PROCEDURA DI GARA APERTA TELEMATICA, SOPRA SOGLIA DI RILEVANZA EUROPEA, FINALIZZATA ALL'AFFIDAMENTO DEI SERVIZI APPLICATIVI E INFRASTRUTTURALI RELATIVI AI SISTEMI WEB-BASED DELL'AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE.

PROCEDURA DI GARA APERTA TELEMATICA

CIG B8B3485154

ALLEGATO 2 AL CAPITOLATO TECNICO

Caratterizzazione dell'attuale infrastruttura tecnologica

Sommario

1 Introduzione

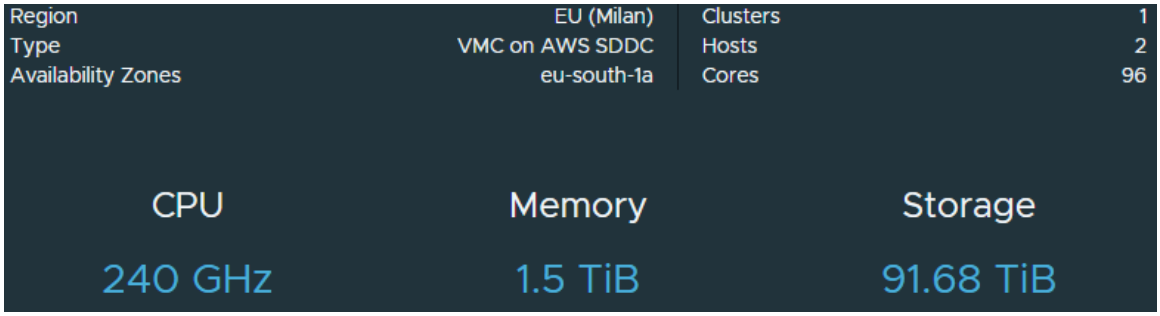
Il presente documento rappresenta la descrizione dello stato attuale dell'infrastruttura hardware e dei sistemi software di base che supportano le applicazioni web dell'Autorità.

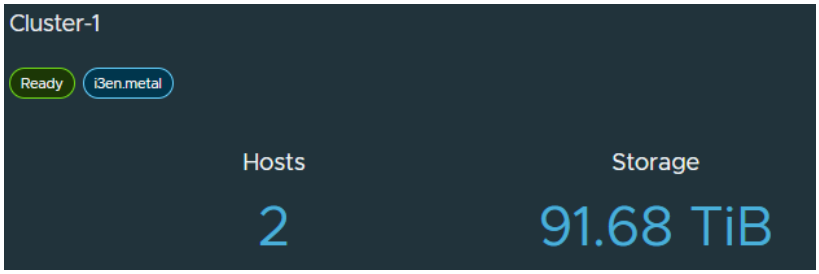
2 Ambienti del Sistema Informativo

2.1 Ambiente Virtualizzato (VMware)

2.1.1 Descrizione dell'infrastruttura VMware

1) Cluster VmWare (VMC on AWS SDDC) con le seguenti caratteristiche:





2) Infrastruttura di Disaster Recovery (Vmware Live Recovery) per le Vm di Produzione circa 40 VM / 20 TiB.

2.2 Sistemi Operativi

2.2.1 Windows

12 vm Windows Server

2.2.1.1 Descrizione e configurazione del sistema operativo Windows

Il perimetro dei server Windows è suddiviso in ambienti DEV/TEST/PROD:

AMBIENTE	RAM	STORAGE
DEV	8 GB	2 TB
	32 GB	4 TB
TEST	8 GB	2 TB
	32 GB	4 TB
PROD	32 GB	13 TB
	4 GB	6 TB
	8 GB	2 TB
	32 GB	4 TB
	32 GB	1 TB
	32 GB	1 TB
	32 GB	1 TB
	32 GB	1 TB

2.2.1.2 Sistemi e servizi su Windows

Si riportano solo i servizi non infrastrutturali.

Microsoft Access database engine 2010 (English) TortoiseGit 1.8.12.0 (64 bit) Zabbix Agent (64-bit) SAS Enterprise Guide 6.1 (64-bit) Microsoft Visual Studio 2010 Tools for Office Runtime (x64) Java 7 Update 55 (64-bit) Java SE Development Kit 7 Update 55 (64-bit) MySQL Connector/ODBC 3.51 SAS Add-In 6.1 for Microsoft Office (32-bit) pgAdmin III 1.22 SAS Enterprise Guide 6.1 (64-bit) - it Resources
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332 Zabbix Agent (64-bit) Open Text eDOCS DM 5.3 Server Open Text eDOCS DM 5.3 Web Server Qexplain2full AipaDocs Symantec Backup Exec Remote Agent for Windows Systems Docflow Pacchetto Integrazione Base DocflowClientComponents

2.2.2 Linux

2.2.2.1 Descrizione e configurazione del sistema operativo Linux

Il perimetro dei server linux è composto da **80 server totali** così suddivisi nei vari ambienti:

23 macchine di sviluppo

24 macchine di test

33 macchine di produzione

2.2.2.2 Sistemi e servizi su Linux

Di seguito il dettaglio del SO e dei software di base installati sui singoli server divisi per ambiente.

AMBIENTE DI SVILUPPO - AMBIENTE DI TEST - AMBIENTE DI PRODUZIONE:

- Apache HTTP Server
- Apache Tomcat
- java
- Docker
- LDAP

- Postfix
- Mongodb
- Proxy Squid
- WildFly
- Nginx
- Ruby
- Oracle
- Elasticsearch
- MariaDB / MySQL
- postgres
- Jenkins
- SASL
- Postfix
- FTP Server

3 Gestione dei Database

3.1 Tipologie di Database

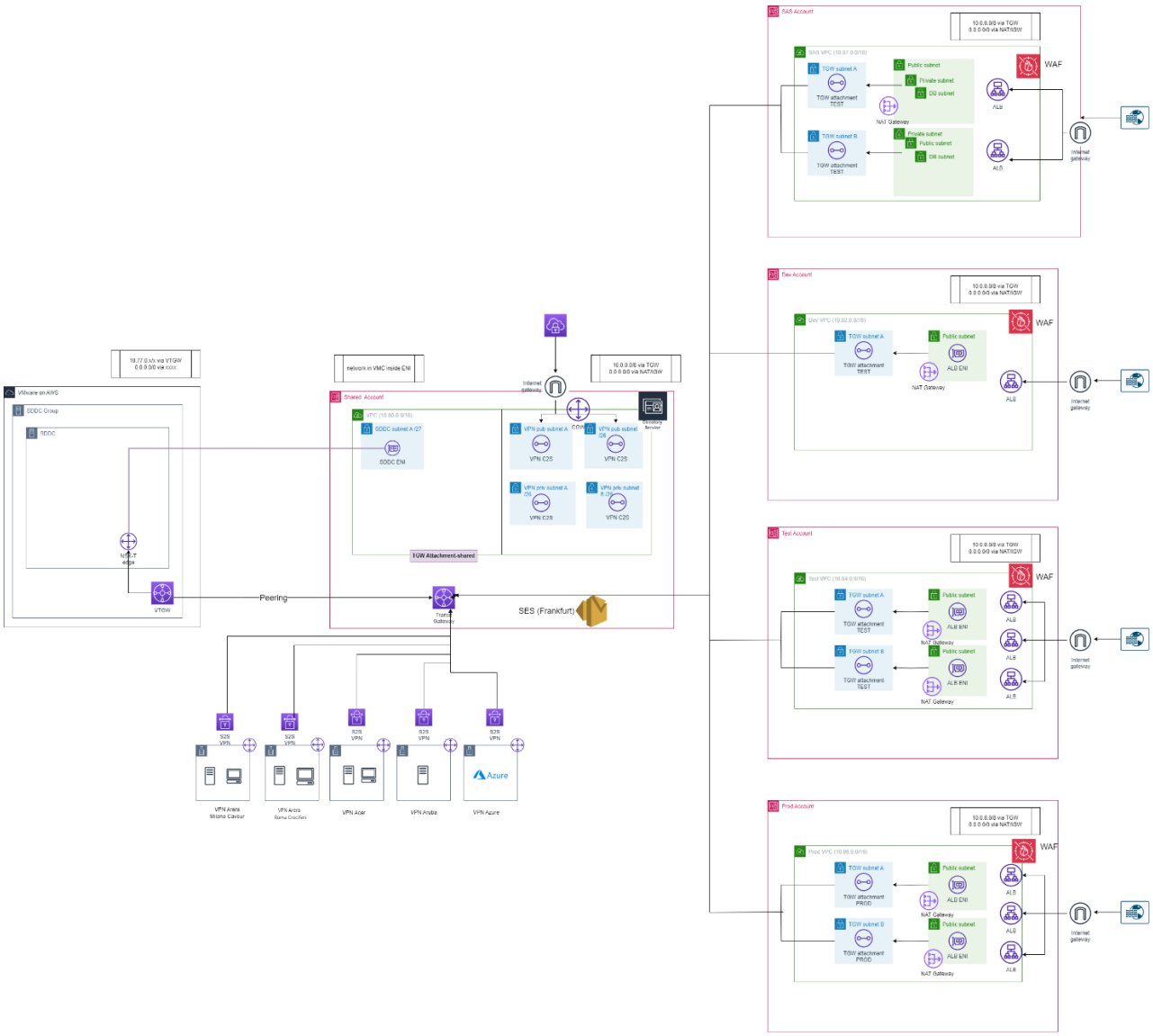
Il perimetro comprende principalmente istanze Oracle affiancate da istanze MongoDB e da presenze MySQL legacy.

Nel complesso emerge un contesto realistico per organizzazioni in evoluzione: base installata matura su Oracle, componenti NoSQL a supporto di specifiche esigenze applicative e talune piattaforme da aggiornare per allineamento a policy di sicurezza, conformità e supporto vendor

4 Cloud Computing

L'infrastruttura cloud di ARERA si trova nella regione di Milano identificata come **eu-south-1** ed è un'architettura multi-account organizzata secondo una AWS Organizations e costruita mediante il servizio AWS Control Tower.

Lo schema ad alto livello è quello rappresentato nella figura seguente:



4.1 Configurazione multi-account

L'architettura multi-account è da considerarsi una best-practice AWS per i landscape cloud Enterprise ed ha come scopo quello di segregare ed organizzare i servizi per account per migliorare la governance e la postura di sicurezza.

Gli account di Arera sono riassunti nella tabella seguente e descritti più in dettaglio nelle sezioni seguenti

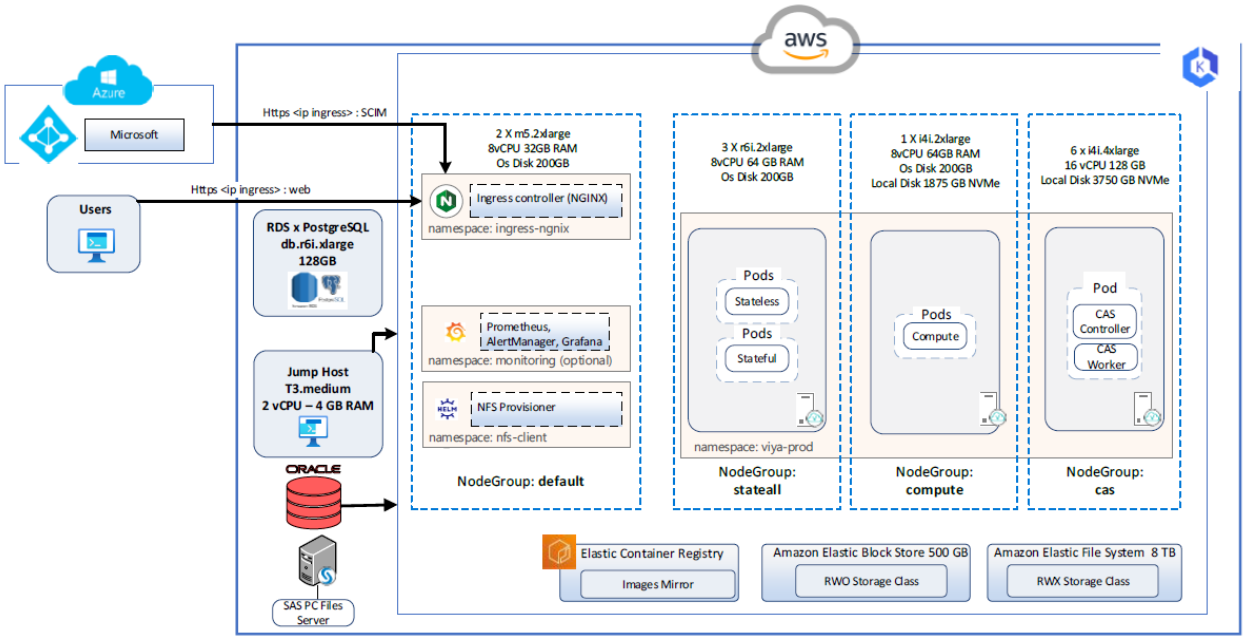
Account	Descrizione
ARERA-AWS-MASTER	Management Account di AWS Organizations.
Audit	Account per la gestione centralizzazione degli audit. È un account configurato di default dal Control Tower in fase di setup.

Log Archive	Account per la gestione centralizzazione dei log. È un account configurato di default dal Control Tower in fase di setup.
Shared	Account che ospita tutti i servizi condivisi dell'infrastruttura (connettività, backup, monitoring).
Arera DEV	Account contenente i servizi a supporto delle attività di sviluppo
Arera TEST	Account contenente i servizi a supporto delle attività di test
Arera PROD	Account contenente i servizi di Produzione ad eccezione di SAS
Arera SAS PROD	Account contenente i servizi di Produzione della piattaforma applicativa SAS Viya 4

4.1.1 Architettura SAS PROD

Questo account ospita i servizi che implementano la piattaforma SAS Viya 4 in accordo alle specifiche tecniche fornite dal team applicativo SAS coinvolto nel progetto.

L'architettura SAS Viya 4 è quella dello schema seguente:



4.2 VPN

L'architettura AWS di Arera utilizza sia la VPN site-to-site che la VPN client ed entrambe sono implementate mediante soluzioni native AWS.

4.2.1 VPN site-to-site

Sono presenti 5 VPN site-to-site configurate ed integrate con il servizio TGW.

4.2.2 VPN client

La VPN client è un servizio configurato per consentire la connessione ad AWS e VMware in modalità client-to-site con un dispositivo esterno all'organizzazione e/o alla rete aziendale.Integrazione con i sistemi ARERA

5 Infrastruttura di rete

5.1 Descrizione

Alla base dell'infrastruttura di rete c'è il VPC Sharing che consente di condividere risorse di rete tra account AWS in modo sicuro e controllato.

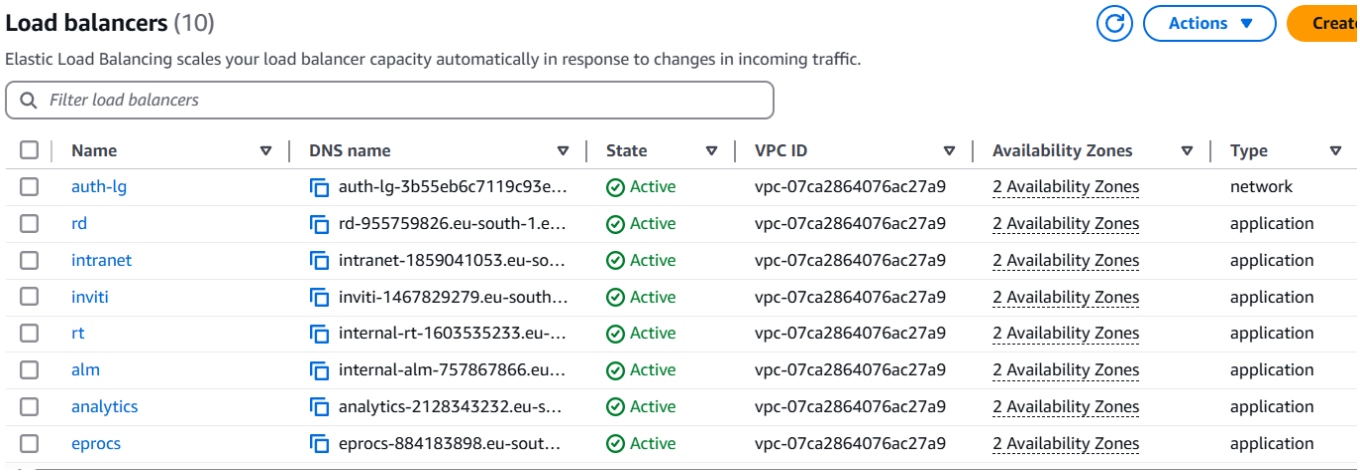
Il Transit Gateway è un componente chiave di questa infrastruttura in quanto agevola il flusso del traffico tra le VPC degli account, le VPN e Vmware on Cloud, fungendo da hub centrale per il routing.

La rete è basata su Amazon VPC con configurazioni di subnet per garantire l'isolamento tra gli ambienti: le subnet sono distribuite su 3 Zone di disponibilità per l'Alta Disponibilità.

La comunicazione con l'esterno avviene tramite Internet Gateway o, a seconda dei requisiti, tramite uno dei 3 Nat Gateway (per ognuna delle 3 zone di disponibilità).

Il traffico in entrata è accolto e distribuito dai bilanciatori (ELB), ognuno nel suo account di ambiente (DEV/TEST/PROD), il quale traffico, tramite un Transit Gateway attachment, raggiungerà il Transit Gateway condiviso nell'account Shared. Sul Transit Gateway poi ci saranno le regole di routing che permetteranno di raggiungere, tramite il peering del Transit Gateway, le vm presenti nei segmenti su VMC.

Tutti i Load Balancer di tipo Application sono stati integrati col WAF e con AWS Config.



Name	DNS name	State	VPC ID	Availability Zones	Type
auth-lg	auth-lg-3b55eb6c7119c93e...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	network
rd	rd-955759826.eu-south-1.e...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application
intranet	intranet-1859041053.eu-so...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application
inviti	inviti-1467829279.eu-south...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application
rt	internal-rt-1603535233.eu-...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application
alm	internal-alm-757867866.eu...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application
analytics	analytics-2128343232.eu-s...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application
eprocs	eprocs-884183898.eu-sout...	Active	vpc-07ca2864076ac27a9	2 Availability Zones	application

5.1.1 VMWARE NSX NETWORK

6 Backup e Recovery

L'infrastruttura di backup Arera presenta come software centrale Veeam Backup Replication collegato con Veeam Backup for AWS (progettato per istanze Amazon EC2, database RDS e file system EFS in un'architettura account singolo o multi-account) e Veeam Kasten che offre protezione sicura nativa di Kubernetes (Sas Viya 4.0 - utilizza come repository AWS). Software e Policy di backup

Come descritto nel primo punto l'infrastruttura di backup Arera presenta tre diversi software di backup Veeam Backup Replication, Veeam Backup for AWS e Veeam Kasten.

6.1 Veeam Backup Replication

Veeam Backup & Replication è una soluzione completa per la protezione dei dati e il disaster recovery, con la possibilità di creare backup a livello immagine di macchine virtuali, fisiche e cloud e ripristinarle. La tecnologia utilizzata nel prodotto ottimizza il trasferimento dei dati e il consumo di risorse, contribuendo a ridurre al minimo i tempi di ripristino in caso di disastro.

I backup configurati su Veeam Backup Replication sono suddivisi in base all'area di lavoro dell'utente, si dividono tra incrementali (6 giorni) e un full settimanale (sabato o domenica) , e tra ambiente produzione, test e dev.

Backup	RPO	RTO	Granularità	Retention
1	1h	4h	File/DB record	65 restore point
2	1h	4h	File/DB record	200 restore point

6.2 Veeam Backup for AWS

Il presente documento definisce le politiche e le procedure di backup e ripristino per l'infrastruttura ospitata su AWS, utilizzando la soluzione Veeam Backup & Replication. L'obiettivo è garantire la salvaguardia del patrimonio informativo dell'organizzazione, assicurando la continuità operativa in caso di perdita o danneggiamento dei dati.

Backup	RPO	RTO	Granularità	Retention
1	1h	4h	File/DB record	7 giorni
2	1h	4h	File/DB record	30 giorni

6.3 Veeam Kasten

Nello schema sotto riportato vengono definite le politiche e le procedure di backup e ripristino per l'infrastruttura ospitata su Kubernetes.

Questo software esegue il backup di applicazioni native sul cloud in tutta sicurezza da attacchi esterni e virus.

Garantisce che l'infrastruttura delle macchine virtuali e le applicazioni su Kubernetes siano facilmente recuperabili in caso di problemi..

Backup	RPO	RTO	Granularità	Retention
1	1h	4h	File/DB record	7 giorni
2	1h	4h	File/DB record	30 giorni

6.4 Gestione dei processi di BackUp

Il perimetro di backup include tutti i dati critici dell'infrastruttura Arera.

Le richieste ordinarie e straordinarie da parte del personale Arera o a parte dell'area L2 Applicativa possono pervenire anche tramite il sistema ITSM Manage Engine, con l'apertura di un ticket alla coda GIN (Gestione Infrastruttura) con la richiesta di restore. Tale ticket sarà preso in carico dalla Control Room e successivamente inoltrato alla coda dell'area Backup, dove il personale preposto gestirà la richiesta e procederà con l'attività di restore.

Classe	Area Funzionale	RPO	RTO	Granularità
	Extranet	8h	24h	File/DB record
	Intranet	24h	48h	File/DB record
	Reportistica	48h	96h	File

6.5 Schema di Backup e Frequenza

- **Backup completo**: Settimanale (Sabato o Domenica, 23:00-04:00)
- **Backup incrementale**: Ogni giorno fuori orario (22:00-6:00)
- **Retention**: 65 restore points su repository primario, 200 restore points su repository secondario.

7 Monitoraggio e Gestione

7.1 Principali Strumenti utilizzati

Qui di seguito si fornisce una descrizione dei tools principali utilizzati per affiancare l'approccio metodologico ai fini delle attività di gestione del servizio erogato.

Accoglienza Telefonica: Caratteristiche tecniche e funzionali

Tutte le comunicazioni relative alle segnalazioni e richieste pervenute al SPOC, sono gestite dalla piattaforma **X-Cally Motion**, che in base a criteri configurabili (come carico e priorità) le indirizza all'operatore più appropriato in modo da garantire i minori tempi di risposta possibili.

- Controllo in tempo reale delle prestazioni, dei KPI e delle statistiche
- Report dettagliati e configurabili
- Consultazione dell'archivio delle interazioni con l'utente
- Funzionalità specifiche per i supervisori del team del Contact Center

Le attività di monitoraggio includono:

- La manutenzione della piattaforma di monitoraggio
- La gestione dei monitoraggi (nuove implementazioni, modifiche, dismissioni) e delle relative impostazioni e soglie
- La raccolta e analisi degli eventi, con attivazione se necessario del processo di Incident Management tramite i tool previsti
- La predisposizione di dashboard e report per la presentazione degli eventi collezionati
- La registrazione delle informazioni storiche necessarie per l'analisi periodica dell'infrastruttura e la rilevazione dei livelli di servizio
- La gestione dei periodi di manutenzione dei sistemi monitorati (per evitare segnalazioni irrilevanti)
- La verifica periodica ed eventuale revisione dei monitoraggi (come parte del processo di Continual Improvement)

7.2 Piattaforma di Monitoraggio

La piattaforma scelta per l'erogazione del servizio di monitoraggio è basata sull'implementazione di una soluzione Open Source di livello Enteprise, ampiamente diffusa e supportata.

Zabbix monitora la disponibilità e performance delle **componenti** server, applicazioni, servizi, processi, file di log, siti web (anche con autenticazione), database, application server Java, infrastrutture VMWare, Container, Docker, **infrastrutture Cloud.** Inoltre, tiene sotto controllo le performance della stessa piattaforma di monitoraggio.

A fronte delle segnalazioni, vengono essere eseguite in automatico o manualmente diverse **azioni** (presa in carico, inserimento di commenti, comandi remoti, consultazione di istruzioni operative, invio di notifiche, inoltro ad altri sistemi) eventualmente con il supporto di **workflow** avanzati. Sono attivi, inoltre, meccanismi di **escalation** automatica delle segnalazioni in caso di persistenza dei problemi.

7.3 Service Management

Lo strumento ufficiale di Service Management adottato è **ManageEngine ServiceDesk Plus** per la gestione di:

- Richieste Cliente (Case)
- Incidenti / Problemi
- Modifiche / Change
- Reporting
- Asset Management

La piattaforma ServiceDesk Plus inoltre ospita una implementazione di CMBD per l'infrastruttura di Arera.

7.4 Descrizione delle Aree Applicative

Nei prossimi paragrafi si descrivono i blocchi funzionali e le aree applicative dei servizi web dell'Autorità.

- di circa 600 GB di spazio disco, 9 vCPU, 28 GB di RAM

7.5 Extranet

Le tecnologie applicativi utilizzate per i servizi di questa area sono:

- Java, Spring (2.x e 4.x), PL/SQL Oracle, GWT
- VM (2 DB e file share) per un totale di circa 1,5 TB di spazio disco, 17 vCPU, 50 GB di RAM
- VM (front-end) per un totale di circa 350 GB di spazio disco, 36 vCPU, 50 GB di RAM

7.6 Intranet e applicazioni interne

La sezione Intranet e applicazioni interne è composta dalle applicazioni ad uso interno all'Autorità fra cui Intranet, Missioni, Programmazione, Indirizzario, Gestione del personale (per un elenco completo delle applicazioni Intranet si veda l'Allegato 1).

Le tecnologie applicativi utilizzate per i servizi di questa area sono:

- Java, Spring (4.x), Ruby on Rails, AngularJS, Python Twisted, PL/SQL Oracle, SAS. Le risorse necessarie per questa funzione sono:
- 3 VM (Oracle, Nosql, ldap) per un totale di circa 150 GB di spazio disco, 8 vCPU, 12 GB di RAM
- 9 VM per un totale di circa 3 TB di spazio disco, 36 vCPU, 55 GB di RAM

7.7 Sistemi di gestione

I servizi di gestione includono, le VM per DNS, per la gestione della sicurezza in termini di obblighi di legge nonché prevenzione, tracciatura e difesa dagli attacchi, appliance di gestione (es. VMware), sistemi di backup, monitoraggio, gestione DR e tutti i sistemi di amministrazione e controllo dell'infrastruttura. Le risorse necessarie per questa funzione sono:

- 20 VM per un totale di circa 3,5 TB di spazio disco, 50vCPU, 120 GB di RAM

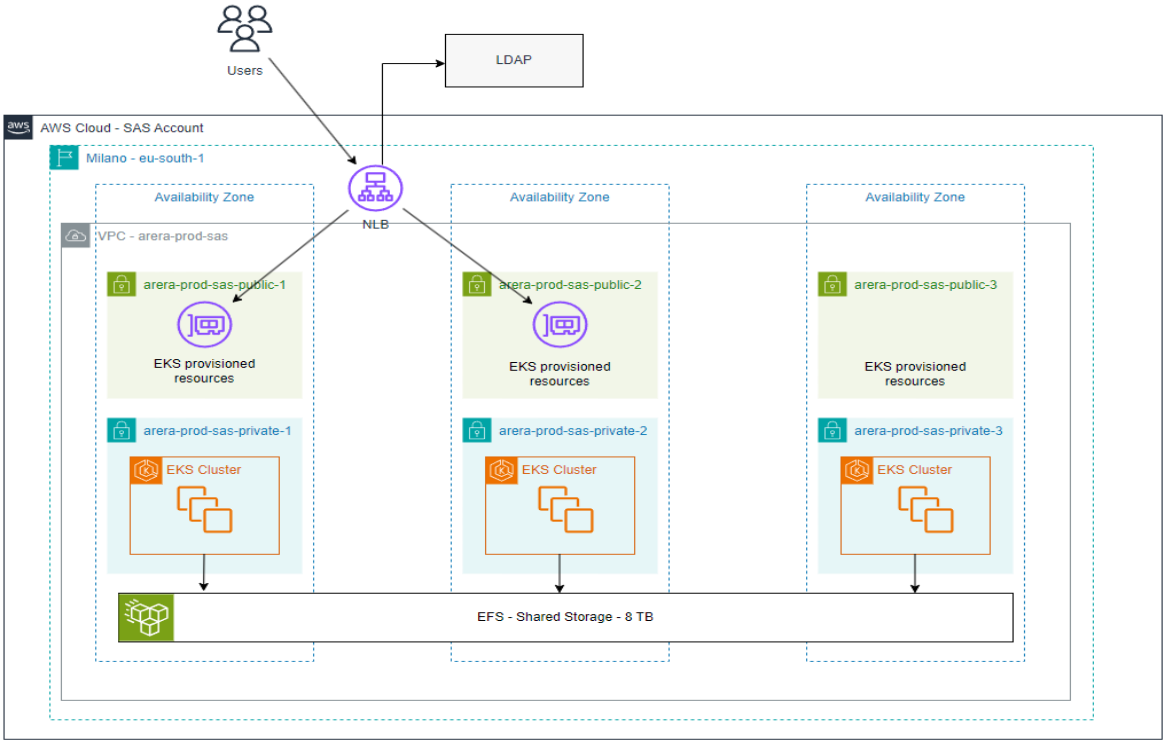
7.8 SAS VIYA

Il documento descrive l'architettura, le specifiche di implementazione ed i servizi operativi dell'applicazione SAS Viya4 su AWS ed è strutturato nelle sezioni seguenti:

- Architettura della soluzione
  - EKS
  - RDS
  - File Sharing
  - Autenticazione e Autorizzazione
  - Accesso applicativo
- Servizi Operativi
  - Servizio di backup
  - Servizio di monitoraggio infrastrutturale

7.8.1 Architettura della soluzione

Il sistema SAS Viya4 è una soluzione SAS basata su servizi AWS definita dal team SAS ed implementata attraverso script Terraform fornito da SAS dal team cloud.



7.8.2 Componente EKS

Il servizio Amazon EKS è implementato in modalità Managed Nodes con un dimensionamento e una distribuzione dei servizi sui singoli nodi definito dal team SAS e indicato nel documento [1].

7.8.3 Componente RDS

La soluzione include un database relazionale di tipo PostgreSQL implementato con il servizio RDS di AWS. Il database è una istanza singola come da specifiche tecniche SAS.

7.9 Sistemi in hosting

I sistemi in hosting sono VM “ospitate” sull’infrastruttura dedicata ma vengono gestite fino al sistema operativo. La gestione della parte applicativa è in carico all’autorità o a terze parti che operano per essa.

- 12 VM per un totale di circa 2,5 TB di spazio disco, 21 vCPU, 45 GB di RAM

Le applicazioni coinvolte sono:

- Protocollo informatico
- Ticket Management (RT)
- Timbratori
- Tuleap

8 Descrizione delle Aree Applicative

8.1 Suite Applicativa Autorità

Le applicazioni utilizzate per conto di ARERA sono le seguenti:

- Anagrafica Operatori
- Anagrafica Stazioni Appaltanti
- Anagrafica web service
- Anagrafiche settoriali - Teleriscaldamento (ATT)
- Anagrafiche settoriali - Territoriale GAS (ATG)
- Anagrafiche settoriali - Territoriale Idrica (ATID)
- Anagrafiche settoriali - Territoriale Rifiuti (ATRIF)
- Anagrafiche settoriali - Venditori (AV)
- Contenzioso
- Cruscotto anagrafica operatori
- Cruscotto Procedure Certificazione
- Estrattore Privato
- Ex Urbi
- Gestione del Personale
- Indirizzario Istituzionale
- Inviti
- Manage Engine
- Monitor raccolta dati 2.0
- Monitor ATRIF
- Procedimenti Sanzionatori
- Programmazione dei lavori del collegio
- Protocollo informatico
- Raccolta documentale
- Reclami
- REMIT webservice
- Separazione funzionale
- Sistema per le Raccolte dati 1.0
- Sistema per le Raccolte dati 2.0

- Sistema Unbundling contabile
- Sistema Unbundling contabile BO
- Sito Intranet
- SSO Extranet
- SSO Intranet
- Ticket Management (RT)
- Timbratori
- Tool FP
- Trello
- Viya 4.0