RdS
RICERCA DI SISTEMA

ENEA
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

Ricerca di Sistema elettrico

LA2.15 Servizi informatici per la realizzazione della piattaforma CI-RES

Simone Giannecchini, Giovanni Allegri, Mattia Giupponi

GeoSolutions
Your one-stop-shop for geospatial open source software

RdS_PTR22-24_PR1.7_LA2.15_368

Servizi informatici per la realizzazione della piattaforma CI-RES

Dicembre 2024

LA2.15 CI-RES: Realizzazione della Piattaforma di servizi e miglioramento della fruibilità della piattaforma ed apertura ad utenti esterni istituzionali e operatori

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dell'Ambiente e della Sicurezza Energetica - ENEA Piano Triennale di Realizzazione 2022-2024

Obiettivo: Decarbonizzazione

Progetto: Tema di ricerca 1.7 – Tecnologie per la penetrazione efficiente del vettore elettrico negli usi finali

Linea di attività: LA1.17

Responsabile del Progetto: Claudia Meloni, ENEA

Responsabile del Work Package: Claudia Meloni, ENEA

Responsabile Linea di Attività: Gregorio, D'Agostino ENEA

Mese inizio previsto: 19

Mese inizio effettivo: 36

Mese fine previsto: 19

Mese fine effettivo: 36

Il presente documento descrive le attività di ricerca svolte all'interno contratto dal titolo: Servizi informatici per la realizzazione della piattaforma CI-RES

Indice

1 Risultati attesi 4
2 Risultati ottenuti 5
3 Prodotti attesi 6
4 Prodotti sviluppati 8
5 Analisi degli scostamenti su attività e risultati 10
6 Sintesi delle attività svolte 11
7 Dettaglio delle attività svolte 12
8 Contributo delle eventuali consulenze alle attività sopra descritte 15
9 Pubblicazioni scientifiche 16
10 Eventi di disseminazione 17

Indice delle figure

Figura 1 Eridu deployment diagram (DEV machine) 13
Figura 2 Kanesh eployment diagram (PROD machine) 13

1 Risultati attesi

La realizzazione della piattaforma CI-RES, come definito nel capitolato tecnico, mirava alla messa in opera di un sistema avanzato e containerizzato per la gestione e la condivisione di dati geospaziali relativi alla resilienza delle infrastrutture critiche. Tale sistema doveva essere composto da componenti software open source, installati e configurati in due ambienti distinti (sviluppo e produzione), e predisposto per una futura migrazione su cluster Kubernetes. I risultati attesi si articolavano in più linee operative, che si possono sintetizzare come segue:

1. **Installazione e configurazione dei servizi software principali**: Il cuore della piattaforma doveva essere costituito da GeoNode, strumento per la gestione e pubblicazione di dati geospaziali, integrato con GeoServer, il motore per la pubblicazione dei layer geografici. Per garantire una gestione centralizzata e federata degli accessi, era prevista l'integrazione di DJAM, un Identity Provider basato su OpenID Connect e OAuth2. Tutti i dati strutturati dovevano essere gestiti attraverso un cluster PostgreSQL con estensione PostGIS, pensato per garantire alta affidabilità e performance elevate.
2. **Creazione e gestione di ambienti di sviluppo e produzione**: Il capitolato richiedeva l'allestimento di due ambienti distinti, uno per lo sviluppo (KANESH) e uno per la produzione (ERIDU). Entrambi dovevano ospitare installazioni complete dei servizi previsti, utilizzando un approccio containerizzato tramite Docker e Docker Compose, così da garantire isolamento, portabilità e coerenza tra i due ambienti.
3. **Sistema di backup automatizzato**: Era richiesto lo sviluppo e l'implementazione di un sistema di backup automatizzato per tutti i componenti della piattaforma. I backup dovevano essere eseguiti su base giornaliera, includere dump logici e snapshot dei dati, e prevedere la possibilità di ripristino su richiesta. Le procedure dovevano essere accompagnate da documentazione tecnica.
4. **Registro Docker privato**: Per garantire autonomia operativa e indipendenza da servizi esterni, il sistema doveva includere un registro Docker locale. Tale registro, installato su uno dei server, doveva essere accessibile anche dall'altro, e configurato per ospitare tutte le immagini Docker necessarie alla piattaforma.
5. **Documentazione tecnica e operativa**: Il progetto doveva includere la redazione di una documentazione esaustiva, comprendente istruzioni di installazione, configurazione, uso e manutenzione dei vari servizi. Dovevano essere forniti anche i file .env e gli script docker-compose.yml per ciascun ambiente, così da facilitare il riutilizzo e la manutenzione futura del sistema.
6. **Formazione e supporto tecnico**: Era prevista un'attività di affiancamento al personale ENEA, con incontri online e produzione di materiale formativo, con l'obiettivo di trasferire competenze per la gestione autonoma della piattaforma, la configurazione dei servizi e il monitoraggio dei backup.
7. **Predisposizione per ambiente Kubernetes**: Tutti i servizi, essendo stati containerizzati, dovevano risultare predisposti per una futura migrazione in ambiente Kubernetes, in linea con le prospettive evolutive dell'infrastruttura IT di ENEA.

2 Risultati ottenuti

Le attività svolte nell'ambito della Linea di Attività hanno portato alla piena realizzazione degli obiettivi tecnici previsti dal capitolato. La piattaforma CI-RES è oggi un'infrastruttura operativa, distribuita su due ambienti separati (sviluppo e produzione), dotata di tutti i servizi previsti: gestione dei dati geospaziali tramite GeoNode, pubblicazione dei layer tramite GeoServer, autenticazione federata con DJAM e database PostgreSQL/PostGIS in configurazione cluster con replica e failover.

I risultati sono stati conseguiti in misura piena e documentata, con un alto livello di affidabilità e una struttura progettata per essere facilmente evolvibile. È stata implementata con successo l'intera architettura containerizzata, comprensiva di un registro Docker locale, un sistema di backup automatizzato e un'infrastruttura di sicurezza gestita tramite reverse proxy.

Oltre agli obiettivi pianificati, sono stati raggiunti anche risultati non previsti dal capitolato ma di rilevante valore operativo: tra questi si segnalano la creazione di script avanzati per l'avvio rapido in ambienti multi-host, template automatizzati per la registrazione dei client OIDC su DJAM, e una documentazione particolarmente dettagliata che ha incluso checklist, esempi pratici, scenari di test e guide visuali.

Il beneficio per il sistema elettrico nazionale si concretizza nella disponibilità di una piattaforma tecnologica robusta e moderna, pensata per supportare l'analisi e la gestione della resilienza delle infrastrutture critiche. La possibilità di gestire dati geospaziali in modo sicuro, tracciabile e condiviso rappresenta un fattore chiave per la pianificazione e il coordinamento delle emergenze. La presenza di strumenti di autenticazione federata e di ambienti separati consente inoltre una gestione più efficace e scalabile delle simulazioni e degli scenari di rischio.

Tali risultati pongono le basi per un ampliamento futuro del sistema, anche verso ambienti cloud-native e Kubernetes, mantenendo l'allineamento con gli standard tecnologici più recenti e incrementando la flessibilità nella gestione delle risorse e dei dati.

3 Prodotti attesi

La realizzazione della piattaforma CI-RES, come definito nel capitolato tecnico, mirava alla messa in opera di un sistema avanzato e containerizzato per la gestione e la condivisione di dati geospaziali relativi alla resilienza delle infrastrutture critiche. Tale sistema doveva essere composto da componenti software open source, installati e configurati in due ambienti distinti (sviluppo e produzione), e predisposto per una futura migrazione su cluster Kubernetes. I risultati attesi si articolavano in più linee operative, che si possono sintetizzare come segue:

1. **Installazione e configurazione dei servizi software principali**: Il cuore della piattaforma doveva essere costituito da GeoNode[1], strumento per la gestione e pubblicazione di dati geospaziali, integrato con GeoServer[2], il motore per la pubblicazione dei layer geografici. Per garantire una gestione centralizzata e federata degli accessi, era prevista l'integrazione di DJAM[3], un Identity Provider basato su OpenID Connect e OAuth2. Tutti i dati strutturati dovevano essere gestiti attraverso un cluster PostgreSQL con estensione PostGIS, pensato per garantire alta affidabilità e performance elevate.
2. **Creazione e gestione di ambienti di sviluppo e produzione**: Il capitolato richiedeva l'allestimento di due ambienti distinti, uno per lo sviluppo (KANESH) e uno per la produzione (ERIDU). Entrambi dovevano ospitare installazioni complete dei servizi previsti, utilizzando un approccio containerizzato tramite Docker e Docker Compose, così da garantire isolamento, portabilità e coerenza tra i due ambienti.
3. **Sistema di backup automatizzato**: Era richiesto lo sviluppo e l'implementazione di un sistema di backup automatizzato per tutti i componenti della piattaforma. I backup dovevano essere eseguiti su base giornaliera, includere dump logici e snapshot dei dati, e prevedere la possibilità di ripristino su richiesta. Le procedure dovevano essere accompagnate da documentazione tecnica.
4. **Registro Docker privato**: Per garantire autonomia operativa e indipendenza da servizi esterni, il sistema doveva includere un registro Docker locale. Tale registro, installato su uno dei server, doveva essere accessibile anche dall'altro, e configurato per ospitare tutte le immagini Docker necessarie alla piattaforma.
5. **Documentazione tecnica e operativa**: Il progetto doveva includere la redazione di una documentazione esaustiva, comprendente istruzioni di installazione, configurazione, uso e manutenzione dei vari servizi. Dovevano essere forniti anche i file .env e gli script docker-compose.yml per ciascun ambiente, così da facilitare il riutilizzo e la manutenzione futura del sistema.
6. **Formazione e supporto tecnico**: Era prevista un'attività di affiancamento al personale ENEA, con incontri online e produzione di materiale formativo, con l'obiettivo di trasferire competenze per la gestione autonoma della piattaforma, la configurazione dei servizi e il monitoraggio dei backup.

[1] https://geonode.org/
[2] https://geoserver.org/
[3] https://github.com/geosolutions-it/djam

7. **Predisposizione per ambiente Kubernetes**: Tutti i servizi, essendo stati containerizzati, dovevano risultare predisposti per una futura migrazione in ambiente Kubernetes, in linea con le prospettive evolutive dell'infrastruttura IT di ENEA.

Prodotti hardware/software eventualmente attesi per la Linea di Attività

- **Hardware fornito da ENEA**:
    - Server ERIDU (ambiente produzione)
    - Server KANESH (ambiente sviluppo)
    - Storage condiviso per backup
- **Software installato/configurato**:
    - Docker e Docker Compose
    - PostgreSQL con estensione PostGIS
    - PGPool-II per gestione cluster PostgreSQL
    - GeoNode (custom)
    - DJAM (Identity & Authorization Management)
    - GeoServer (standalone)
    - Nginx come reverse proxy
    - Registro Docker privato
    - Bash scripts per backup e restore
    - Certificati SSL self-signed (in attesa di quelli ufficiali)
- **Documentazione prodotta**:
    - Specifiche tecniche di progetto
    - Manuale di deployment (per ERIDU e KANESH)
    - Manuale operativo
    - Guida backup & restore
    - Guida configurazione DJAM e client OIDC
    - Verbali e note tecniche delle riunioni

4 Prodotti sviluppati

Nell'ambito della Linea di Attività, sono stati sviluppati e configurati diversi prodotti software e componenti infrastrutturali. Alcuni di questi erano espressamente previsti nel capitolato, mentre altri sono stati realizzati come valore aggiunto, al fine di migliorare l'affidabilità e l'autonomia operativa della piattaforma CI-RES.

I prodotti realizzati coincidono con quelli attesi che potevano essere realizzati tramite diversi software. In questo paragrafo si è utilizzato il nome del software che realizza il prodotto atteso.

Dal punto di vista software, il principale prodotto sviluppato è l'infrastruttura containerizzata della piattaforma, articolata in moduli Docker che integrano:

- **GeoNode**: installato in versione personalizzata (GeoNode CI-RES), consente la gestione, il caricamento e la pubblicazione di dati geospaziali. Gli utenti accedono tramite browser autenticandosi con credenziali fornite da DJAM. L'accesso avviene tramite dominio dedicato, configurabile con certificati SSL forniti da ENEA.
- **DJAM**: modulo centralizzato per la gestione di utenti, organizzazioni e ruoli. Funziona come provider SSO per tutti i servizi della piattaforma. Gli amministratori possono configurare applicazioni client da interfaccia web, registrando URL di callback e scope di accesso. Gli utenti accedono tramite interfaccia web autenticandosi via username/password o con autenticazione delegata.
- **GeoServer**: installato come istanza standalone, pubblica layer geografici dinamici e consolidati. Le credenziali di accesso sono gestite tramite DJAM e il reverse proxy Nginx.
- **Cluster PostgreSQL con PostGIS**: database relazionale distribuito in replica, garantisce alta affidabilità e integrità dei dati geospaziali. Il cluster è gestito con PGPool-II per supportare bilanciamento del carico e failover automatico.
- **Registro Docker locale**: soluzione autonoma per l'hosting e il versionamento delle immagini Docker dei componenti sviluppati. È accessibile in lettura e scrittura da entrambe le macchine del sistema (KANESH e ERIDU).
- **Backup e ripristino**: sono stati creati e testati script Bash automatizzati per il backup quotidiano dei servizi GeoNode, DJAM, GeoServer e PostgreSQL. I backup vengono salvati su storage locale, con possibilità di integrazione a sistemi di rete (es. NAS).
- **Reverse proxy con Nginx**: configurato per gestire l'instradamento verso i servizi interni della piattaforma, applicando regole di autenticazione e autorizzazione fornite da DJAM.
- **Documentazione tecnica e operativa**: tutti i componenti sono accompagnati da guide di installazione, configurazione, uso e aggiornamento. I manuali sono organizzati per ambiente (DEV/PROD) e includono anche check-list operative, esempi di file .env e configurazioni Docker Compose.

Tra i prodotti sviluppati non esplicitamente previsti nel capitolato, ma inclusi a beneficio della Linea di Attività, si segnalano:

- **Configurazioni e script di avvio rapidi** per ambienti Docker in modalità multi-host.
- **Template di registrazione automatica client OIDC** per DJAM, utili per integrare nuovi servizi frontend.

- **Logica di backup intelligente con logging dettagliato e rotazione programmata dei backup**.

L'accesso ai servizi da parte degli utenti finali avviene sempre tramite browser, con autenticazione centralizzata gestita da DJAM. Per l'accesso amministrativo e la manutenzione dei sistemi, sono disponibili interfacce SSH e dashboard web. Tutte le configurazioni critiche sono documentate e replicabili su altri ambienti, anche in contesti Kubernetes.

5 Analisi degli scostamenti su attività e risultati

Nel corso dell'attuazione delle attività previste per la realizzazione della piattaforma CI-RES, non sono emersi scostamenti significativi rispetto agli obiettivi tecnici ed economici delineati nel piano iniziale. Le attività si sono svolte in linea con la pianificazione concordata, sia in termini di funzionalità implementate che di tempi di esecuzione.

L'unico elemento da segnalare, come lieve deviazione dal piano previsto, riguarda la configurazione dei certificati SSL e dei domini definitivi per i servizi GeoNode, DJAM e GeoServer. Questa attività non è stata completata per motivi indipendenti dall'esecuzione tecnica del progetto, in quanto l'emissione dei certificati e l'assegnazione dei domini è di competenza dell'amministrazione centrale ENEA. A tal fine, durante le fasi di testing e collaudo, sono stati utilizzati certificati self-signed e domini temporanei mappati via file hosts. La struttura è tuttavia predisposta per completare l'integrazione non appena saranno disponibili i certificati ufficiali.

Dal punto di vista economico, non sono stati rilevati scostamenti o extra costi rispetto a quanto inizialmente concordato. Tutti i prodotti software, compresi quelli non previsti esplicitamente nel capitolato (es. template di configurazione OIDC, script di verifica backup, strumenti avanzati di logging), sono stati realizzati senza richiedere variazioni economiche, rientrando nelle ore di lavoro allocate.

Per quanto riguarda i rischi segnalati nel piano iniziale, in particolare quelli legati all'infrastruttura messa a disposizione da ENEA e all'accessibilità ai sistemi, si evidenzia che non si sono verificate criticità gravi. I tempi di attivazione degli accessi e di predisposizione delle macchine sono stati compatibili con il calendario delle attività. Inoltre, la disponibilità di ambienti di test ben configurati ha consentito di eseguire verifiche funzionali in parallelo allo sviluppo.

Nel complesso, l'esecuzione delle attività ha beneficiato di una buona comunicazione tra le parti coinvolte e di un'attenta pianificazione condivisa, che ha permesso di anticipare e mitigare eventuali criticità, garantendo il rispetto degli obiettivi prefissati e la piena riuscita della Linea di Attività.

6 Sintesi delle attività svolte

Nel corso della Linea di Attività, GeoSolutions ha eseguito l'analisi, progettazione, realizzazione e documentazione di una piattaforma software distribuita, altamente configurabile e orientata alla gestione di dati geospaziali legati alla resilienza delle infrastrutture critiche. Le attività si sono articolate in più fasi successive, a partire dall'analisi preliminare dell'infrastruttura messa a disposizione da ENEA, fino al rilascio completo della piattaforma e alla formazione del personale interno.

Sono stati predisposti due ambienti distinti, uno per lo sviluppo (KANESH) e uno per la produzione (ERIDU), entrambi basati su sistemi Linux CentOS 9 stream, configurati per l'esecuzione di servizi containerizzati tramite Docker. In ciascun ambiente sono stati installati e configurati i seguenti componenti software: GeoNode, per la gestione e visualizzazione dei dati geospaziali; DJAM, come sistema centralizzato di autenticazione e autorizzazione; GeoServer, in configurazione standalone per la pubblicazione dei layer; un cluster PostgreSQL/PostGIS ad alta affidabilità, con gestione del failover tramite PGPool-II.

Parallelamente è stato realizzato un registro Docker privato, accessibile da entrambi gli ambienti, che consente di ospitare e versionare le immagini dei container necessari, in modo indipendente da risorse pubbliche. Per garantire la sicurezza e la resilienza del sistema, è stato implementato un sistema di backup completo, con procedure automatizzate per il salvataggio giornaliero dei dati e script per il ripristino. Tutte le operazioni sono accompagnate da logging dettagliato e meccanismi di rotazione dei file.

Oltre alla parte tecnica, particolare attenzione è stata dedicata alla produzione di documentazione dettagliata (manuali di installazione, configurazione, uso e manutenzione) e alla formazione del personale ENEA tramite incontri operativi e affiancamento da remoto. Le attività si sono concluse con la validazione della piattaforma da parte di ENEA, in seguito a test funzionali che hanno confermato il raggiungimento di tutti gli obiettivi previsti.

Il progetto si è concluso con successo, senza scostamenti significativi rispetto alla pianificazione iniziale. La piattaforma è pronta per l'utilizzo operativo e può essere ulteriormente evoluta per un deployment in ambiente Kubernetes, come già ipotizzato nel contesto del progetto.

7 Dettaglio delle attività svolte

Le attività realizzate nell'ambito della Linea di Attività si sono articolate in una serie di fasi integrate, che hanno portato alla realizzazione completa della piattaforma CI-RES, in coerenza con quanto previsto nel capitolato tecnico e nella pianificazione iniziale. Di seguito si riportano nel dettaglio le attività svolte, con riferimento ai risultati ottenuti e agli strumenti adottati.

Analisi preliminare e predisposizione ambienti

La prima fase del progetto ha riguardato l'analisi dell'infrastruttura server messa a disposizione da ENEA. Le due macchine, denominate KANESH (sviluppo) ed ERIDU (produzione), sono state configurate con sistema operativo CentOS 9 Stream e predisposte all'esecuzione di ambienti containerizzati. Sono state installate le dipendenze di sistema (Docker, Docker Compose, PostgreSQL) e definiti i criteri per la distribuzione dei servizi. In questa fase, si è provveduto anche all'analisi dei requisiti di rete, sicurezza e gestione delle credenziali.

Deployment e configurazione dei servizi

Una volta predisposti gli ambienti, si è proceduto con l'installazione e la configurazione dei seguenti componenti software:

- **GeoNode**, in versione personalizzata, per la gestione dei dati geospaziali.
- **DJAM**, configurato come Identity Provider centralizzato, in grado di gestire utenti e ruoli, e supportare l'autenticazione per tutti i servizi della piattaforma.
- **GeoServer**, distribuito in modalità standalone e connesso tramite reverse proxy per la pubblicazione dei layer.
- **Cluster PostgreSQL/PostGIS**, con configurazione di replica e gestione failover via PGPool-II.

Ogni servizio è stato containerizzato e integrato in uno stack Docker Compose, con file .env dedicati per ambiente. Le configurazioni sono state sottoposte a test incrementali in ambiente KANESH, prima del rollout definitivo su ERIDU.

Implementazione del sistema di backup e sicurezza

È stato realizzato un sistema completo di backup, basato su script Bash personalizzati e job schedulati. Ogni componente (GeoNode, DJAM, GeoServer, PostgreSQL) è oggetto di backup quotidiano. I file sono salvati su volumi locali, con possibilità di montaggio su storage di rete. Le routine includono log dettagliati, meccanismi di verifica automatica e script per il ripristino. Sono stati testati scenari di fault per validare il funzionamento del processo di restore.

Registro Docker e gestione delle immagini

Per garantire autonomia operativa e velocità nel rilascio degli aggiornamenti, è stato configurato un registro Docker locale, accessibile da entrambe le macchine. Il registro ospita tutte le immagini customizzate dei servizi e consente il controllo delle versioni in modo indipendente dai registry pubblici.

Documentazione tecnica

Ogni componente della piattaforma è stato documentato in maniera esaustiva. Sono stati prodotti:

- Manuali di installazione e configurazione per ERIDU e KANESH
- Istruzioni per la registrazione e gestione dei client OIDC su DJAM

- Guida al backup e ripristino
- Check-list per il controllo dei servizi

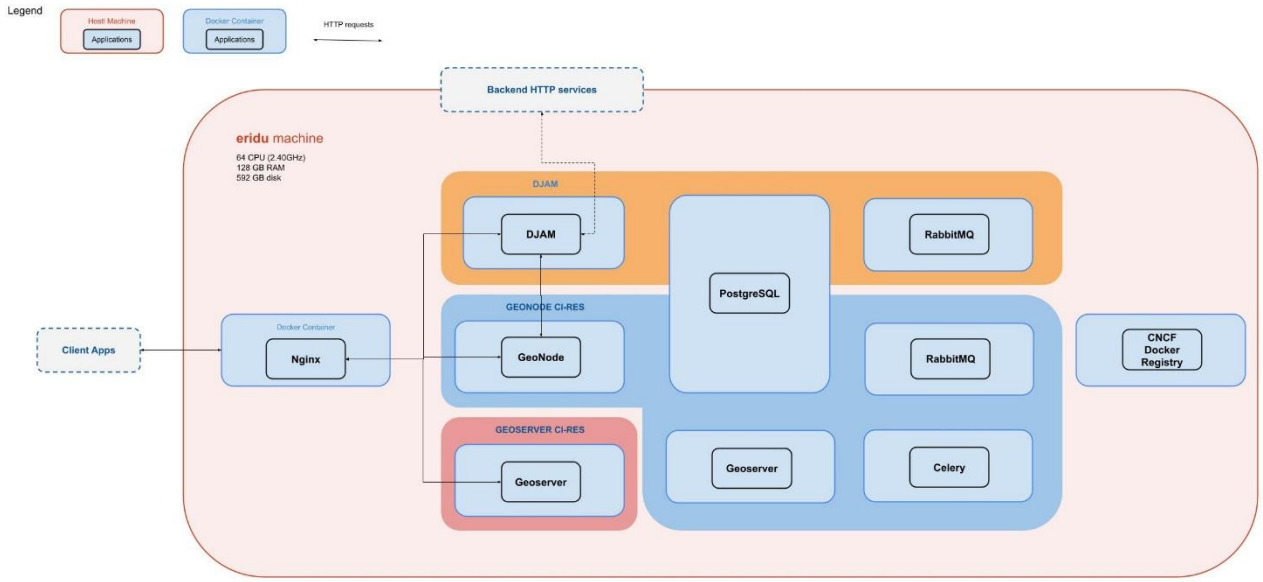

Figura 1 Eridu deployment diagram (DEV machine)

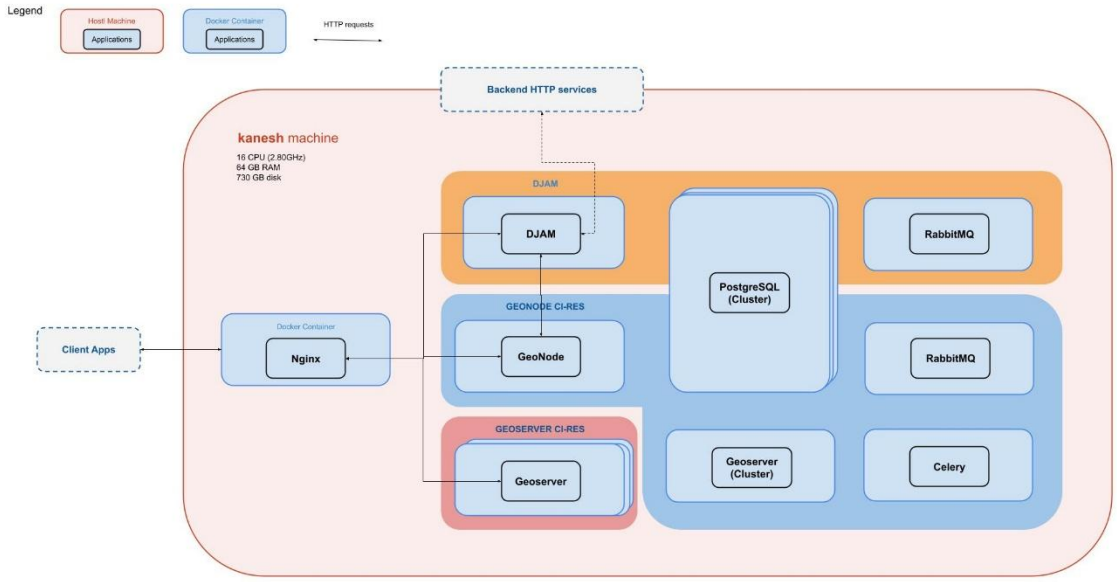

Figura 2 Kanesh eployment diagram (PROD machine)

Attività di formazione e affiancamento

Sono stati svolti incontri tecnici e sessioni di formazione con il personale ENEA, finalizzati a trasmettere conoscenze operative e fornire autonomia nella gestione dei servizi. Le sessioni hanno incluso walkthrough operativi, dimostrazioni pratiche e supporto alla configurazione dei domini e certificati.

Attività esplorative non evolute in risultati definitivi

Tra le attività svolte ma non consolidate in prodotti finali si segnala la predisposizione di una configurazione iniziale per un cluster Kubernetes, valutata come potenziale evoluzione futura della piattaforma. A causa delle limitazioni temporali e dell'assenza di una infrastruttura condivisa su cui validare il deployment, l'attività si è fermata allo studio preliminare e alla predisposizione di alcuni file manifest. Questa attività, pur non portando a un risultato consolidato, ha fornito elementi utili per orientare eventuali sviluppi futuri.

Nel complesso, le attività svolte hanno consentito di ottenere tutti i risultati attesi, con un'elevata coerenza rispetto al piano iniziale e una rendicontazione delle risorse in linea con quanto dichiarato.

8 Contributo delle eventuali consulenze alle attività sopra descritte

Non ci si è avvalsi di consulenze esterne

9 Pubblicazioni scientifiche

Pubblicazioni non previste

10 Eventi di disseminazione

Disseminazione non prevista