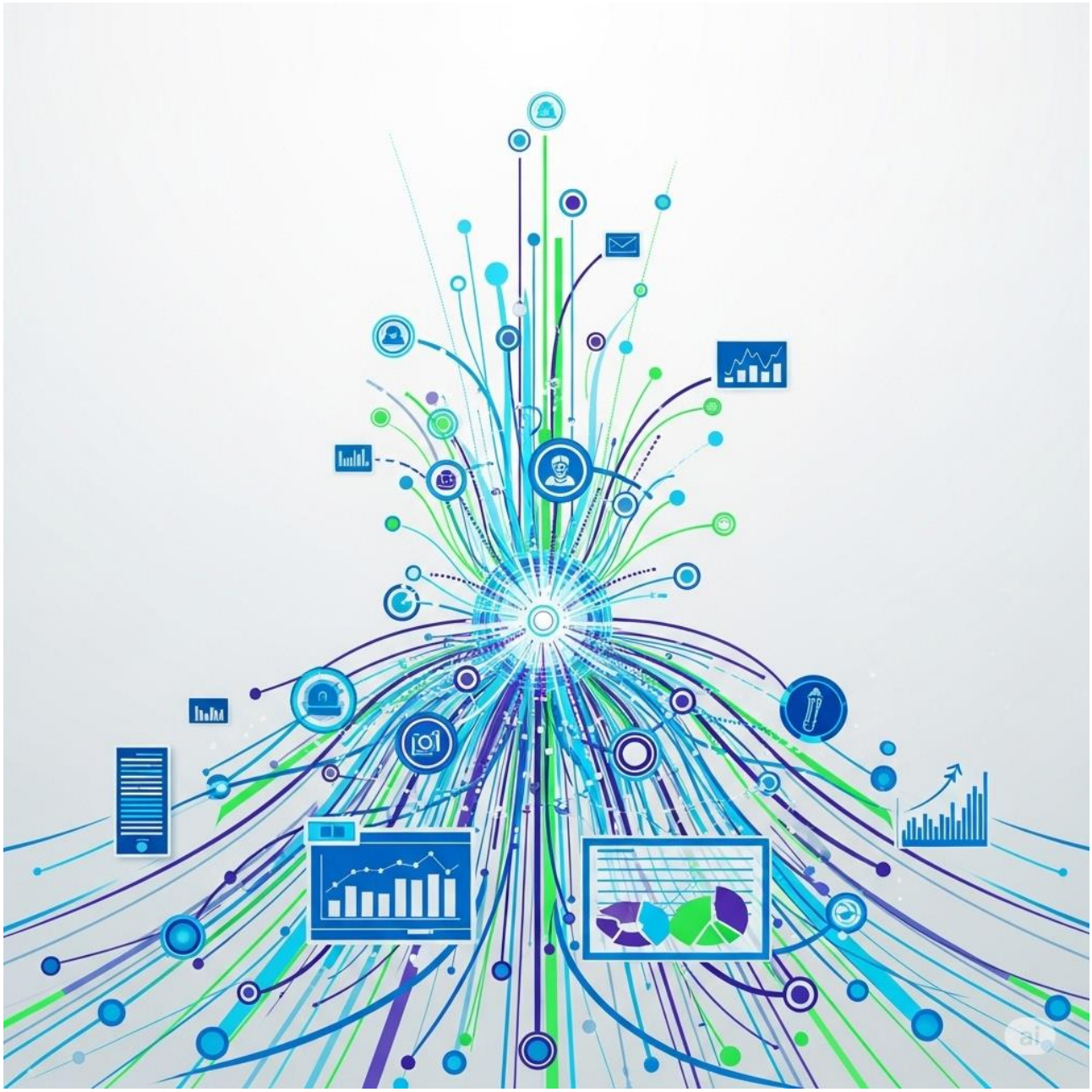
MANAGE+



INDICE DEL DOCUMENTO

2 DESCRIZIONE GENERALE

Manage+ è un sistema per la raccolta e la correlazione di dati eterogenei a cui applica algoritmi di misura dei KPI. Il modello architetturale del sistema prevede che MANAGE+ sia configurabile in modo da poter raccogliere dati oggetto del calcolo da sistemi esterni. Il sistema è pensato in modo da poter garantire un'elevata configurabilità e quindi, tale da poter essere utilizzato anche per estendere eventuali variazioni contrattuali. I dati potranno essere importati tramite file, tramite viste DB sui database o attraverso API REST e potranno essere caricati manualmente (on demand) oppure secondo una specifica frequenza. I dati elaborati saranno visualizzabili via web con i livelli di dettaglio disponibili a seconda del livello di autorizzazione impostato e saranno resi disponibili al Cliente finale automaticamente allo scadere dei tempi previsti e secondo le specifiche.

2.1 Principi guida

MANAGE+ è un software pensato tenendo bene in mente tutti questi principi guida, che sono alla base di tutte le nostre soluzioni:

- **valore**: il nostro obiettivo è collezionare in modo rapido ed efficiente i dati (anche in grandi quantità), analizzarli, correlarli e fornire informazioni di grande valore per l'azienda. In altre parole, vogliamo dare valore al dato
- **risultati**: fornire analisi di grande qualità in poco tempo e con risorse limitate
- **utilità**: fornire report analitici che permettono di conoscere lo stato della propria azienda, di potere ridurre i costi ed ottimizzare i servizi attraverso un sistema sicuro e garantito
- **sicurezza**: grande importanza è stata data alla sicurezza. Tutti i nostri software rispettano le linee guida dell'OWASP e sono compliant con le direttive del GDPR. La 2FA, ruoli e permission ben definiti, segmentazione e segregazione dei dati e registro dei log permettono accessi sicuri, dati protetti ed azioni non ripudiabili (vedi appendice A).
- **garanzia**: i risultati sono comprovati dalla generale soddisfazione dei nostri Clienti

2.2 Descrizione generale

Manage+ è una suite che integra i nostri principali prodotti, con delle specifiche finalità:

- **IWH+**: è il sistema che permette la raccolta dei dati, la normalizzazione, la gestione, la condivisione dei report ed il dispatching verso altri sistemi
- **SLAM+**: è il sistema che permette di calcolare tutti i KPI (SLA, OLA e UC)
- **NIMS+**: è il sistema che permette il monitoraggio di rete e applicativo, secondo un modello complesso di topologia

Nello specifico, IWH+ è il modulo che si potrebbe occupare di rispondere a requisiti generici quali, ad esempio, relativi al censimento dei contratti, dell'inventory e, in generale, della raccolta dei dati elementari, facendo le funzioni dei seguenti sistemi:

- sistema di Order Management
- sistema di Delivery (ed in genere per il collezionamento di dati elementari)
- sistema di Inventory
- sistema di Reporting

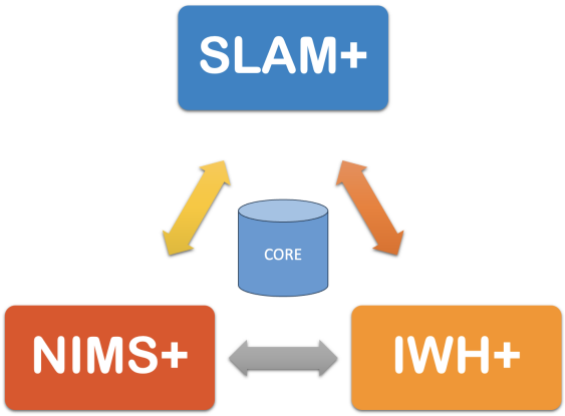
SLAM+ è lo strumento per il monitoraggio dei livelli di servizio e NIMS+ per tutto quanto riguarda le informazioni di rete.
Alcune delle caratteristiche principali del sistema sono le seguenti:

- **Granularità**: definire KPI e report per qualunque granularità: contratto, cliente, sito, servizio o item

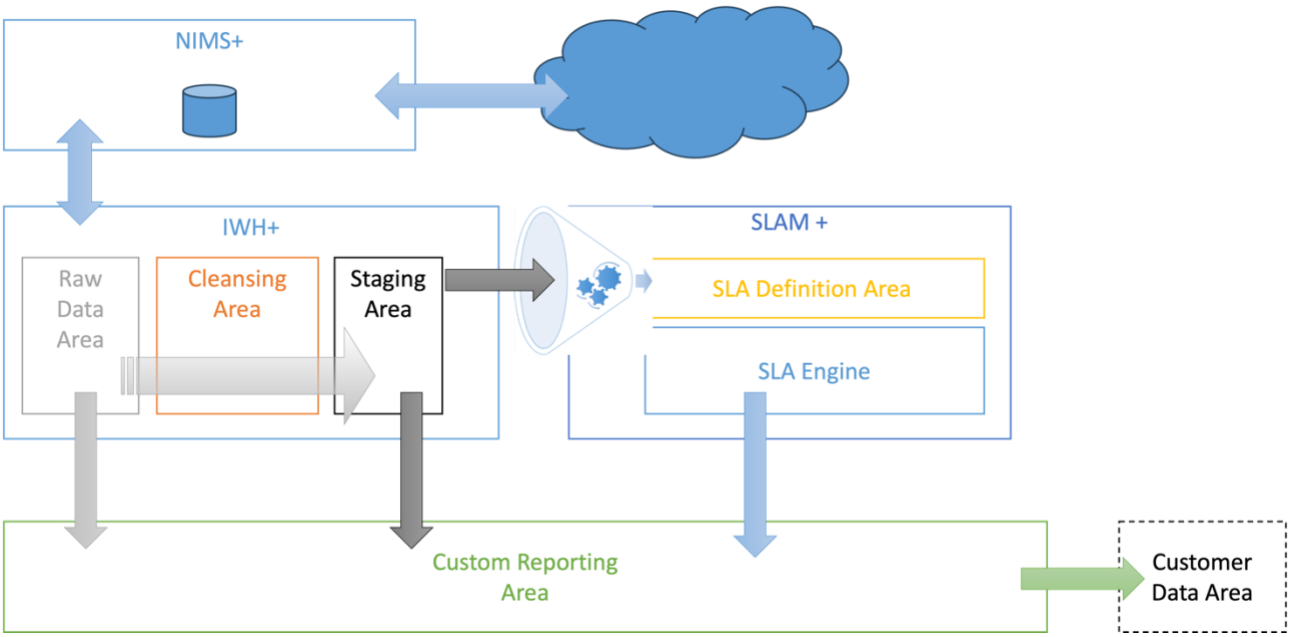
- **Storicizzazione del contratto**: Gestire versioni e storia del contratto tenendo conto dell'evoluzione dei servizi inclusi
- **Storicizzazione dei dati**: tracciamento automatico delle modifiche nel corso del tempo
- **Allarmi soglia**: Definire regole di alarming basate sul superamento di soglie predeterminate
- **Gestore delle anomalie**: Definire regole per stabilire la congruità e la correttezza dei dati provenienti da sistemi esterni
- **Riconciliazione**: Trattare e catalogare i dati e renderli omogenei con le richieste del contratto o del cliente
- **Profilatura avanzata**: Accedere a funzionalità o a singole porzioni di dati attraverso regole definite per ruolo
- **Pubblicazione**: Pubblicare report verso i Clienti in modalità manuale o automatica
- **Reporting avanzato**: Dashboards, andamenti grafici, filtri di ricerca avanzati ed export in vari formati o in un unico PDF
- **Simulazioni**: simulare scenari attraverso caricamenti opportuni
- **Correlatore**: permette la correlazione di dati provenienti da fonti eterogenee

2.3 Architettura funzionale

I moduli di MANAGE+ sono tutti integrati fra loro: si parlano nativamente e condividono un unico core per la gestione dei login e dei profili.



Gli elementi logici che andranno a comporre l'applicazione sono mostrati nella figura di seguito.

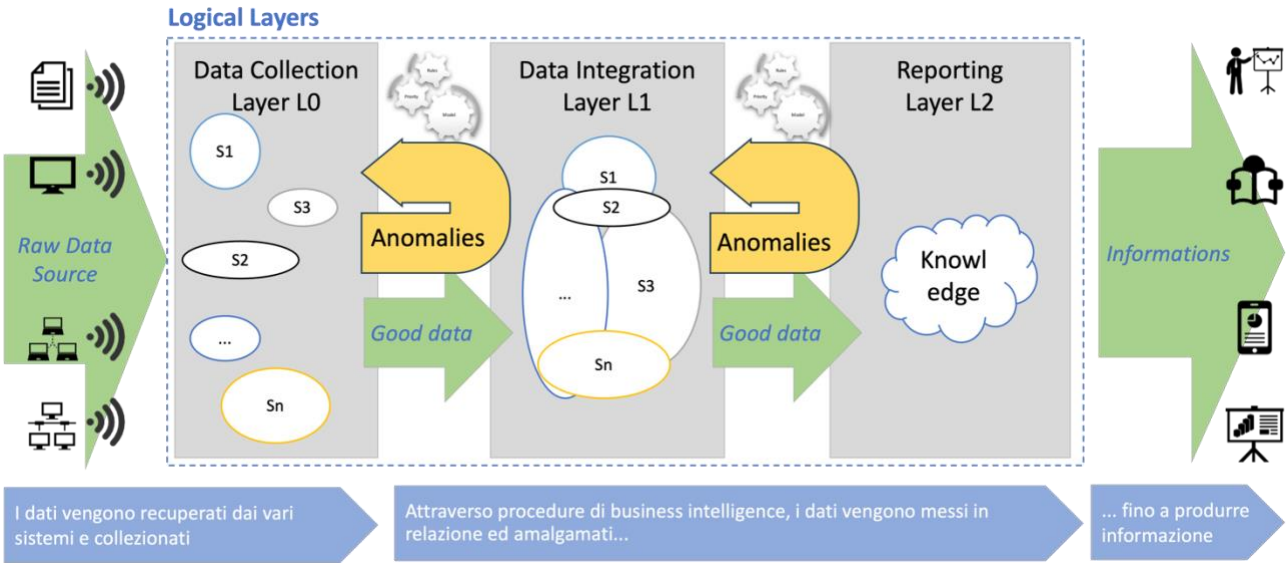


Il sistema è composto da 5 aree che vengono toccate da un generico flusso di dati. Le 5 aree fondamentali del flusso (o processo) sono le seguenti:

- **Import Raw Area**: area deputata al caricamento dei dati grezzi dalle varie fonti alimentanti o template. Le modalità previste sono le seguenti:
  - Attraverso file (testo, CSV o Excel)
  - Attraverso l'accesso a Database (viste o tabelle)
  - Attraverso l'accesso ad API REST (secondo metodi definiti)
  - Attraverso l'interrogazione di applicazioni o oggetti connessi alla rete da parte di NIMS+
- **Cleansing Area**: area deputata al controllo delle regole di entrata, normalizzazione, riconciliazione, ecc….. Nello specifico, le principali sottoaree comprendono:
  - Validation Area: area per il controllo dei vari campi
  - Trasformation Area: area per la trasformazione automatica dei vari campi
  - Reconciliation Area: area per la riconciliazione automatica dei vari campi
- **Staging Area**: area deputata alla gestione del dato e del template. Le principali funzionalità messe a disposizione sono:
  - Sui dati: inserimento/modifica/cancellazione (sia singolarmente che massivamente)
  - Sui template: gestione delle proprietà (nome, chiavi, correlazioni, permessi, gestione degli stati, ecc.…)
- **SLA Definition Area**: tutta la parte che attiene ai vari KPI, ne permette la definizione, la gestione, il controllo e la storicizzazione attraverso lo SLA Design.
- **Reporting Area**: area deputata alla definizione, gestione ed esportazione di tutta la reportistica. Nello specifico, i moduli presenti all'interno di quest'area sono:
  - Designer: area che permette la progettazione e la definizione dei report
  - SLA Report: area deputata alla reportistica SLA
  - Reports: area di consultazione dei vari report ad hoc
  - Exporter: area che permette l'esportazione dei report verso altre fonti
  - Dashboard: area che permette di visualizzare le varie metriche su tool grafico

2.4 Struttura Multi Layer

Il sistema è costituito sulla base di tre strati logici. Ogni strato (Layer) identifica una ben precisa area del sistema (viste al paragrafo precedente), con funzioni specifiche. I layer sono, in ordine di processo L0, L1 ed L2.
Ogni layer è isolato (non possono crearsi commistioni di dati tra diversi strati) e svolge una specifica attività.
Se un generico pacchetto dati supera tutti i test previsti nel proprio layer allora è pronto per essere trasferito al successivo e manipolato.
Tutto ciò che non supera i controlli viene rigettato ed esposto come anomalia. Tutte le anomalie di ogni strato sono naturalmente visibili dall'esterno e pronti per essere bonificati e ritrattati. Così fino al layer finale L2, dove il dato è pronto per la visualizzazione.
Di seguito una rappresentazione dei layer appena descritti.



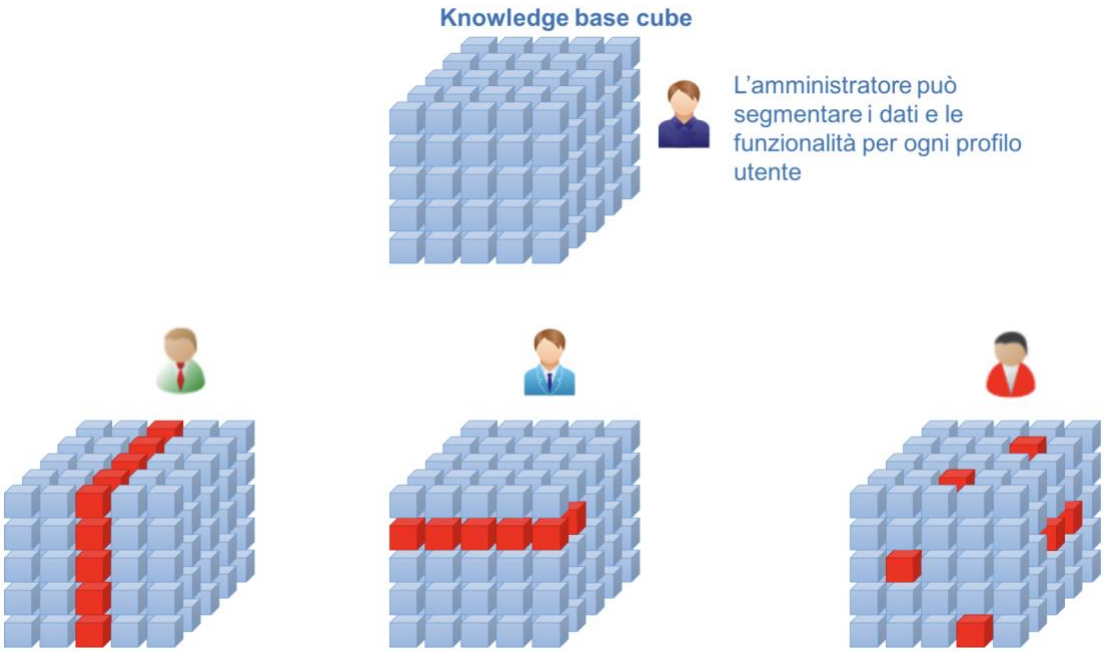
Gli elementi logici servono principalmente per due scopi:

- **controllare i dati**: ad ogni passaggio da un layer ad un altro vengono controllati e "stoppati" tutti quegli elementi che non rispettano le regole definite o che non hanno i requisiti per passare al livello successivo. Proprio come in una dogana, il sistema controlla tutti gli elementi che cercano di entrare e li sottopone ai controlli specificati in fase di configurazione (es. campi vuoti, non congruenti, non validi, ecc.…)
- **amalgamare i dati**: i dati ad ogni salto di livello vengono sempre più normalizzati e "fusi" con gli altri presenti. Tutto questo genera una base di conoscenza (o Knowledge base) uniforme ed omogenea, senza nessuna anomalia

2.5 MultiTenant, MultiClient e Data Segregation

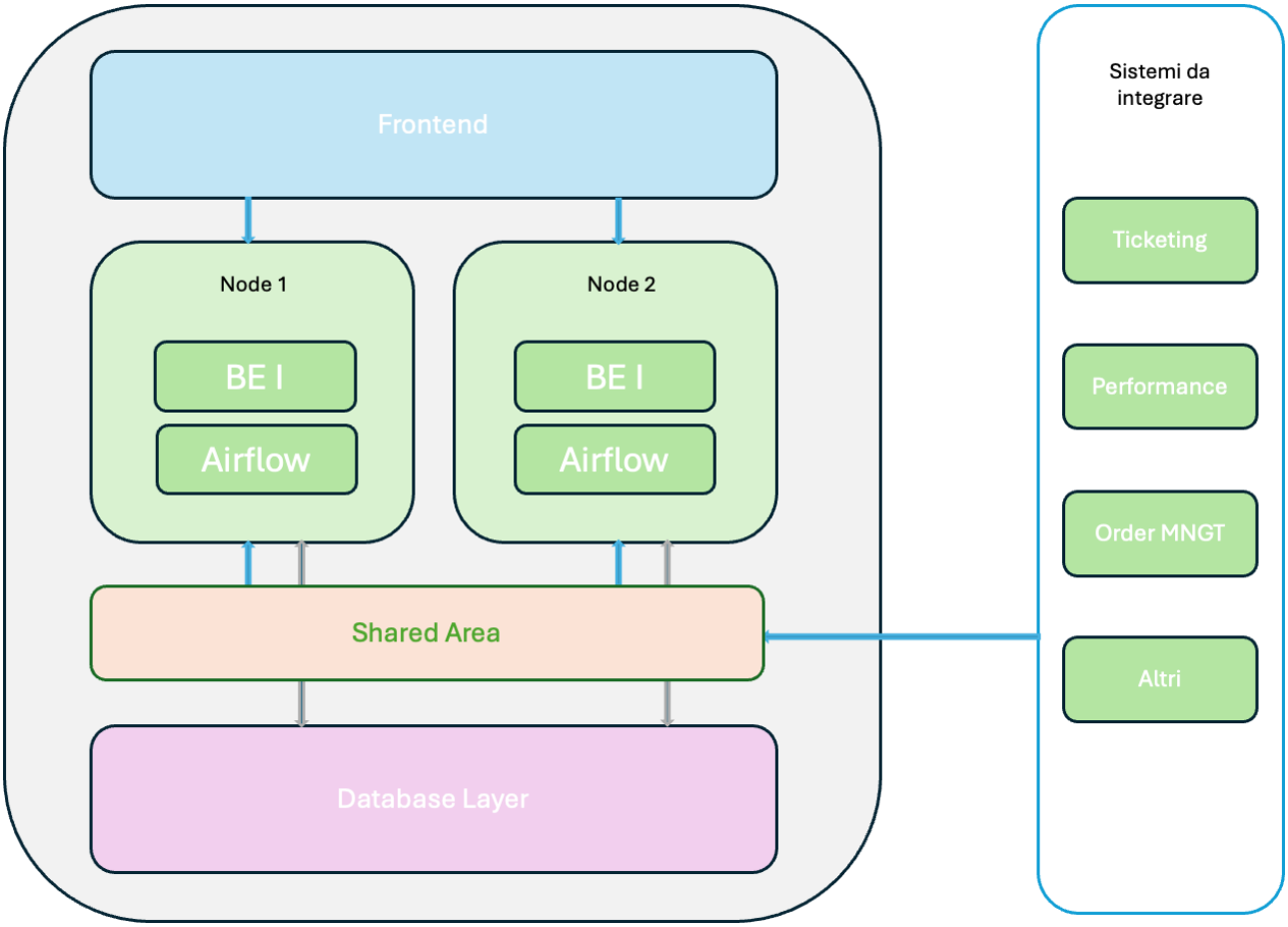
Il sistema è stato pensato per essere completamente configurabile e per gestire le esigenze di diversi clienti.
In ambito multiclient è stata data particolare importanza alla Data Segregation, ovvero alla possibilità di permettere e garantire l'isolamento di un singolo cliente o gruppo, attraverso la configurazione di un proprio catalogo ed un proprio strumento di caricamento e lettura delle informazioni di ingresso.
Ogni singola utenza potrà pertanto essere identificata come parte di una specifica community di utenti, con accesso solo ad una porzione di dati, quella attribuita dall'amministratore di sistema. L'amministratore di sistema potrà stabilire quindi per le diverse tipologie di profilo le

caratteristiche non solo per quanto concerne la visibilità dei dati (accesso ad un sottoinsieme generico di informazioni), ma anche per l'accesso alle diverse funzionalità (amministrazione, configurazione cataloghi, inserimento o cancellazione di record, ecc…).
La figura seguente mostra un esempio di come l'amministratore di sistema possa configurare i vari profili utente e segmentare dati e funzionalità da mettere a disposizione.



2.6 Architettura HW

L'architettura software è a 3 livelli come sintetizzato nello schema seguente



- Frontend applicativo: layer di accesso delle utenze. Questo layer è scritto utilizzando la nota libreria Javascript React, libreria moderna ed efficiente per la creazione di applicazioni Web con contenuto UI/UX accattavante e funzionale. A questo livello accedono gli utenti esterni, sia Intranet sia Internet. La funzione è quella di segregare, anche per garantire aspetti di sicurezza, le attività utente dalle attività applicative.
- un layer di backend applicativo in alta affidabilità e scalabile. Questo livello è diviso in 3 sezioni:
    - Shared area: un layer fisico (es: disco) o logico (Es: Data collection layer) che raccoglie i dati dai sistemi da integrare come fonti dati, come i sistemi di Ticketing, Performance, order management.
    - Airflow: utilizza Airflow Apache per la gestione e schedulazione dei batch applicativi di elaborazione
    - BE I: è la backend intelligence, che applica le specifiche di configurazione orchestrando le attività di elaborazione nei flussi applicativi (Data collection, data integration fino a reporting)
- layer DB: dove vengono salvati i dati.

Il layer applicativo è scalabile e clusterizzabile per garantire la massima sicurezza in termini di disponibilità anche in caso di forti carichi o di volumi crescenti nel tempo
L'aspetto applicativo critico è sostenuto dai Nodi di Backend (nel disegno, node1 e node2).
I nodi possono essere estesi secondo le esigenze ed essere inseriti "a caldo" ossia senza interrompere il servizio.
La presenza di più nodi, oltre a garantire la scalabilità, garantisce inoltre l'alta affidabilità.
Il numero di nodi è definito con l'utente in base alle necessità.

2.7 Sistema operativo e Software Middleware

Vengono riportati gli elementi applicativi di middleware che compongono Manage+

Elemento applicativo	Descrizione
Linux	Sistema operativo Linux tipo Red Hat like. Versione 9.x o successiva
React	Framework di frontend javascript per la generazione dalla UI / UX Versione 19 o successiva
yiiframework	Framework PHP di backend con cui è costituita la Backend Intelligence
Apache Airflow	Workflow manager utilizzato per l'elaborazione batch dei caricamenti e per la gestione dello scheduler. Versione 2.x o superiore
python™	Linguaggio di backend utilizzato nei processi di workflow
MySQL®	Oracle MySQL: Database di supporto all'applicazione

2.8 Best practice utilizzate

Il software è sviluppato utilizzando gli standard di programmazione più attuali come ad esempio:

- Restful API: per la comunicazione fra nodi e livelli applicativi
- CI/CD: Processi di sviluppo ed integrazione continui
- OWASP API Security Top 10: un occhio di riguardo alle 10 vulnerabilità principali (https://owasp.org/www-project-api-security)
- Uso di comunicazioni sicure con protocollo HTTPS
- Sanitizzazione degli input
- Performance optimisation: attenzione costante alla gestione delle performance applicative
- GDPR compliant con un approccio nativo alla sicurezza ed alla segregazione dei dati secondo il principio di Privacy by design
- È sottoposto regolarmente ad analisi automatica da software di code review e Vulnerability Assessment

3 APPENDICE A

Ecco un elenco dei principi e delle linee guida generali nel campo della sicurezza informatica implementati nel nostro software:

- **Confidentiality** (Confidenzialità): questo principio assicura che le informazioni siano accessibili solo a soggetti autorizzati
- **Integrity** (Integrità): garantisce che i dati siano accurati e completi, e che non siano stati alterati o manomessi in modo non autorizzato
- **Availability** (Disponibilità): assicura che i sistemi e le informazioni siano accessibili e utilizzabili quando necessario dagli utenti autorizzati
- **Authentication** (Autenticazione): rappresenta il processo di verifica dell'identità di un utente, sistema o entità prima di concedere l'accesso e si occupa di rispondere alla domanda che l'autenticazione si pone: "Sei davvero tu?"
- **Authorization** (Autorizzazione): determina a quali risorse un utente o un sistema autenticato può accedere e quali azioni può eseguire
- **Non-Repudiation** (Non ripudio): fornisce la prova che un'azione è stata eseguita da una specifica entità e impedisce a tale entità di negare di averla eseguita
- **Separation of duties** (Separazione dei compiti): permette la suddivisione di un processo critico in più passaggi, assegnando ciascun passaggio a utenze diverse, per prevenire gli errori
- **Least Privilege** (Privilegio Minimo): concede agli utenti e ai sistemi solo i diritti e le autorizzazioni strettamente necessarie per svolgere le loro funzioni
- **Defense in Depth** (Controlli di Sicurezza a Livelli): implementa più strati di controlli di sicurezza (front-end, back-end, DB) per proteggere il sistema. Se un livello fallisce, ci sono altri livelli a protezione
- **Auditability** (Verificabilità): la capacità di esaminare i log del sistema per tracciare le azioni, identificare attività sospette e garantire la conformità. Permette di sapere chi ha fatto cosa e quando.
- **Privacy by Design**: protezione delle informazioni personali e sensibili degli individui, in conformità con le leggi e i regolamenti applicabili
- **Security by Design**: integrare la sicurezza fin dalle prime fasi di progettazione di un sistema o di un'applicazione
- **Security by Default**: configurare il sistema con le impostazioni di sicurezza più stringenti come predefinite