinano e controllano le attività dei nodi worker, assicurando che le applicazioni vengano distribuite ed eseguite correttamente.

* **Etcd**:

Ogni master node ospita un'istanza di etcd, un datastore distribuito e consistente. Etcd memorizza in modo affidabile la configurazione del cluster e lo stato complessivo del sistema, garantendo la coerenza delle informazioni tra tutti i nodi del master.

* **Comunicazione con Nodi Worker:**

I master node comunicano con i nodi worker per distribuire applicazioni, monitorare lo stato e coordinare le attività.

Ogni cluster OCP, da best practice di Red Hat, deve contenere almeno 3 Master Node. Per la predisposizione infrastrutturale dei nodi master e come richiesto da best practice RedHat, ciascun Master Node deve essere posizionato su un host fisico separato.

In CAGS, dunque, sono state predisposte regole di affinity (OCP\_Separate\_Master) sui nodi ESXi dedicati alla piattaforma.

### Nodi Infra

Gli infra node sono utilizzati per i servizi infrastrutturali specializzati. Nel dettaglio, i nodi infra di OCP ospitano i servizi aggiuntivi:

* “Istio” (service mesh) utilizzato per gestione del traffico verso i Worker node e Kiali utilizzata come sua console grafica.
* Prometheus e Grafana utilizzati in combinazione per il monitoraggio e la visualizzazione delle prestazioni applicative (in valutazione).
* Kibana/ Elasticsearch utilizzati in combinazione per la gestione dei log applicativi (in valutazione).
* Loki è la componente che:
  + Raccoglie e archivia i log da container e altri componenti OpenShift
  + Fornisce un'interfaccia per la query e la visualizzazione dei log.
* Quay è la componente installata per utilizzo di registry delle immagini.

Nota:

Per preservare a meglio la distribuzione dei nodi infra sono state predisposte regole di Affinity sui nodi ESXi dedicati alla piattaforma (ocp\_<ambiente>\_infra).

### Nodi Storage (ODF)

Gli storage node sono utilizzati come nodi che ospitano la componente ODF.

L’ODF è la componente RH per l'archiviazione dati su OpenShift, incluso un servizio di archiviazione oggetti compatibile con S3.

In CAGS sarà adottata per necessità di utilizzo, su ambiente On Prem, di Storage di tipologia S3 per l’installazione di Loki e Quay.

Nel dettaglio gli storage di tipologia S3 supportati in Openshift sono:

* Per Loki: AWS, Azure, Google Cloud, Minio, ODF, Swift
* Per Quay: AWS, Azure, Google Cloud, Ceph Object Gateway, OpenStack Swift (ODF), CloudFront + s3, NooBaa S3

Nota:

Per preservare a meglio la distribuzione dei nodi ODF sono state predisposte regole di Affinity sui nodi ESXi dedicati alla piattaforma (ocp\_<ambiente>\_odf).

### Nodi Worker

I worker node sono i nodi che erogano servizio e su cui girano le applicazioni. Di fatto ospitano i workload eventualmente in istanze replicate (pod).

I worker node sono orchestrati e gestiti dai nodi master, anche attraverso la console OCP.

All’interno dei nodi worker saranno presenti, al fine di garantire gli standard di sicurezza CAGS, per ogni nuova applicazione 3 differenti namespace front-end, back-end e micro-gateway (ove necessario).

Qualsiasi applicazione ospitata sul cluster OCP, dunque, dovrà utilizzare i 3 differenti namespace, basandosi sulla seguente naming convention:

A screen shot of a cell phone

Description automatically generated

A titolo di esempio e per dettagli applicativi si può far riferimento alle applicazioni attualmente ospitate su cluster OCP (3i e 3j).

La comunicazione tra namespace è permessa di default, tuttavia in Openshift Platform può esserci anche segregazione tra differenti namespace.

Tale segregazione dovrà avvenire attraverso:

* *Istio Policy 🡪* 
  + Le principali componenti di una network policy sono:
    - Nome: Identifica la Network Policy.
    - Namespace: Specifica a quale namespace si applica la Network Policy.
    - Regole di rete: Definiscono il flusso di traffico consentito.
  + La modalità per l’applicazione delle Istio Policy sarà quella di settare una authorization policy di *Deny-All* tra tutti i namespace applicativi e applicare configurazioni puntuali tra i namespace per cui è permessa la comunicazione.
  + Le Istio Policy possono essere configurate utilizzando diverse modalità:
    - Console di Kiali: è possibile utilizzare la console di Istio per creare e gestire le Istio Policy.
    - File YAML: È possibile definire le policy in file YAML e quindi applicarle utilizzando il comando istioctl apply.

Qualsiasi comunicazione tra APP Terze e Openshift dovrà avvenire considerando i seguenti due punti:

* Aperture di rete da e verso l’intera vLan della piattaforma di Openshift (segregata) - 10.215.86.0/24; 10.215.87.0/24; 10.215.88.0/24 (Collaudo; Parallelo; Produzione) con porte e protocolli dedicati.
* Le regole dovranno essere definite a livello applicativo e nei vari DDS applicativi. A titolo di esempio e per dettagli applicativi si può far riferimento alle applicazioni attualmente ospitate su cluster OCP (3i e 3j).

### REPO esterno Autorizzato

I repo esterni autorizzati rappresentano gli insiemi dei siti richiesti da OCP; in generale prima di installare OpenShift Container Platform, è necessario configurare il firewall per garantire l'accesso ad essi.

Le regole Firewall in CAGS sono da intendersi da OCP verso il vip per “proxy navigazione server” (vip-navproxy-server.cariprpc.it). Le rotte dei siti sono direttamente configurate sul proxy.

## API & Web Service

Trattandosi di disegno tecnologico, non sono presenti API applicative da riportare.

## Requisiti Infrastrutturali

### Ambiente di Sviluppo & Test

I requisiti infrastrutturali sono dettagliati nell’allegato di seguito riportato:



### Ambiente di Pre-Produzione

I requisiti infrastrutturali sono dettagliati nell’allegato di seguito riportato:



### Ambiente di Produzione

I requisiti infrastrutturali sono dettagliati nell’allegato di seguito riportato:



### Business Continuity - HA-Scalabilità-Resilienza

|  |  |  |  |
| --- | --- | --- | --- |
| **Evento** | **Tipo di Evento** | **Tipo di soluzione per la BC** | **Tipo di soluzione per il Recovery** |
| Failure Cluster ACM | Failure Cluster ACM | Qualsiasi Cluster di Openshift è scalabile nativamente. | Switch del Cluster attraverso attivazione o disattivazione del cluster in stand by verso Datacenter secondario. |
| Failure Cluster Openshift/Quay | Failure Cluster Openshift | Qualsiasi Cluster di Openshift è scalabile nativamente. | Switch del Cluster attraverso attivazione o disattivazione dei pool dei vip di F5. I pool conterranno i nodi infra dei due Cluster di Openshift sui differenti Datacenter.  Durante lo switch sul nuovo Cluster di Rozzano i log del Cluster di Acilia non saranno consultabili. |

Tabella 10, Elenco dei possibili eventi con le relative soluzioni

## Architettura Dati

N.A.

### Note implementative

N.A.

### Parametri di connessione

N.A.

STANDARD ARCHITETTURALE

1. Allinearsi con il Team Sistemi per applicare politiche di svecchiamento
2. E’ possibile l’introduzione di nuove famiglie DB in relazione alle necessità del progetto ed all’evoluzione tecnologica. In tal caso è necessario allinearsi con team Architetture.

## Architettura di Rete

Di seguito sono riportati i dettagli relativi alle aperture regole FW per ogni ambiente.

****

### Schema di rete

L’Architettura OCP con Kubernetes installata in modalità IPI ha necessità di una vLan dedicata per ogni ambiente, che sarà estesa su Host dedicati, verso F5 e verso componenti standard di infrastruttura su altre vLan (es. NTP, DNS, AD, zabbix, satellite, flexera, SNOW, SCCM, sentinel one, proxy ironport).

Ciascuna nuova vLan (di ogni ambiente: sia esso Collaudo, Parallelo, Produzione, Management) necessita di abilitazione, lato Ironport, verso le seguenti destinazioni:

* registry.redhat.io
* access.redhat.com
* quay.io
* cdn.quay.io
* cdn01.quay.io
* cdn02.quay.io
* cdn03.quay.io
* sso.redhat.com
* cert-api.access.redhat.com
* api.access.redhat.com
* infogw.api.openshift.com
* console.redhat.com/api/ingress
* console.redhat.com/openshift
* mirror.openshift.com
* storage.googleapis.com/openshift-release
* quayio-production-s3.s3.amazonaws.com
* api.openshift.com
* rhcos.mirror.openshift.com
* registry.connect.redhat.com
* rhc4tp-prod-z8cxf-image-registry-us-east-1-evenkyleffocxqvofrk.s3.dualstack.us-east-1.amazonaws.com
* oso-rhc4tp-docker-registry.s3-us-west-2.amazonaws.com
* https://alerta.it.accenture.com/

*Nota*:

Per integrazione con il sistema Alerta del command Center ACN è necessario configurare su ironport https://alerta.it.accenture.com/

### Bilanciamento

Il bilanciatore F5 si occupa di fare da VIP per accesso in https da Client verso Istio installato su namespace distribuiti sui nodi Infra.

Negli ambienti produttivi – parallelo e produzione - lo switch su datacenter secondario dovrà essere considerato attivando o disattivando il pool - di ogni vip applicativo - relativo alla farm 2 che contiene i nodi infra dei Cluster Openshift del datacenter di Rozzano.

STANDARD ARCHITETTURALE

Per tutte le applicazioni intranet e Internet è necessario utilizzare il protocollo HTTPS

### Note implementative

#### Link to internet

NA

#### Link to intranet – Strumenti operativi

NA

#### Altro

NA

## Architettura di sicurezza

### Sistemi di protezione e autenticazione

#### Autenticazione

Il cluster OCP con Kubernetes è integrato con AD aziendale e l’autenticazione avviene attraverso l’utilizzo di LDAPS.

Per l’autenticazione con LDAPS è necessario:

* portare su VM bastion la CA che firma il certificato utilizzato dal domain controller, *caldap.pem*, che espone in LDAPS, all’interno della directory *“/root/ocp4-free-<env>/installation\_dir/day2conf/*”
* creare la configmap che contiene la CA, ad uso dell’oauth
* creare il secret contenente la password di bind per l’utenza
* configurare l’oggetto oauth del cluster indicando quanto sopra, utenza tecnica di dominio e gruppi/utenti configurati in AD

In linea generale dovranno essere predisposti su AD i seguenti nuovi gruppi per ogni ambiente:

* CN=GU\_OCP\_ADMIN, CN=Users, DC=<dominio ambiente>, DC=it 🡪 Utilizzato per accesso alla console web di Openshift come ADMIN
* CN=GU\_OCP\_USER, CN=Users, DC=<dominio ambiente>, DC=it 🡪 Utilizzato per accesso alla console web di Openshift come USER

Per esempio, per gli ambienti di sviluppo e collaudo, affinché ci sia integrazione con Cyberark occorre configurare console in modo da avere un gruppo ldap-admin su dominio

* CN=GU\_OCP\_ADMIN, CN=Users, DC=gbcaipre, DC=it 🡪 Utilizzato per accesso alla console web di Openshift come ADMIN
* CN=GU\_OCP\_USER, CN=Users, DC=cariprpccoll.it, DC=it 🡪 Utilizzato per accesso alla console web di Openshift come USER

Al fine di permettere integrazione con Cyberark della console amministrativa di Openshift, come riportato nell’esempio è essenziale che:

* ci sia binding dinamico di due differenti domini Active Directory
* siano configurati due differenti plug-in ldap visibili nella pagina di log-on della console di OCP e due differenti sync operator ldap.

Per l’integrazione Cyberark saranno utilizzati i gruppi LDAP con la seguente naming convention:

* *Collaudo*

GBCAIPRE-OPENSHIFT-Admins

* *Parallelo e Produzione*

GBCAI-OPENSHIFT-Admins

In fase di installazione saranno comunque creati i gruppi AD di tipologia amministrativa per i vari ambienti (es. collaudo CN=GU\_OCP\_ADMIN, CN=Users, DC= cariprpccoll.it, DC=it 🡪 Utilizzato per accesso alla console web di Openshift come ADMIN).

Inoltre, per un corretto funzionamento dell’autenticazione e del sync dei gruppi, sarà necessario tenere allineate le configurazioni Oauth e GroupSync a livello di gruppi definiti. In tal senso, qualsiasi nuovo gruppo/utente integrato in AD viene sincronizzato – ogni 5 minuti - nel cluster OCP attraverso l’operator “Group Sync Operator”.

Il link della console web di Openshift è il seguente

https://console-openshift-console.apps.ocp-collaudo.<domain>

(esempio per collaudo):

<https://console-openshift-console.apps.ocp-collaudo.cariprpccoll.it>

La console è utilizzata:

* dagli amministratori di sistema come console amministrativa di prodotto;
* dagli utenti applicativi per temi di osservabilità per mondo sviluppo. In tale ambito gli utenti avranno accesso in visualizzazione alle parti applicative di competenza, per cui è stata richiesta apposita autorizzazione.

I Cluster OCP con Kubernetes hanno dei meccanismi di accesso standard CAGS, su AD. Pertanto, rispettano le linee guida aziendali.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Specifiche** | | **NOTE** |
| **Protezione in caso di attacco Brute-force** | Si  No | Blocco di un account dopo n tentativi  Tempo tra un tentativo e l’altro  Processo di recovery di un account bloccato  Altro |  |
| **Protezione della password** | Si  No | Salvataggio sicuro della password  Cifratura della password  Altro |  |
| **Algoritmo di Hashing** | Si  No | Algoritmo di hashing  Scopo del meccanismo (applicazioni, log-in , etc.)  Parametri di costo e numero d’iterazioni eseguite  Altro |  |
| **Sistema di autenticazione** | Si  No |  |  |
| **Other** |  |  |  |

Tabella 13, Sistemi di protezione e autenticazione dell’applicazione

### Utenze tecniche non nominative

L’installazione della piattaforma Openshift Container Platform ha necessità di un account tecnico per collegamento vCenter (cp\_12\_vcenter\_OCP) e di un’utenza che faccia bind al dominio cp\_4462\_ocp\_ldap.

STANDARD ARCHITETTURALE

1. Gli algroritmi di hashing MD5 e SHA-1 sono deprecati.
2. Tutte le applicazioni intranet devono utilizzare i sistemi di autenticazione centralizzati di Gruppo (AD, Ldap, Wam5)
3. I Sistemi di protezione per le applicazioni internet DEVONO essere specificati e trattati con il team di Sicurezza
4. Le password devono essere memorizzate e cifrate in tabelle diverse rispetto alle utenze
5. Tutte le applicazioni Internet devono essere integrate all’interno dell’architettura WAF
6. Per tutte le applicazioni Internet è necessario eseguire i Penetration test

### Protezione dati – INFO SU CMDB

|  |  |
| --- | --- |
| **Tipologia Dati** | Vedi CMDB, (Gestione dati sensibili, Gestione dati personali, Gestione dati giudiziari, Gestione dati generici) |
|  |
| **Disponibilità log di Accesso ai Dati degli Amministratori di Sistema (cd. Garante 1)** | Vedi CMDB, (Garante 1) |
| **Disponibilità log delle funzioni di inquiry dei dati bancari dei clienti (cd. Garante 2)** | Vedi CMDB, (Garante 2) |
| **Log per Antifrode** | Vedi CMDB, (Log antifrode) |
| **GDPR** | |
| **Art. 17: Diritto alla cancellazione**  Nota: indicare se sono state previste funzionalità per poter puntualmente eliminare i dati di un NDG a fronte di una richiesta proveniente dai clienti | Vedi CMDB, ( Art. 17: Diritto alla cancellazione ) |
| **Art. 15: Diritto di accesso**  Nota: Gestito centralmente mediante applicazione Tool Privacy | Vedi CMDB, ( Art. 15: Diritto di accesso) |
| **Art. 20: Diritto alla portabilità**  Nota:  indicare se sono state previste funzionalità per poter trasferire i dati di un NDG ad altro titolare del trattamento a fronte di una richiesta proveniente dai clienti | Vedi CMDB, ( Art. 20: Diritto alla portabilità ) |
| **Art. 18: Diritto di limitazione di trattamento**  Nota:  indicare se sono state previste funzionalità per poter anonimizzare i dati di un NDG al raggiungimento della fine del periodo di retention (10 anni dalla chiusura dell’ultimo rapporto). | Vedi CMDB, ( Art. 18: Diritto di limitazione di trattamento) |

Tabella 14, Dettaglio sicurezza dei dati

# System Management

## Administration Console

Durante la fase di installazione di OCP è generato di default un operator “console” che configura la rotta di accesso alla console amministrativa permettendo di accedere tramite il seguente link (esempio per collaudo, per parallelo e produzione cambierà il dominio di riferimento):

<https://console-openshift-console.apps.ocp-collaudo.cariprpccoll.it>

Da console OpenShift gli amministratori di sistema – allo stesso modo di quanto effettuato con la CLI dal nodo Bastion - gestiscono tutte le attività relative alla creazione, distribuzione e manutenzione di componenti infrastrutturali.

In particolare, da un punto di vista infrastrutturale è possibile:

* Creare e gestire nuovi nodi
* Creare e gestire namespace
* Gestire il monitoraggio delle applicazioni
* Creare e Aggiornare le componenti operator

I link per le console della componente Quay avranno la seguente struttura di naming convention:

https://instance-quay-namespace.apps.basedomain

STANDARD ARCHITETTURALE

1. Le interfacce di rete di tutti gli apparati di amministrazione devono essere configurate nella rete di management.
2. Le console di amministrazione devono, ove possibile, essere integrate con l’AD del gruppo.

## Change & Release Management

* L’installazione del Cluster OCP avviene attraverso gli automatismi di ACM.
* L’installazione del Cluster ACM avviene attraverso Ansible.
* Le modalità di rilascio e dimensionamento intra-cluster verranno definite nel documento di ogni applicazione ospitata nel cluster.

Note:

1. L’Applicazione delle Policy per ogni componente non è possibile farla da ACM. Il processo sarà quello di configurare YAML ed applicarlo attraverso comando su Bastion.
2. L’Installazione degli Operator, in virtù della ripetibilità, non è possibile automatizzarla poiché è necessario al momento dell’installazione – per operator non all’ultima versione - eseguirli in modalità Manuale.

NOTE

1. Se lo stack non è tra quelli indicati verificare con il gruppo di CM/Architetture la necessità di progetto
2. Se l’installazione utilizza script specificare nel dettaglio la tipologia e confrontarsi con il gruppo di CM.
3. Se l’installazione è di tipo custom specificare nel dettaglio il metodo/tecnologia e confrontarsi con il gruppo di CM.

**(\*) In caso di automatismo custom, questo deve essere fornito al Team Change a partire dall’installazione in ambiente di collaudo**

## Gestione dei Log

La Gestione dei Log è da suddividere per due differenti ambiti:

* i **Log infrastrutturali** o comunque il monitoraggio della piattaforma Openshift verrà demandato a uno stack nativo Lokistack così composto: Loki – Vector – Grafana, le componenti vengono deployate e configurate automaticamente in fase d’installazione con delle dashboard già presenti che permetteranno di tenere sotto controllo le metriche di principale interesse o accedere ai log Infrastrutturali. Per non modificare le modalità di monitoraggio a contratto si procederà al forworder delle suddette metriche verso Zabbix.

*Nota*:

Per integrazione con il sistema Alerta del command Center ACN è necessario configurare su ironport https://alerta.it.accenture.com/

* Per i **log applicativi** si è deployato l’operator di Loki logging che raccoglie i log di tutti i pod sui worker. I log sono consultabili da console openshift sotto observability 🡪 logging.

È stata impostata una retention di 10 giorni. Per permettere la corretta consultazione si è creato il ruolo “View and Loki” da associare ai gruppi che consente la consultazione dei log per i soli namespace a cui si è abilitati.

# Validazione

Questo capitolo riporta gli esiti della valutazione della soluzione riguardo al rispetto di vincoli architetturali e delle specifiche di sicurezza di Gruppo.

La sezione viene compilata in occasione del Tavolo Architetture per tracciare la validazione della soluzione rispetto i seguenti elementi:

* Specifiche Architetturali applicative di area
* Specifiche Architetturali
* Specifiche Infrastrutturali
* Specifiche Business Continuity
* Specifiche di Sicurezza

|  |  |
| --- | --- |
| **Tavolo Architetture - Data:** |  |
| **Stato approvazione** | Approvata  Approvata con raccomandazioni  Respinta |
| **Motivazione / Descrizione raccomandazioni** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*QUESTA E’ L’ULTIMA PAGINA DEL DOCUMENTO\*\*\*\*\*\*\*\*\*\*\*\*