Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

NUMERO DOCUMENTO: **C000CMP01STP01**

REVISIONE: **01.00**

DATA: **04/11/2025**

CAGE CODE: **A0069**

Leonardo Services Documentation

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Firme

Autore: **Digital Proposal & Pre Sales** Digital Proposal & Pre Sales| Digital Systems & Engineering Technologies | Engineering	..... Elio Arena
Verifica: **PEM IPT di Prodotto** R. Digital Systems & Engineering Technologies | Engineering	..... Andrea Giorgio Busà
Verifica: **PAM IPT Sviluppo** Quality Cyber Security, Intelligence & Digital Solutions	..... Simonetta De Biase
Approvazione: **IPT Leader IPT di Sviluppo** R. Digital Platform | Digital Systems & Engineering Technologies | Engineering	..... Daniele Leone
Approvazione: **Technical Authority** Solution Architects | LoB Public Admin., Defence & Inter. Agencies	..... Susanna Fortunato
Autorizzazione: **Product Manager IPT Prodotto** Product Management Digital Trasformation | Product Management	..... Fabio Russo

Contatti

Elio Arena **Digital Proposal & Pre Sales** Digital Proposal & Pre Sales | Digital Systems & Engineering Technologies | Engineering	**Leonardo S.p.A.** Via A. Agosta SNC 95121 Catania

Leonardo Cyber & Security Solutions

Lista delle Revisioni

Rev.	Numero Modifiche	Data	Descrizione	Autore
01.00	-	24/01/2022	Prima emissione	D. Leone
02.00	DCN222372	29/07/2022	Integrazione Rilascio SCMP 2.0.0	D. Leone
03.00	DCN222981	20/12/2022	Integrazione Rilascio SCMP 3.0.0	D. Leone
04.00	DCN230550	30/06/2023	Integrazione Rilascio SCMP 4.0.0	D. Leone
05.00	DCN231199	22/12/2023	Integrazione Rilascio SCMP 5.0.0	D. Leone
06.00	DCN240480	28/07/2024	Integrazione Rilascio SCMP 6.0.0	D. Leone
07.00	DCN240891	20/12/2024	Integrazione Rilascio SCMP 7.0.0	D. Leone

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Leonardo Services Documentation

1 Leonardo Services

Leonardo provides and manages various services divided into service families.
From a logical-functional perspective, these services can be divided into the following four macro-categories:

- Infrastructure as a Service (IaaS)
- Container as a Service (CaaS)
- Platform as a Service (PaaS)
- Hybrid Services

Below are listed the services for each macro category.

1.1 Infrastructure as a Service (IaaS)

Below is a list of services included in this category.
For details on each service, please see the dedicated section.

FAMILY	LIST OF SERVICES
Compute	Confidental Private IaaS
Compute	Confidential Shared-IaaS (VMs)

List of families and related IaaS services

1.2 Container as a Service (CaaS)

Below is a list of services included in this category.
For details on each service, please see the dedicated section.

FAMILY	LIST OF SERVICES
Compute	Kubernetes Confidential Computing

List of families and related CaaS services

1.3 Platform as a Service (PaaS)

Below is a list of services included in this category.
For details on each service, please see the dedicated section.

FAMILY	LIST OF SERVICES
Security	Identity & Access Management (IAM) Service
Security	Key Vault as a Service - Standard
Security	Endpoint Protection
Security	NGFW Platform
Security	PAM (Privileged Access Management)
Security	Intrusion Prevention System (IPS)
Security	PaaS Web Application Firewall (WAF)
Middleware	PaaS API Management
Middleware	Functions As A Service (FAAS)
Middleware	Jboss as a Service
Middleware	Spring boot as a Service
Middleware	PaaS Business Process as a Service
Middleware	PaaS CMS as a Service
Middleware	Semantic Knowledge Search
Data Protection	Backup Platform
Infra & Ops Platform	Multicloud Management Platform
Infra & Ops Platform	IT infrastructure Service Operations (Logging & Monitoring)
Infra & Ops Platform	PaaS Ticket Management Service
Infra & Ops Platform	PaaS Operations Management

FAMILY	LIST OF SERVICES
DevSecOps	Configuration Manager
DevSecOps	Test Automation
DevSecOps	Quality Code Analysis
DevSecOps	DevSecOps As A Service
DevSecOps	Qualizer DevSecOps
Big Data	Data Lake
Big Data	Business Intelligence Platform
Big Data	PaaS ETL Batch/Real time Processing
Big Data	Event Message
Big Data	Data Governance
Artificial Intelligence (AI)	Speech to Text
Artificial Intelligence (AI)	PaaS - AI Audio & Video Analytics
Artificial Intelligence (AI)	OCR
Artificial Intelligence (AI)	Text Analytics/NLP
Artificial Intelligence (AI)	Translation
Artificial Intelligence (AI)	AI Search - RAG
Artificial Intelligence (AI)	AI Platform
Artificial Intelligence (AI)	AI SLM/LLM
Collaboration	Instant Messaging
Database	PaaS SQL - PostgreSQL
Database	PaaS SQL - MariaDB
Database	PaaS SQL - MS SQL Server EE

FAMILY	LIST OF SERVICES
Database	PaaS SQL - MS SQL Server EE (BYOL)
Database	PaaS GraphDB
Database	PaaS NoSQL - MongoDB
Database	PaaS In Memory - Redis
Networking	PaaS CDN (Content Delivery Network)
Networking	PaaS Domain Name System (DNS)
Networking	Single public IP
Networking	L7 Load Balancer (regional)
Networking	Cloud interconnect Gold SW (10 Gbps max throughput)
Networking	Managed VPN Access Service
Networking	PaaS Client/Forward Proxy
Networking	PaaS Reverse Proxy
Storage	Block Storage (1000 GB) - High Density
Storage	Archive Storage (1000 GB)

List of families and related PaaS services

1.4 Hybrid Services

Below is a list of services included in this category.
For details on each service, please see the dedicated section.

FAMILY	LIST OF SERVICES
Hybrid	Edge Location - Pool Small (Confidential)
Hybrid	Bulk Data Transfer

List of families and related Hybrid services

2 Infrastructure as a Service (IaaS)

The following table lists the services included in the *Infrastructure as a Service (IaaS)* category.

FAMILY	LIST OF SERVICES
Compute	Confidental Private IaaS
Compute	Confidental Shared-IaaS (VMs)

List of families and related IaaS services

2.1 Compute Family

Below is the list of services belonging to the Compute family:

- Confidental Private IaaS
  - Pool Small (Confidential)
  - Pool Medium (Confidential)
  - Pool Large (Confidential)
  - Pool X-Large (Confidential)
- Confidential Shared-IaaS (VMs)
  - VM Small (Confidential)
  - VM Medium (Confidential)
  - VM Large (Confidential)
  - VM X-Large (Confidential)

2.1.1 Confidental Private IaaS

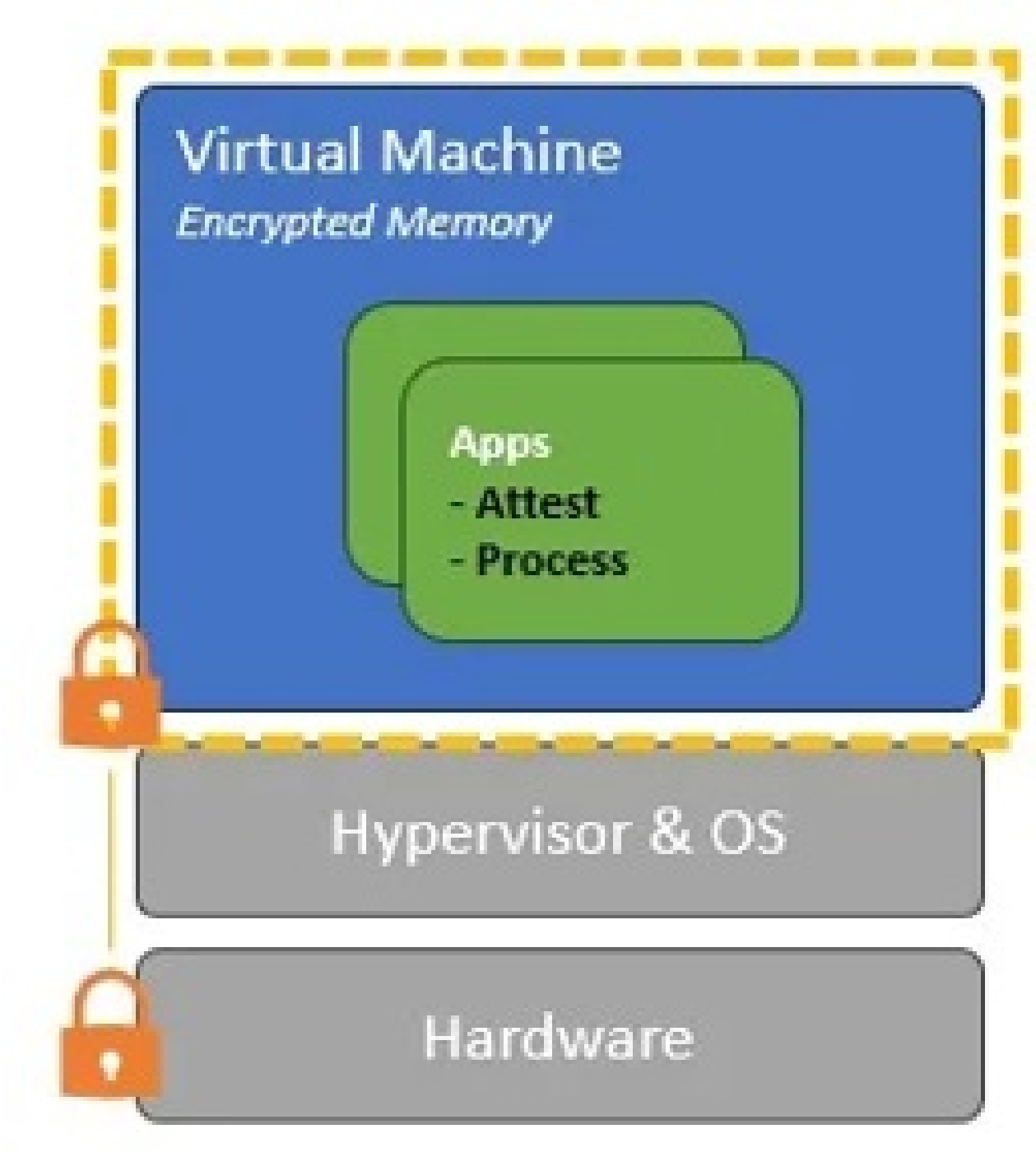


Figura 1 – Confidental Private IaaS Architecture

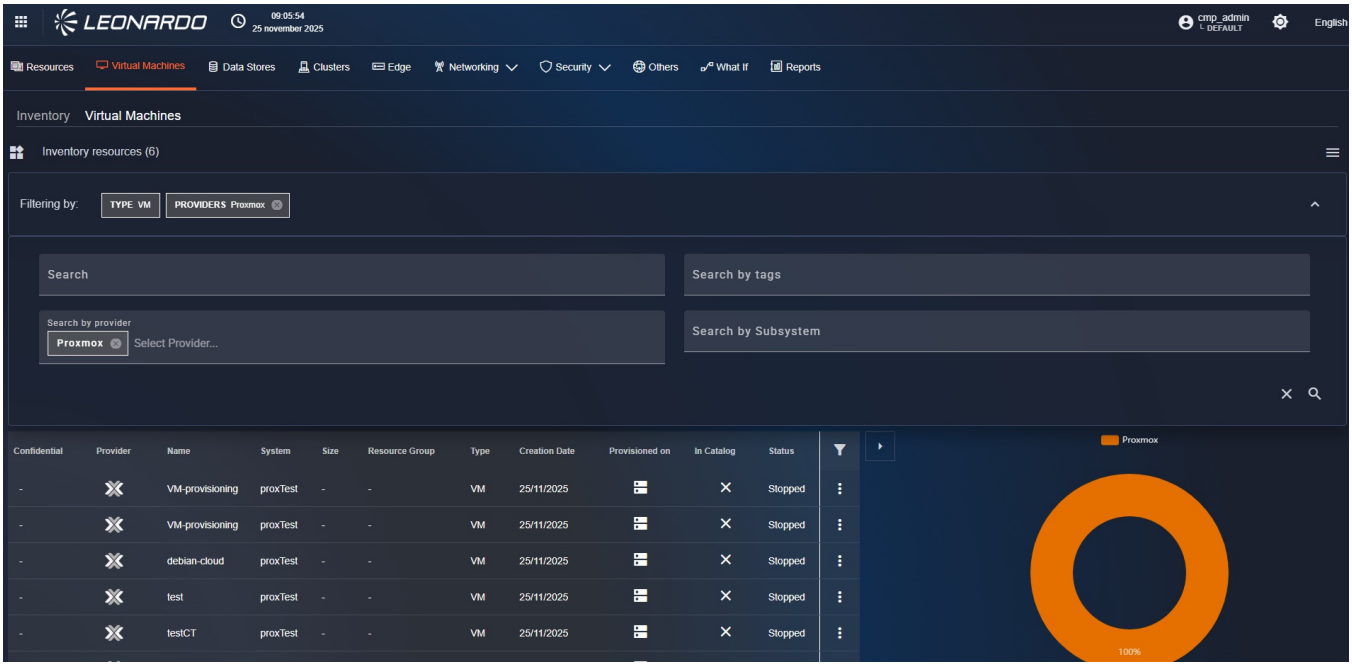


Figura 2 – Administration of Confidental Private IaaS

2.1.1.1 Services Description

These services, deveoloped by Leonardo, enable the provision of Private virtual computing environments (IaaS), i.e., on a pool of physical resources, dedicated and isolated for each individual customer, based on the use of bare metal computing instances.
Data from physical resources is encrypted and kept secure throughout all phases of use (at rest, in transit, and in use), leveraging the Confidential Computing paradigm.
The Private IaaS (Confidential) services are based on the use of the Proxmox virtualizer, which allows the provision of IaaS services with confidential computing capabilities.
Depending on the pool of computing resources required for each individual Organization, the most suitable service from the four available types can be selected:

Type	Contained Elements
Pool Small (Confidential)	3 Hosts (2xCPU 24 Core - 512 GB RAM - 32 TB SSD)
Pool Medium (Confidential)	6 Hosts (2xCPU 24 Core - 512 GB RAM - 32 TB SSD)
Pool Large (Confidential)	9 Hosts (2xCPU 24 Core - 512 GB RAM - 32 TB SSD)
Pool X-Large (Confidential)	12 Hosts (2xCPU 24 Core - 512 GB RAM - 32 TB SSD)

List of elements for each private IaaS pool

2.1.1.2 Features and Advantages

Private Cloud resources are dedicated exclusively to each customer.
The services use secure enclaves based on Trusted Execution Environments (TEEs) based on Confidential Hardware, which offer an advanced level of security for data in use, protecting it during processing.
They support advanced encryption of data at rest, in transit, and in use.
They use advanced remote attestation systems to verify the correctness of the TEE environment, isolating virtual machine memory from the host operating system and other malicious guests.

The services offer the following advantages:

- *Multi-Layer Security* → data security and confidentiality in dedicated environments. Workload isolation through advanced virtualization. Dedicated firewalls and network micro-segmentation
- *Faster Time-to-Market* → automated provisioning and rapid resource management.
- *Comprehensive control and centralized governance*: centralized monitoring and auditing for traceability.
- *Business continuity* → built-in backup, snapshot, and high availability (HA) features ensure service continuity in case of hardware failures. Minimizes operational risk for critical applications.

2.1.2 Confidential Shared-IaaS (VMs)

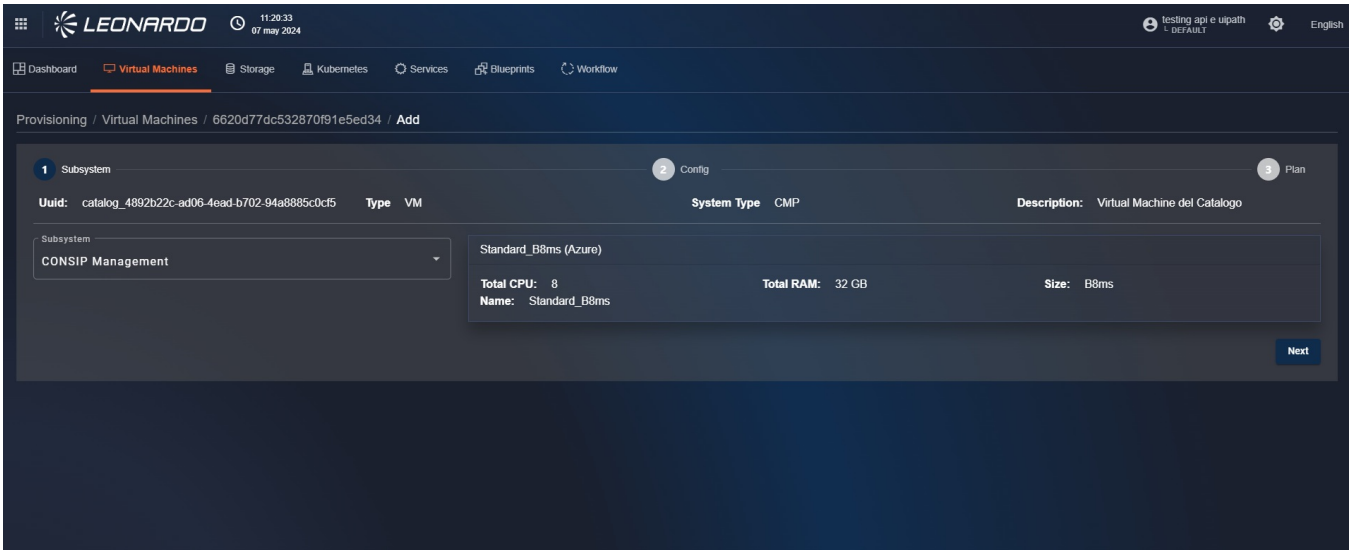


Figura 3 – How to create a VM - Step 1

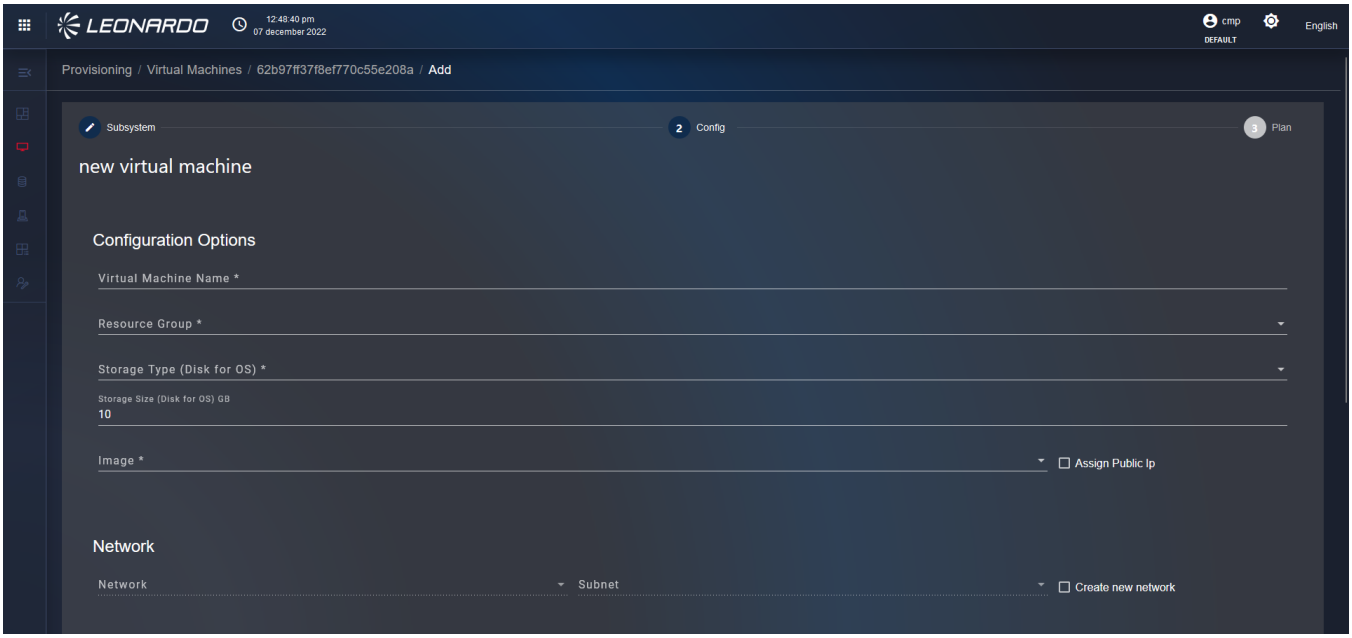


Figura 4 – How to create a VM - Step 2

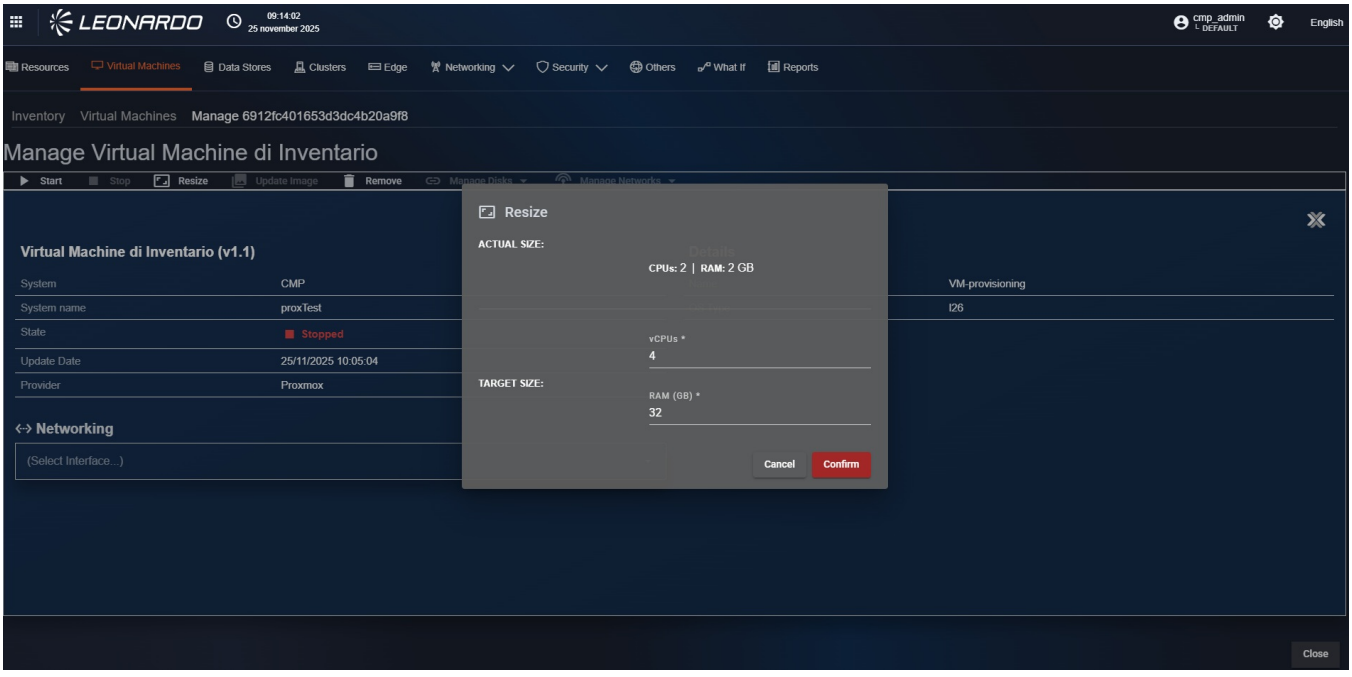


Figura 5 – How to manage a VM

2.1.2.1 Services Description

These services, deveoloped by Leonardo, enable organizations or individuals to deploy and manage Virtual Machines (VMs) without the need to maintain their own physical servers. They provide users with virtualized computing resources—such as CPU, memory, storage, and networking—hosted on a managed and shared physical infrastructure.
The services are implemented using the Proxmox virtualizer, with a customized version offering Confidential Computing capabilities. Each user operates in a logically isolated environment, sharing the underlying hardware with other tenants. Data from physical resources is encrypted and kept secure during all phases of use (at rest, in transit, and in use), leveraging the Confidential Computing paradigm.
Depending on the resource pool required by each individual organization, the most suitable service can be selected from the four available types:

Type	Contained Elements
VM Small (Confidential)	2 Vcpu 4 GB RAM
VM Medium (Confidential)	4 Vcpu 8 GB RAM
VM Large (Confidential)	8 Vcpu 16 GB RAM
VM X-Large (Confidential)	16 Vcpu 32 GB RAM

List of elements for each VMs type

2.1.2.2 Features and Advantages

The services offer the following features:

- *High Availability (HA)* → automatic VM failover in case of node failure when HA is enabled.
- *Backups* → scheduled full or incremental backups using Proxmox Backup Server integration.
- *Templates* → predefined OS images (e.g., Ubuntu, Debian, CentOS, Windows Server) for rapid VM deployment.
- *User Access* → secure web interface and console access (noVNC/SPICE).
- *Monitoring* → real-time performance metrics and resource usage monitoring.
- *Security and isolation* → tenant isolation using VLANs and hypervisor-level separation.
- *Access Control* → role-based access control (RBAC).
- *Data protection* → encrypted storage backends and secure backup transfer protocols.
- *Audit logging* → comprehensive logging of user and system activities for compliance and troubleshooting.
- *Provisioning* → fully automated via API or web interface.

The service architecture is built on a Proxmox cluster consisting of multiple physical nodes connected via a high-speed network.
Each node contributes CPU, memory, and storage resources to a shared resource pool managed by Proxmox VE.
The main components of the service are:

- *Hypervisor* → Proxmox VE with KVM (for full virtualization).
- *Cluster management* → centralized management via Proxmox Cluster Manager with quorum-based consistency.
- *Storage backend* → shared storage using Ceph supporting redundancy, scalability.
- *Networking* → virtual networking implemented through Linux bridges or VLAN tagging, with optional SDN integration for advanced network segmentation.
- *Management interface* → Web-based GUI and REST API for VM lifecycle operations (creation, modification, deletion, migration, snapshot, backup, restore).

The services offer the following advantages:

- *Cost reduction* → no upfront investment in physical hardware, expensive hypervisor licenses, or datacenter infrastructure.
- *Flexibility* → resources (CPU, RAM, storage) can be scaled up or down quickly according to business needs.
- *Faster Time-to-Market* → virtual environments can be provisioned quickly. Ideal for testing, development, or rapid deployment of new services and applications. It reduces provisioning and approval times inside the organization.
- *Capital and resource optimization* → unused resources are dynamically shared across tenants, maximizing infrastructure efficiency. Better capital utilization compared to underused dedicated environments.
- *Business Continuity* → built-in backup and high availability (HA) features ensure service continuity in case of hardware failures. Minimizes operational risk for critical applications.

3 Container as a Service (CaaS)

The following table lists the services included in the *Container as a Service (CaaS)* category.

FAMILY	LIST OF SERVICES
Compute	Kubernetes Confidential Computing

List of families and related CaaS services

3.1 Compute Family

Below is the list of services belonging to the Compute family:

- Kubernetes Confidential Computing

3.1.1 Kubernetes Confidential Computing Service

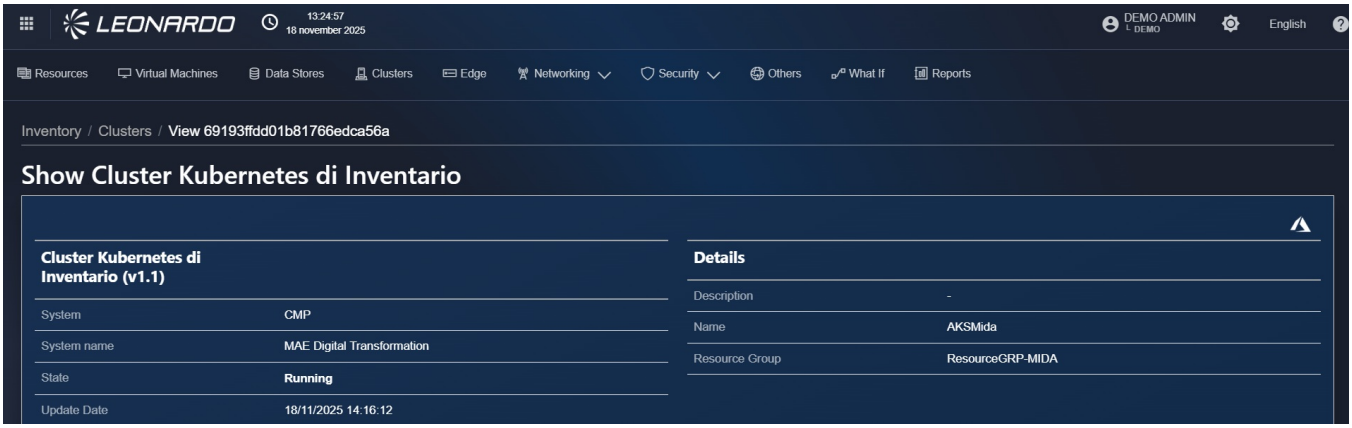


Figura 6 – Kubernetes Confidential Computing Overview

3.1.1.1 Service Description

This service, deveoloped by Leonardo, provides an automated Kubernetes platform for orchestrating private and secure containers, designed to manage containerized applications in highly regulated environments or with confidentiality requirements.
The platform ensures automation of node scaling, monitoring, and high availability management, without requiring any operational activities on the customer's part.
The cluster capacity can be increased or decreased through automated scaling mechanisms based on predefined node block increments, in line with the proposed SKU sizing.
This approach ensures architectural consistency, predictable performance, and alignment with the design constraints of the underlying infrastructure.

Type	Contained Elements
Kubernetes cluster	15 node workers with 8 GB RAM for each unit

Contained Elements for the Kubernetes Confidential Computing Service

3.1.1.2 Features and Advantages

Implementation requires a combination of hardware certified for Confidential Computing, a private, security-hardened Kubernetes infrastructure, and a suite of observability and governance tools to maintain complete control over the container lifecycle.

Features included:

- *Data protection* → The operating system is configured to ensure protection at all stages: data in memory, through full disk encryption; data in transit, using secure and encrypted communication protocols; and data in use, adopting Confidential Computing practices and secure execution environments.
- *Secure enclaves* → Enforces isolation and encryption, ensuring that only authorized parties can access data.
- *Trusted execution environments (TEEs)* → Adds a secure computing environment, protecting data from external threats.
- As a managed Kubernetes solution, the customer does not have to worry about managing the infrastructure and its complexity, as the infrastructure layer is managed by Leonardo throughout the service lifecycle.

The service includes a comprehensive set of security tools and services designed to ensure the secure usage of containers running on the Managed Service for Containers.
It implements a multilayered infrastructure security model that safeguards the entire container lifecycle—from image creation to runtime execution—ensuring platform integrity, operational compliance, and consistent protection of containerized workloads.

Platform security:

- Real-time security monitoring and vulnerability scanning are implemented through the use of StackRox, providing continuous assessment of container images and runtime workloads. The platform enables automated detection of CVEs, policy violations, and security threats ensuring a secure, compliant, and monitored environment without operational intervention.
- Host-level malware and virus detection to secure container nodes with EDR provided by Bitdefender
- Kernel-level hardening and enforcement of mandatory security profiles to isolate workloads (by design)

Access Security:

- Identity-based access controls (RBAC) and integration with centralized identity management systems.

Compliance, Monitoring, and Auditing:

- Centralized logging and security-related events are forwarded directly to the SOC team SIEM, enabling correlation, alerting, and continuous security monitoring.

The service offers the following advantages:

- *Security and confidentiality of containerized applications* → end-to-end encryption, confidential computing for workloads, container isolation on dedicated nodes with hardware-based protection, integrated security policies, and advanced RBAC.
- *Centralized cluster control and governance*.
- *Scalability and flexibility*.
- *Integration with multicloud and legacy environments*.

4 Platform as a Service (PaaS)

4.1 General features

4.1.1 Auto Scaling & Scaling-to-Zero

The PaaS services described in this document are designed to run on orchestrated, cloud-native platforms where horizontal auto scaling is a native capability. Auto scaling dynamically adjusts the number of active instances in response to application load so that services can absorb traffic peaks while avoiding unnecessary over-provisioning during off-peak periods.

At the platform level, an Horizontal Pod Autoscaler (HPA) or analogous controller continuously observes key metrics exposed by the workloads and the underlying infrastructure. These metrics commonly include CPU utilization, memory consumption, request rate, queue or backlog depth, and custom application indicators exported through standard monitoring interfaces. When the measured values exceed or fall below configured thresholds, the controller increases or decreases the replica count within the minimum and maximum limits defined for each service.

The same mechanism applies to many PaaS building blocks beyond purely stateless functions. These components can be configured to scale out when demand increases, distributing traffic across additional instances, and to scale in when demand subsides, consolidating activity on fewer instances. This behavior reduces the need for manual capacity planning, while still allowing organizations to define guardrails such as per-tenant quotas, reserved capacity, or upper bounds imposed by licensing and compliance requirements.

For suitable workloads, several PaaS services also support scaling-to-zero. When a workload becomes idle and there are no active requests or tasks to process, the orchestration layer can progressively drain and stop all runtime instances associated with that service, leaving only the control and configuration plane active. In this state, compute capacity is released instead of being reserved for an idle service, which reduces the operational surface exposed to potential threats and improves infrastructure utilization. When new load arrives after a scale-to-zero phase, the platform automatically recreates the necessary runtime instances and starts routing work to them as soon as they become healthy; this can introduce a controlled start-up latency, which can be mitigated for latency-sensitive services by configuring a small minimum number of always-on instances.

Scaling-to-zero applies to workloads whose runtime instances can be stopped while still meeting durability and availability requirements. State-heavy services such as relational databases, message brokers, and some analytics engines typically maintain at least one active replica or a minimal cluster footprint to guarantee durability, failover, and predictable performance characteristics. For these services, elasticity is achieved through controlled horizontal scaling of nodes, vertical tuning of resource allocations, and scheduled maintenance windows, with the serving tier remaining continuously available.

In all scenarios, auto scaling integrates with the platform's monitoring, logging, and governance capabilities. Scaling events are traceable, auditable, and can be correlated with business and security metrics to validate that capacity changes remain compliant with corporate policies.

4.1.2 Security Patching

Security patching is part of the Vulnerability Management (VM) process and concerns the operational activities involved in applying software updates (called patches or fixes) designed to resolve security vulnerabilities found in operating systems, applications, firmware, or other IT components.

In practice, security patching:

- fixes security flaws that could be exploited by attackers.
- improves system stability and reliability.
- reduces the risk of attacks such as malware, ransomware, or unauthorized access.

These activities are carried out according to established schedules (Periodic VM) or as a result of risk analyses, internal/external alerts, or specific needs in response to urgent patches (such as emergency patches or zero-day patches), i.e., non-periodic (on-demand) VM.

The VM process pursues the following objectives:

- identifying and assessing potential weaknesses (vulnerabilities) in the technological infrastructure.
- verifying compliance with security standards and corporate policies.
- checking the robustness of networks, systems, or applications against the possibility of exploitation by new cyber threats. evaluating the effectiveness of remediation actions taken to improve the security of systems, networks, or applications.

The Security Operation Center (SOC) manages the VM process by performing the following activities:

- defines the scope of Vulnerability Management activities.
- contributes to planning the activities.
- relays any alerts or warnings from external or internal sources.
- analyzes the reports produced by the SOC.
- validates the remediation plan.

The SOC, for its part, performs the following operational activities:

- collects vulnerability alerts from both internal and external sources.

- gathers information about the affected assets.
- plans, together with the CISO, security assessments aimed at identifying the technological perimeter subject to VM.
- carries out VA/PT activities and prepares the related reports.

The phases of the vulnerability management process are:

a) Planning b) Execution of activities c) Definition of the remediation plan d) Implementation of the remediation plan e) Monitoring

In the specific case of PaaS services provided on the Kubernetes cluster, VM and security patching activities make use of the StackRox tool. StackRox is the solution used to verify container security, providing capabilities to identify critical vulnerabilities in managed StackRox environments and supporting the processes of checking, monitoring, and correcting identified security issues:

- Vulnerability Management
- Network Segmentation
- Compliance
- Detection and Response

4.1.3 Encryption

The Data at Rest Encryption requirement—i.e., ensuring the confidentiality of data stored on the infrastructure's disks through encryption—is fulfilled by integrating the storage solutions, for both block storage and object storage, with a centralized Key Management System (KMS).

Specifically, for block storage, the confidentiality of data within Persistent Volumes (PV) created on the Kubernetes cluster infrastructure is ensured through the Ceph storage solution, which supports volume encryption. The enablement and configuration of the integration with the external KMS is performed at the storage class level, using the Key Management Interoperability Protocol (KMIP).

For object storage, the confidentiality of stored data is guaranteed through the native integration provided by the storage application solution (MinIO) with the KMS. MinIO supports automated SSE-KMS encryption for all objects written to a bucket, using a specific external key (EK) stored in the external KMS. MinIO encrypts stored data using a unique key retrieved from the KMS. The KMS is responsible for storing and managing the master key used to protect the data-encryption key utilized by the MinIO system.

All data-transmission communications are secured in accordance with the Data in Transit Encryption requirement. Protection is ensured through the mandatory use of the Transport Layer Security (TLS) protocol across all network channels. TLS provides confidentiality, integrity, and authentication for data exchanged between system components.

4.1.4 Replication

The protection of data integrity and availability within the PaaS platform is ensured by integrating the Kubernetes cluster with a centralized backup service delivered through a Veeam solution.

To integrate Veeam with Kubernetes clusters, the Veeam architecture must include a Media Agent responsible for executing the actual backup of the K8S cluster. Backup operations are performed through APIs exposed by the K8S infrastructure.

The Kubernetes objects subject to backup are:

- the distributed etcd database hosted on the master nodes.
- the Persistent Volumes (Block & File Storage) provided by the Ceph service.

Given the criticality of the etcd database - which manages and stores the state and configuration of all objects within K8S - its backup is performed at a very high frequency (several times per hour).
Furthermore, for certain types of applications (e.g., PostgreSQL databases) running on the K8S platform, achieving Application-Consistent backups requires integrating pre/post-backup scripts.
These scripts place the application in a “quiesce” (read-only) state for the duration of the volume snapshot, and then perform an “unquiesce” operation to restore normal read-write activity.
The Veeam backup platform allows the configuration of these pre/post scripts for each application requiring this approach to ensure Application-Consistent backup execution.

4.1.5 Serverless Managed Container Platform

4.1.5.1 Integration with Software Development Processes

The service facilitates integration with software development processes by providing declarative Infrastructure as Code (IaC) blueprints. Developers can describe the entire deployment in configuration files, which are then applied through the management portal or APIs. This allows automatic provisioning of clusters, networking, and container runtimes. Continuous deployment is supported through integration with common CI/CD tools such as GitHub Actions, GitLab CI, Azure DevOps, and Jenkins. Pipelines can push new container images to the registry, and the platform automatically redeploys workloads. Rollbacks are possible by reverting to previous IaC templates.

Progressive rollout strategies are supported. Rolling updates can be configured to gradually replace old container replicas with new ones, with parameters such as batch size, wait time, and health checks. Blue/green deployments are possible by running two environments simultaneously and switching traffic through Envoy Proxy routing rules. Canary releases can be achieved by directing a percentage of traffic to a new version, monitoring metrics such as latency and error rate before completing the rollout.

Debugging and development support is provided through integration with popular IDEs such as Visual Studio Code, IntelliJ, and Eclipse. Developers can deploy, monitor logs, and debug containers directly from their IDE. Dapr sidecar provides observability features including tracing, metrics, and logging. Logs are streamed to centralized monitoring services, and health probes are automatically configured to ensure resilience. Failover to replicas ensures minimal downtime during debugging or patching.

4.1.5.2 High-Level User Manual

Getting Started

Users provision the service by logging into Leonardo management portal, navigating to the Serverless Managed Container Platform, and creating a new service instance. They select the region, security context, and resource limits. Alternatively, the API can be used to provision services by submitting configuration files.

Deploying with IaC Blueprints

Applications are defined in YAML or JSON configuration files that describe containers, scaling rules, and networking. These files are applied through the portal or CLI. For example, a configuration may specify replicas, autoscaling parameters, and port mappings. Once applied, the platform provisions the resources automatically.

Configuring Networking

Containers are reachable via HTTPS by default. Supported protocols include HTTP/1, HTTP/2, and arbitrary TCP ports. Developers can configure ingress rules to expose services externally.

Scaling and Resilience

Autoscaling is supported through declarative configuration based on CPU or memory thresholds. The platform supports scale-to-zero, meaning no compute costs are incurred when applications receive no requests. Replication ensures that containers are deployed across multiple nodes, with automatic failover in case of deactivation.

Security and Maintenance

Leonardo is responsible for patching the cluster control plane and the operating system of underlying virtual machines. Users can deploy services in isolated security contexts. Maintenance notifications are provided between 24 and 72 hours in advance, except for critical security patches. Users may request postponement of scheduled maintenance.

Debugging and Monitoring

Logs can be accessed through the portal or CLI. Metrics and traces are available through Dapr integration. IDE plugins allow developers to attach debuggers directly to running containers. Continuous monitoring ensures that applications remain resilient and available.

4.2 List of services

The following table lists the services included in the *Platform as a Service (PaaS)* category.

FAMILY	LIST OF SERVICES
Security	Identity & Access Management (IAM) Service
Security	Key Vault as a Service - Standard
Security	Endpoint Protection
Security	NGFW Platform
Security	PAM (Privileged Access Management)
Security	Intrusion Prevention System (IPS)
Security	PaaS Client/Foward Proxy
Middleware	PaaS API Management
Middleware	Functions As A Service (FAAS)
Middleware	Jboss as a Service
Middleware	Spring boot as a Service
Middleware	PaaS Business Process as a Service
Middleware	PaaS CMS as a Service
Middleware	Semantic Knowledge Search
Data Protection	Backup
Infra & Ops Platform	Multicloud Management Platform

Leonardo Cyber & Security Solutions

FAMILY	LIST OF SERVICES
Infra & Ops Platform	IT infrastructure Service Operations (Logging & Monitoring)
Infra & Ops Platform	PaaS Ticket Management Service
Infra & Ops Platform	PaaS Operations Management
DevSecOps	Configuration Manager
DevSecOps	Test Automation
DevSecOps	Quality Code Analysis
DevSecOps	DevSecOps As A Service
DevSecOps	Qualizer DevSecOps
Big Data	Data Lake
Big Data	Business Intelligence Platform
Big Data	PaaS ETL Batch/Real time Processing
Big Data	Event Message
Big Data	Data Governance
Artificial Intelligence (AI)	Speech to Text
Artificial Intelligence (AI)	PaaS - AI Audio & Video Analytics
Artificial Intelligence (AI)	OCR
Artificial Intelligence (AI)	Text Analytics/NLP
Artificial Intelligence (AI)	Translation
Artificial Intelligence (AI)	AI Search - RAG
Artificial Intelligence (AI)	PaaS - AI Platform
Artificial Intelligence (AI)	AI SLM/LLM
Collaboration	Instant Messaging

FAMILY	LIST OF SERVICES
Database	PaaS SQL - PostgreSQL
Database	PaaS SQL - MariaDB
Database	PaaS SQL - MS SQL Server EE
Database	PaaS SQL - MS SQL Server EE (BYOL)
Database	PaaS GraphDB
Database	PaaS NoSQL - MongoDB
Database	PaaS In Memory - Redis
Networking	PaaS CDN (Content Delivery Network)
Networking	PaaS Domain Name System (DNS)
Networking	Single public IP
Networking	L7 Load Balancer (regional)
Networking	Cloud interconnect Gold SW (10 Gbps max throughput)
Networking	Managed VPN Access Service
Networking	PaaS Client/Forward Proxy
Networking	PaaS Reverse Proxy
Storage	Block Storage (1000 GB) - High Density
Storage	Archive Storage (1000 GB)

List of families and related PaaS services

4.3 Security Family

Below is the list of services belonging to the Security family:

- Identity & Access Management Service

- Key Vault as a Service - Standard
- End point protection
- NGFW Platform
- PAM (Privileged Access Management)
- Intrusion Prevention System (IPS)
- PaaS Web Application Firewall (WAF)

4.3.1 Identity & Access Management (IAM) Service

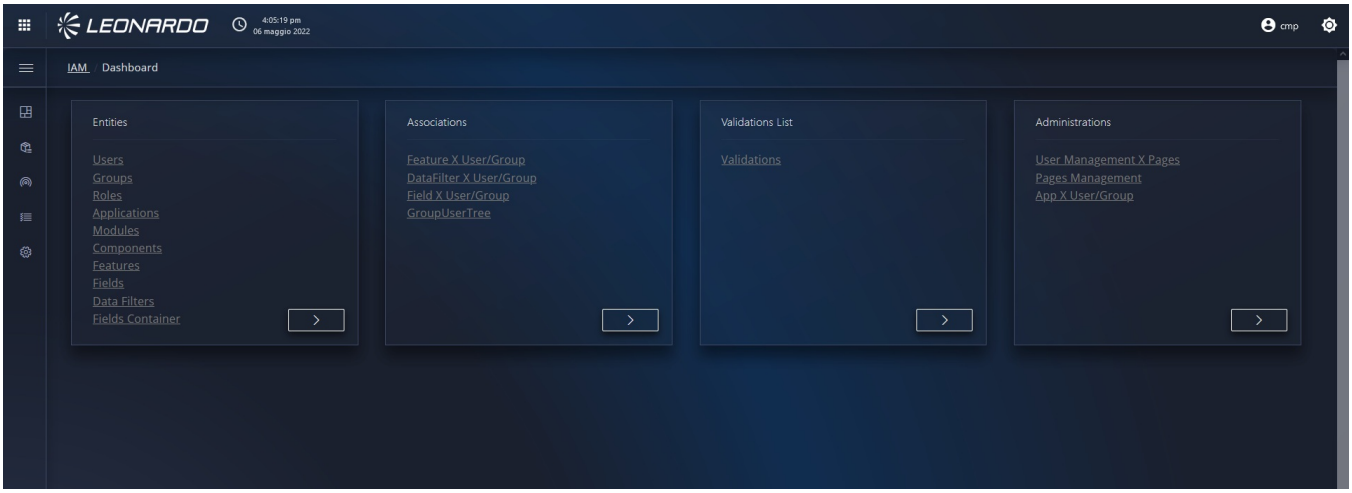


Figura 7 – Identity & Access Management Service (IAM) Overview

4.3.1.1 Service Description

The Service, developed by Leonardo, provides an essential level of security for identity and access management, ensuring foundational protection against unauthorized access.
It manages single sign-on access to guarantee access to all protected resources with a single authentication. It supports standard OIDC/OAUTH and SAML protocols for easy integration with applications and products.
It enables first-level authentication with username/password and second-level authentication with multi-factor authentication based on Time-based One-Time Password (TOTP) protocols.
It manages access authorization to system-protected resources only for users with rights to use them according to the Role-based Access Control (RBAC) and Attribute-based Access Control (ABAC) paradigms. Integration with external user repositories (LDAP or Active Directory) is also available.
It manages the user lifecycle and related authorizations via the console.

The service is offered with the following unit metric: *100 concurrent users*.

4.3.1.2 Features and Advantages

The main features and functionalities of the service are:

- *Identity Management*
  - User Management → creation, modification, and deletion of users; management of user profiles (name, email, custom attributes, roles, etc.); import/export of users from external directories (LDAP, Active Directory).
  - Identity Federation → integration with external providers via LDAP or Active Directory; two-way or one-way synchronization of users and roles.
  - Account Management UI → self-service portal for users to update profiles and passwords, manage devices and active sessions, and view permissions.
- *Access Management*
  - Single Sign-On (SSO) / Single Logout (SLO).
  - Multi-Factor Authentication (MFA).
  - Delegated Authentication (Identity Brokering).
  - Role-Based Authorization (RBAC) and policies.
- *Protocol and Integration*
  - Support for standard protocols, such as OpenID Connect (OIDC), OAuth 2.0, and SAML 2.0.ì
  - Ability to integrate with API Gateways, microservices, and web frontends.
- *Security and Management*
  - Session and Token Management.
  - Password Policies.
  - Events and Auditing.
  - Scalability and High Availability → distributed architecture, with support for clustering and replication.
- *Extensibility*
  - REST API for automated user, role, and client management.
  - SPI (Service Provider Interfaces) for extending authentication, validation, or provisioning capabilities.
  - Ability to implement custom authenticators or connect to external systems.

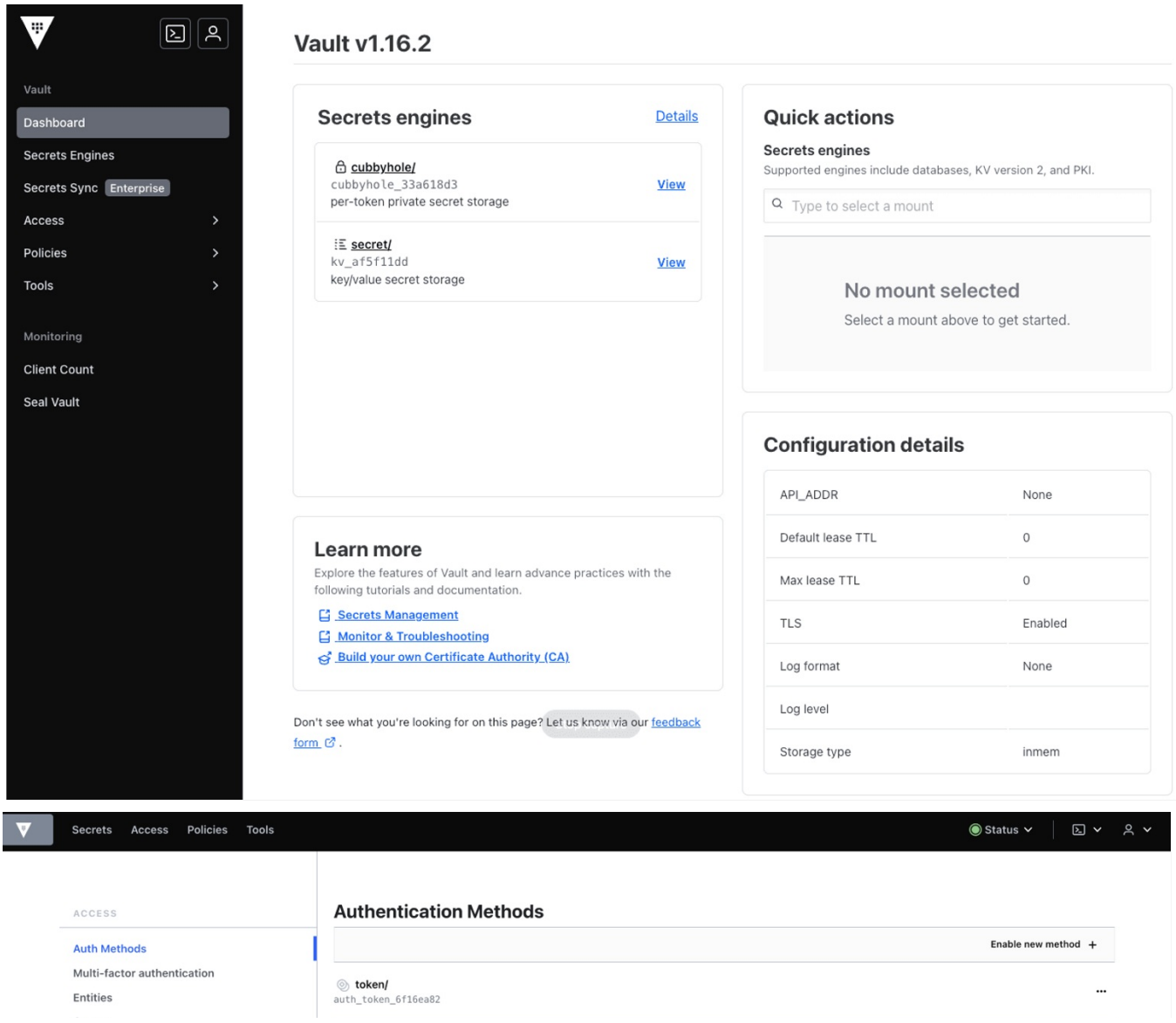
The service offers the following advantages:

- *Improved overall security* → Centralizing authentication reduces the risk of vulnerabilities distributed across

applications.

- *Reduced maintenance and development costs* → A single, centralized platform reduces the complexity and duplication of authentication code across applications.
- *Agility and Scalability* → Increased speed of onboarding new applications thanks to the use of standard protocols (OIDC, SAML, OAuth2).
- *Maintainability and Standardization* → Use of standard protocols (OIDC, SAML, OAuth2) that eliminate proprietary implementations and facilitate interoperability.

4.3.2 Key Vault as a Service - Standard



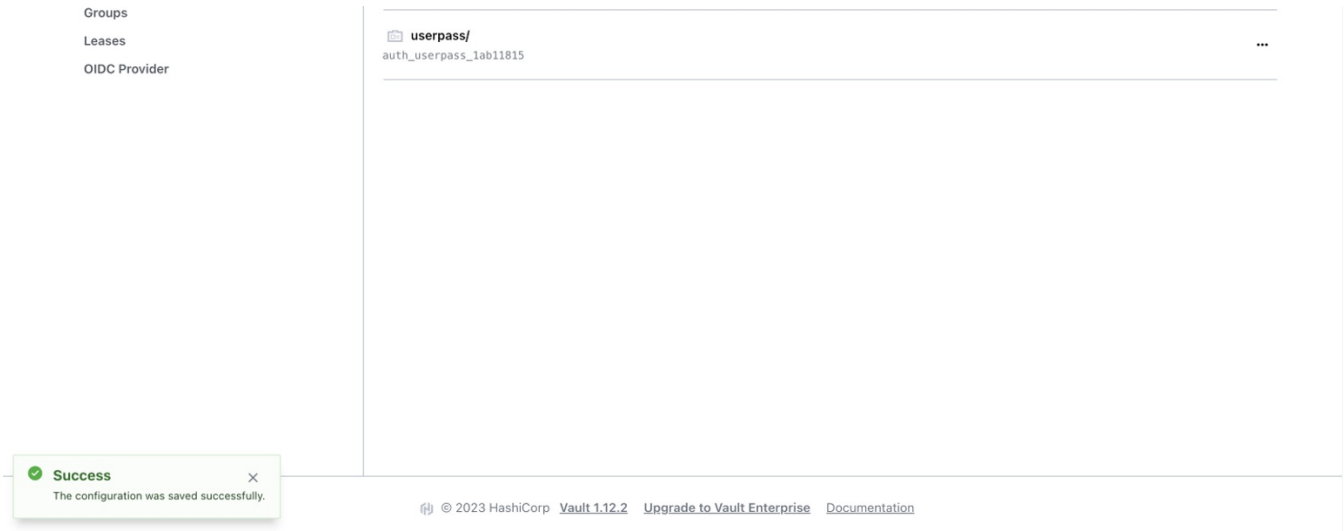


Figura 8 – Key Vault as a service

Overview

4.3.2.1 Service Description

The service, based on Hashicorp Vault technology, provides a secure cloud repository (Vault) for storing and managing credentials and passwords used by cloud applications without having to manually install and manage dedicated IaaS machines.
The service consists of a software platform that enables centralized and automated management of encryption keys, secrets, and certificates, with access controlled by identity-based authentication and authorization methods.
It also allows organizations to significantly simplify key lifecycle management, ensuring centralized control while leveraging the native cryptographic capabilities of KMS providers.

The service is offered with the following unit metric: *500 clients*.

4.3.2.2 Features and Advantages

The main features and functionalities of the service are:

- *Secure Secret Storage* → Key/value secrets are stored in Key Vault As A Service in encrypted form, ensuring their integrity in the event of unauthorized access to raw storage.
- *Dynamic Secrets* → Key Vault As A Service can generate secrets on demand to allow users and/or applications to access different systems.
- *Data Encryption* → Key Vault As A Service can encrypt and decrypt workloads running on the customer infrastructure without archiving them, managing the entire lifecycle of the cryptographic material used in the encryption process.
- *Leasing and Renewal* → Key Vault As A Service associates a lease with each key or secret managed, which will

result in its automatic revocation upon expiration and which can be renewed by clients through the integrated APIs provided by the platform.

- *Revocation* → Key Vault As A Service has integrated support for revoking keys and secrets, which can be revoked individually or in bulk (e.g., all keys of a specific user), for example in case of compromise.

The service offers high availability and geographic replication.
The main workflow of Key Vault as a Service consists of four phases:

- *Authentication* → The process by which a client provides information that Key Vault as a Service uses to determine the authenticity of the requester. Once the client is authenticated, the system generates a token that is associated with the relevant policy.
- *Validation* → Validation occurs through trusted third-party sources, such as Active Directory, LDAP, and Okta.
- *Authorization* → The client is then associated with the Key Vault as a Service security policy, which consists of a set of rules that define which API endpoints a user, machine, or application is allowed or denied access to with its token.
- *Access* → Key Vault as a Service then grants access to keys and encryption features, secrets, and certificates.

The service offers the following advantages:

- *Risk reduction* → thanks to automatic key rotation and secret lifecycle management, it increases the protection of sensitive data, simplifies regulatory compliance and reduces the risk of human errors.
- *Operational efficiency and cost reduction* → less internal management, automation and standardization, scalability without hardware investment.
- *Optimized time-to-market* → developers focus on code, not key management; also enables secure applications to be delivered faster, improving agility and innovation.
- *Improved trust and reputation* → audit and traceability to demonstrate secure secret management to stakeholders or customers.
- *Cryptographic and standardized compliance* → can be configured to use FIPS (Federal Information Processing Standards) validated cryptographic modules, ensuring that all encryption, signing, HMAC and key derivation operations comply with the standards.

4.3.3 Endpoint Protection Service

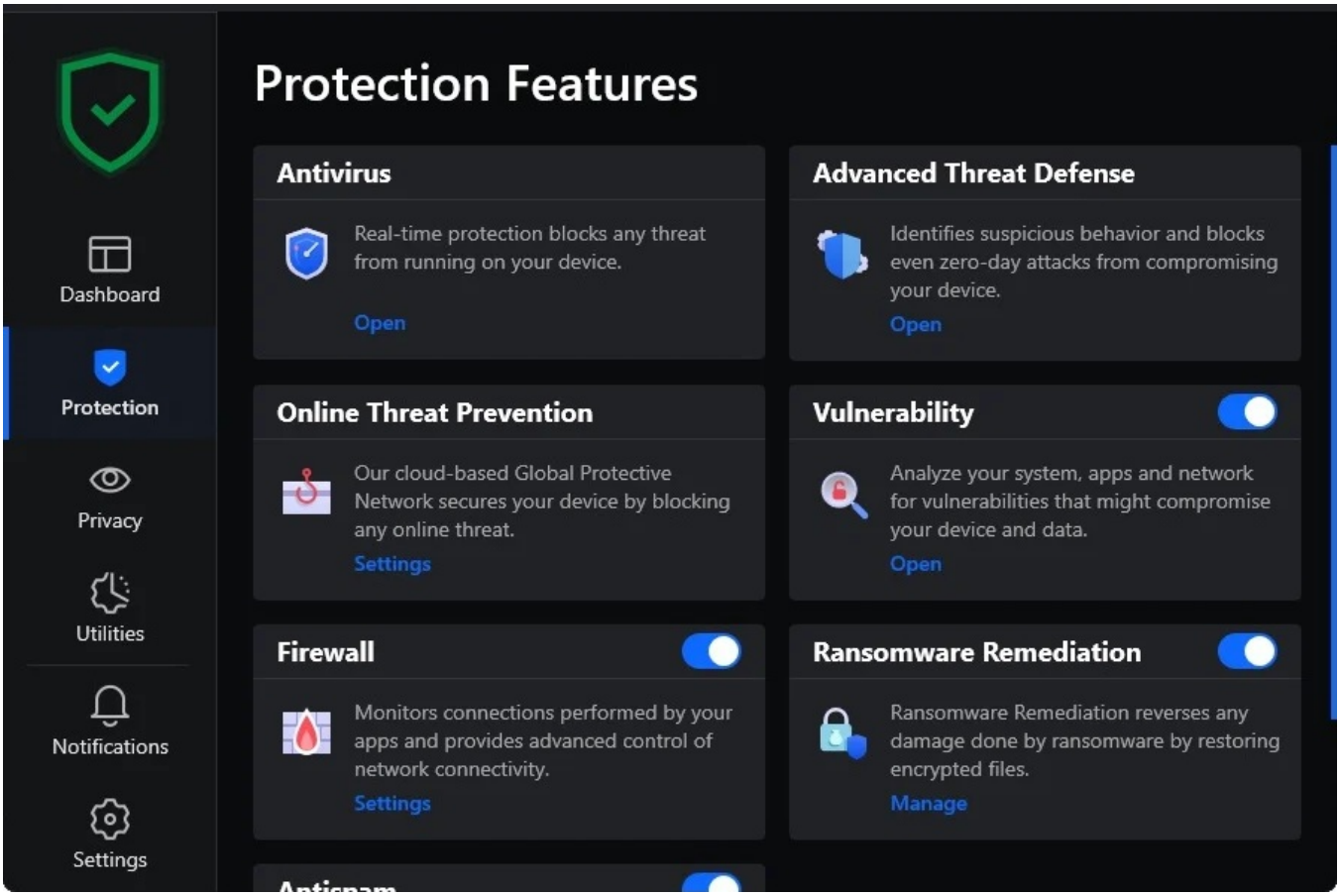


Figura 9 – Endpoint Protection Service Overview

4.3.3.1 Service Description

Powered by Bitdefender technology, the Endpoint Protection (EPP) Service offers comprehensive protection for endpoint devices against malware, ransomware, and other threats. The service provides a cloud-delivered, scalable, and centrally managed EPP providing multi-layered protection to broad spectrum of cyber threats.
The service is delivered as a managed PaaS solution, offering continuous protection and simplified administration for organizations seeking robust endpoint security without the overhead of managing on-premise security infrastructures.

The service is offered with the following unit metric: *100 endpoints*.

4.3.3.2 Features and Advantages

The Endpoint Protection service offers a full suite of integrated security functions aimed at ensuring endpoint resilience and threat visibility across the organization:

- *Antivirus and anti-Malware protection* → continuous real-time scanning, heuristic analysis, and signature-based detection to identify and block known and emerging threats.
- *Behavioral and threat analysis* → advanced behavioral monitoring and threat intelligence integration to detect and mitigate unknown or zero-day attacks.
- Personal firewall → endpoint-level firewall providing granular control over inbound and outbound network connections, preventing unauthorized access and lateral movement.
- Web protection and URL filtering → protects users from malicious or fraudulent websites by evaluating URLs and blocking access to unsafe domains.
- *Application control* → allows administrators to define and enforce policies for approved and restricted applications, reducing the risk of untrusted software execution
- Patch and vulnerability management → automates the identification, prioritization, and deployment of patches and updates for operating systems and third-party applications.
- *Centralized management console* → offers unified visibility and control over all protected endpoints, enabling configuration management, alert handling, policy enforcement, and reporting from a single interface.
- *Incident Detection and Response (EDR Integration)* → provides integration capabilities with Endpoint Detection and Response tools to enhance investigation and automated remediation processes.
- *Reporting and compliance monitoring* → delivers customizable reports and dashboards to support compliance with organizational and regulatory security standards.

The main components of the service are:

- *Endpoint Agent* → a lightweight client installed on each endpoint device that performs local threat detection, policy enforcement, and communication with the management server. *Management and control console* → the central administrative interface, hosted within the PaaS environment, responsible for policy management, configuration, event correlation, and reporting.
- *Threat intelligence service* → continuously updated databases and analytics engines that provide real-time intelligence on emerging threats, indicators of compromise (IoCs), and reputation data.
- *Policy management module* → defines and distributes security configurations and operational rules across endpoint agents, ensuring uniform protection and compliance.
- *Update and Patch Repository* → centralized repository for antivirus signatures, security updates, and software patches, ensuring endpoints are continuously updated with the latest protection mechanisms. *Event correlation and logging module* → collects and analyzes security events from all endpoints, correlating data to detect anomalies and trigger automated responses when threats are identified. *Integration and API layer* → enables interoperability with other PSN security services (such as SIEM, SOC, or IAM systems) for advanced monitoring, alerting, and orchestration.

The service offers the following advantages:

- *Comprehensive, multi-Layered protection* → combines antivirus, anti-malware, firewall, web protection, and application control for complete endpoint security coverage.
- *Centralized management and visibility* → a unified management console provides real-time visibility across all endpoints, simplifying administration and reducing operational complexity.
- *Continuous updates and threat intelligence* → the service is continuously updated with the latest threat intelligence feeds, ensuring protection against emerging and zero-day threats.
- *Automated patch and vulnerability management* → streamlines the detection and remediation of system vulnerabilities, maintaining secure and compliant endpoint configurations.
- *Advanced detection and Rrsponse capabilities* → integrates with EDR (Endpoint Detection and Response) systems for enhanced detection, investigation, and automated threat remediation.
- *High availability and resilience* → built on a redundant and fault-tolerant cloud infrastructure to ensure uninterrupted protection and service continuity.
- *Rapid incident response and containment* → provides automated isolation and remediation of compromised endpoints, minimizing attack spread and impact.
- *Integration with security ecosystem* → supports API-based integration with SIEM, SOC, and IAM systems for centralized event correlation and coordinated response.
- *Policy standardization across devices* → ensures consistent security policies and enforcement across heterogeneous endpoint environments (Windows, macOS, Linux, mobile).
- *Detailed reporting and analytics* → offers customizable dashboards and reports for compliance, performance monitoring, and trend analysis.

4.3.4 NGFW Platform

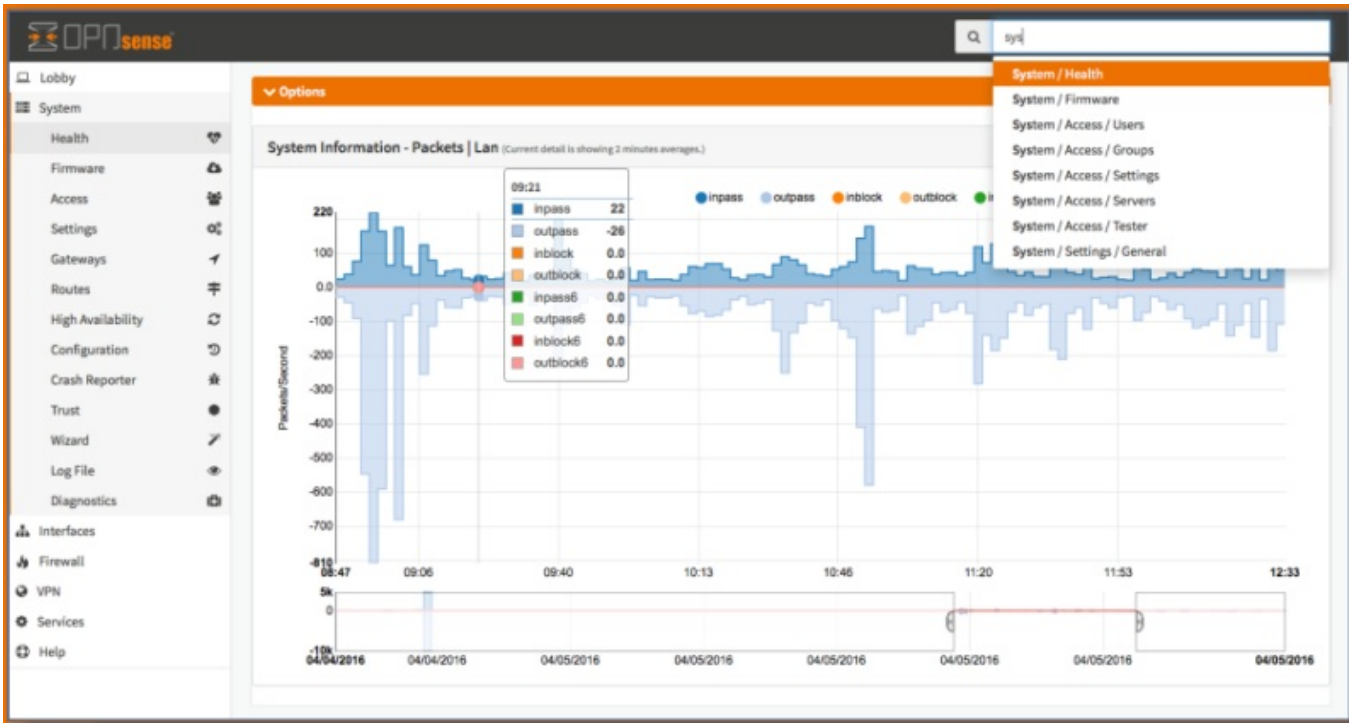


Figura 10 – NGFW platform Overview

4.3.4.1 Service Description

The Next-Generation Firewall (NGFW) service, based on OPNsense technology, implements a firewall application system to manage inbound and outbound traffic flows.
The platform includes all the advanced features of a firewall with additional threat detection capabilities based on artificial intelligence and machine learning.
The device is also capable of analyzing the content of network packets, down to the application layer (deep packet inspection), and managing rules based on more than just ports and protocols.
The service delivers intelligent traffic inspection, application-aware control, intrusion prevention, and threat detection across cloud, on-premise, and hybrid infrastructures. Unlike traditional firewalls that rely solely on port and protocol filtering, the NGFW PaaS incorporates deep packet inspection (DPI), machine learning-based threat analysis, and context-aware security policies to identify and mitigate sophisticated attacks, including malware, ransomware, zero-day exploits, and data exfiltration attempts.

The service is offered with the following unit metric: *1 Gbps of Throughput*.

4.3.4.2 Features and Advantages

The main features and functionalities of the service are:

- *Intrusion prevention system (IPS)* → provides signature-based and behavior-based detection to prevent known

and unknown exploits. Protects against buffer overflows, SQL injection, cross-site scripting, and command injection attacks. Continuously updated with global threat intelligence feeds.

- *Virtual Private Network (VPN) and secure remote access* → provides site-to-site and remote access VPN with AES-256 encryption. Supports IPsec, SSL, and hybrid VPN tunnels for secure communication. Integrates with multi-factor authentication (MFA) for secure user access.
- *Logging, monitoring, and analytics* → real-time visibility into network traffic, user activity, and threat events. Integrated dashboards and customizable reports for compliance and auditing. Supports integration with SIEM/SOAR platforms for advanced analytics and incident response.
- *High availability and scalability* → redundant architecture ensuring failover, session synchronization, and minimal downtime. Auto-scaling capabilities to handle fluctuating workloads and peak network demand. Supports multi-zone and multi-region deployment for resilience and disaster recovery.

The main components of the service are:

- *Web filtering and URL categorization / Web and email security* → filters web traffic by category, blocks o restringe accesso a siti malevoli o non autorizzati." — Corretto, almeno a livello di proxy/filtraggio tramite plugin (es. proxy HTTP/HTTPS, filtraggio URL/blacklist).
- *Firewall enforcement nodes / Stateful firewall, policy-based filtering, support VLAN, NAT, port forwarding, etc* .

The service offers the following advantages:

- *Enhanced cyber resilience* → provides continuous protection against advanced cyber threats, ensuring business continuity and minimizing the risk of network downtime, data loss, or reputational damage.
- *Regulatory compliance and risk reduction* → simplifies compliance with major cybersecurity frameworks by enforcing standardized policies, secure configurations, and comprehensive audit logging.
- *Operational efficiency and cost optimization* → delivered as a managed PaaS, the service eliminates the need for dedicated hardware, manual updates, and specialized maintenance, significantly reducing operational costs.
- *Scalable and flexible network protection* → cloud-native design enables dynamic scaling according to traffic demand, ensuring consistent performance across hybrid and multi-cloud environments.
- *Accelerated security modernization* → enables organizations to transition from legacy firewalls to a modern, intelligent, and centrally managed security platform without downtime or complex migrations.
- *Improved Visibility and Governance* → consolidates monitoring and policy control across distributed environments into a single interface, empowering governance, risk, and compliance teams.
- *Faster incident response* → automated detection and orchestration reduce the time to identify and mitigate attacks, minimizing business impact and resource overhead.
- *Business continuity and resilience* → redundant and geo-distributed infrastructure ensures uninterrupted protection and service availability even during outages or attacks. Support for digital transformation initiatives →

enables secure adoption of cloud services, remote access, and IoT solutions by integrating network security directly into cloud workflows.

- *Comprehensive layered protection* → combines firewall, intrusion prevention, antivirus, web filtering, and sandboxing into a unified, multi-layered security stack. Application and user awareness → identifies and controls applications and users regardless of port, protocol, or encryption, ensuring contextual, identity-based access control.
- *Deep Packet Inspection (DPI)* → examines every packet in real-time to detect encrypted or obfuscated threats, ensuring accurate threat identification and minimal false positives.
- *AI-Driven threat detection and prevention* → uses artificial intelligence, behavioral analytics, and threat intelligence feeds to detect zero-day attacks, ransomware, and polymorphic malware.
- *Centralized Policy Management* → provides unified control of security rules, compliance baselines, and configurations across all NGFW instances through a single management console.
- *Real-Time analytics and reporting* → offers comprehensive visibility into traffic patterns, security events, and policy compliance, with exportable reports for auditing and SOC integration.
- *High availability and elastic scalability* → implements active-active clustering, load balancing, and autoscaling to maintain performance and fault tolerance under varying network loads.
- *Zero Trust and microsegmentation support* → enforces least-privilege access and segmentation at the application, user, and workload level to contain breaches and minimize lateral movement.
- *Integration with security ecosystem* → seamlessly connects with SIEM, SOAR, CSPM, and IAM platforms for unified threat management, incident response, and automation workflows.
- *Secure VPN and remote access* → delivers site-to-site and user-based VPN capabilities with strong encryption and MFA integration for secure remote connectivity.
- *Automated policy enforcement and updates* → automatically distributes updated rules, signatures, and threat intelligence across all firewalls, ensuring continuous protection with minimal manual effort.
- *Robust logging, monitoring, and auditability* → maintains detailed, immutable logs for compliance, forensics, and real-time incident response, ensuring full visibility and traceability.
- *Support for multi-tenant and hybrid environments* → designed for organizations and service providers managing multiple clients or business units with logical separation and delegated administration.

4.3.5 PAM (Privileged Access Management) Service

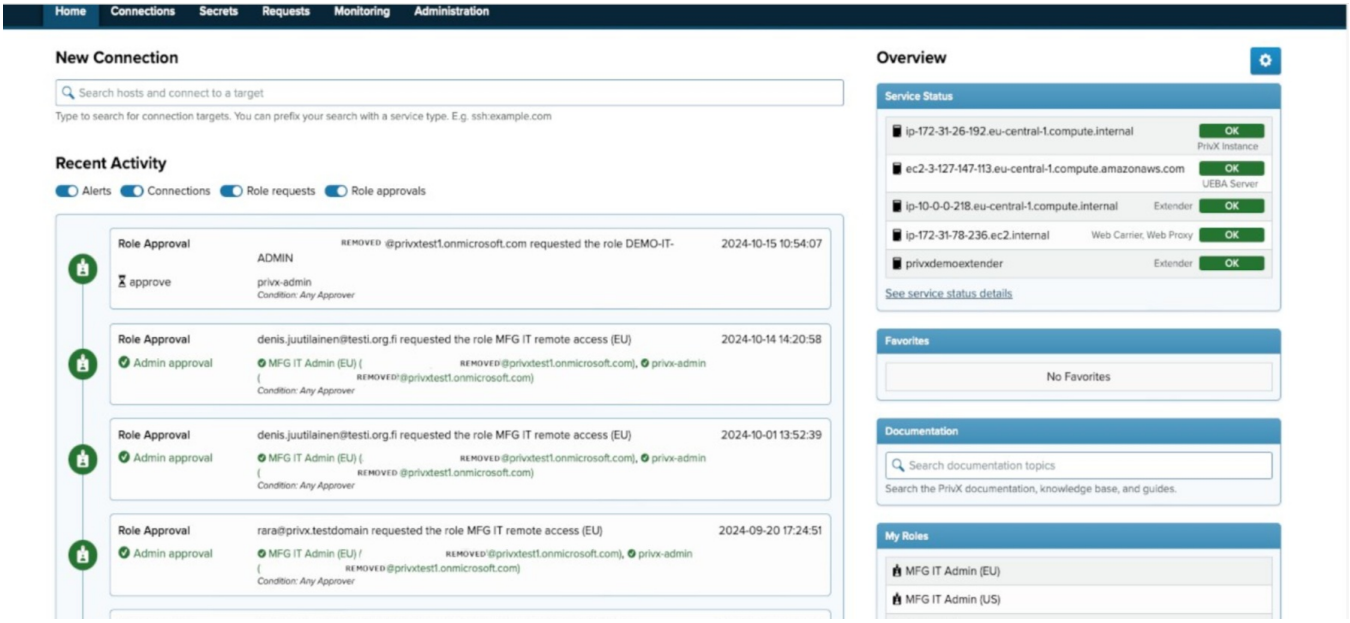


Figura 11 – PAM (Privileged Access Management) Service Overview

4.3.5.1 Service Description

Based on SSH solution, the Privileged Access Management (PAM) service manages and protects privileged access to critical environments, including credential management, session control, and real-time monitoring.
PAM allows organizations to activate a privileged access management system. Its purpose is to act as a bridge between users (especially administrators) and the systems they manage, ensuring that administrative credentials are protected within a "vault" and hidden from the administrators themselves.
Furthermore, the system can rotate administrative credentials or deny access to an administrator on a per-profile basis.
Privileged accounts — such as system administrators, database managers, and DevOps automation services — represent a primary attack vector for cybercriminals. Compromise of these accounts can lead to severe data breaches, ransomware propagation, or full system takeover.
The PAM PaaS delivers identity-centric protection and governance for all privileged credentials, sessions, and activities across on-premises, cloud, and hybrid environments. It enforces the principle of least privilege, enables session monitoring and recording, and automates credential rotation, vaulting, and just-in-time access provisioning to minimize risk exposure.
Delivered as a managed PaaS, the service eliminates the complexity of deploying and maintaining traditional PAM infrastructure, providing organizations with continuous protection, compliance enforcement, and operational efficiency.

The service is offered with the following unit metric: *10 administrative users*.

4.3.5.2 Features and Advantages

The PAM PaaS provides a rich set of functionalities to secure and manage privileged accounts, credentials, and access sessions throughout their lifecycle.

- *Centralized credential vaulting* → securely stores and manages privileged credentials (passwords, SSH keys, API tokens, certificates) in an encrypted vault. Eliminates hard-coded or shared credentials across systems. Provides strong encryption, multi-factor authentication, and access auditing.
- *Automated password and key rotation* → enforces automatic, policy-driven rotation of privileged passwords and cryptographic keys.Integrates with directories, databases, network devices, and cloud services. Reduces exposure time in case of credential compromise.
- *Just-in-Time (JIT) privilege elevation* → grants temporary, time-bound privileged access based on contextual approval workflows. Automatically revokes privileges after task completion. Minimizes standing privileges and insider threat exposure.
- *Session management and monitoring* → records, monitors, and audits all privileged sessions (SSH, RDP, SQL, web consoles). Enables real-time session oversight and automated termination on policy violation. Provides full playback for forensic investigation and compliance.
- *Multi-Factor Authentication (MFA) and adaptive access* → enforces MFA for all privileged access events. Supports adaptive authentication based on device, geolocation, and behavioral risk scoring. Integrates with corporate identity providers (Azure AD, LDAP, SAML, OIDC).
- *Role-Based Access Control (RBAC)* → assigns privileges based on predefined roles, ensuring least-privilege enforcement. Supports fine-grained policies that define who can access what, when, and how. Facilitates separation of duties for compliance with ISO 27001 and NIS2.
- *Command filtering and policy enforcement* → inspects and filters privileged commands during active sessions.Blocks or flags suspicious commands or administrative actions in real time. Supports custom rule sets aligned with compliance and internal security standards.
- *Secure remote access gateway* → provides agentless, browser-based remote access to critical systems without exposing credentials. Supports RDP, SSH, and web management interfaces through encrypted tunnels. Logs all session activity for security and compliance.
- *Integration with SIEM and SOAR platforms* → sends logs, events, and alerts to centralized SIEM/SOAR solutions. Enables automated incident response, anomaly detection, and correlation with threat data. Provides standardized APIs and connectors for integration.
- *Privileged Account Discovery* → scans the environment to identify unmanaged privileged accounts, keys, and secrets. Assesses risk exposure and automates onboarding into the vault. Supports discovery across Active Directory, cloud platforms, databases, and containers.
- *Audit, compliance, and reporting* → provides detailed reports on access requests, approvals, and session activity.

Supports compliance with GDPR, ISO 27001, PCI-DSS, HIPAA, and NIS2 directives. Offers customizable dashboards and automated report scheduling.

- *Threat analytics and anomaly detection* → leverages behavioral analytics to identify suspicious privileged user behavior. Detects deviations from normal activity patterns using AI and machine learning models. Generates alerts and can automatically revoke access on detected anomalies.
- *API and DevOps integration* → provides RESTful APIs and SDKs for integrating PAM controls into CI/CD pipelines. Protects privileged secrets in DevOps environments (Jenkins, GitLab, Ansible). Enables machine identity management and service account governance.

The main components of the service are:

- *Credential vault (Secure storage layer)* → core repository for all privileged credentials, keys, and secrets. Implements AES-256 encryption, HSM integration, and strong key management. Enforces access via secure APIs and MFA-protected sessions.
- *Access control and policy engine* → centralized component that enforces RBAC, access approval workflows, and least-privilege rules. Evaluates contextual access conditions (user role, time, device, risk score). Integrates with IAM and directory services for authentication and authorization.
- *Session management and recording subsystem* → manages all privileged session connections, including RDP, SSH, and database access. Captures full video/audio/text logs of user sessions for replay and forensic analysis. Supports live session termination, keystroke logging, and behavioral analytics.
- *Just-in-Time (JIT) access provisioning engine* → automates temporary privilege elevation for approved tasks. Integrates with ITSM systems for request/approval workflows. Ensures access expiration and automatic credential revocation.
- *Discovery and onboarding module* → continuously scans infrastructure to locate unmanaged privileged accounts and secrets. Automatically imports discovered credentials into the vault. Generates visibility reports and risk scores for unprotected assets.
- Multi-Factor Authentication and identity federation layer → connects with enterprise IAM systems for identity verification. Supports SSO, SAML 2.0, OIDC, and FIDO2 standards.Applies adaptive MFA policies based on context and risk posture.
- *Analytics and threat detection engine* → aggregates PAM telemetry to detect abnormal privileged activity. Uses AI-based behavioral baselines for early threat detection. Feeds alerts and analytics to SIEM/SOAR systems for incident correlation.
- *Secure remote access gateway* → provides proxy-based, credential-free access to internal systems. Prevents credential exposure during remote administration. Logs all actions for compliance and traceability.
- *Integration and API gateway* → exposes APIs for integration with ITSM, SIEM, SOAR, DevOps, and IAM tools. Supports automation and policy synchronization across multi-cloud environments. Enables secure machine-to-

machine communications.

- *Logging and audit repository* → centralized collection point for all PAM events, access logs, and session data. Ensures immutability and time synchronization for forensic integrity. Supports long-term storage and secure archiving.
- Web management console → provides administrators with a unified interface for configuration, policy management, and monitoring. Offers dashboards, risk indicators, and compliance views. Supports delegated administration and role-based visibility.
- *High availability and scalability layer* → multi-zone deployment with redundant components to ensure continuous availability. Supports horizontal scaling for concurrent session and credential workloads. Implements backup, failover, and disaster recovery capabilities.

The service offers the following advantages:

- *Reduced risk of data dreaches and insider threats* → minimizes the attack surface by enforcing strict control and monitoring of privileged accounts, effectively reducing both external and insider threat vectors.
- *Regulatory and compliance alignment* → simplifies adherence to key cybersecurity and privacy frameworks through standardized access policies, complete audit trails, and automated compliance reporting.
- *Improved security governance and accountability* → centralizes management of all privileged identities and enforces policy consistency across business units, increasing accountability and transparency.
- *Operational efficiency and cost savings* → delivered as a managed PaaS, it eliminates the need for on-premises infrastructure, manual credential management, and complex maintenance tasks, reducing operational overhead and total cost of ownership.
- *Enhanced Business Continuity* → ensures uninterrupted access to critical systems while maintaining full security control, even during infrastructure failures or security incidents.
- *Support for digital transformation and cloud adoption* → enables secure access to hybrid and multi-cloud environments, supporting DevOps pipelines, cloud-native workloads, and remote operations securely and efficiently.
- *Increased organizational agility* → automated workflows and just-in-time access provisioning streamline operational processes and accelerate response to evolving business and security needs.
- *Improved trust and peputation* → demonstrates strong security posture to clients, partners, and regulators by safeguarding the most sensitive access credentials and administrative activities.
- *Comprehensive privileged access lifecycle management* → covers the full lifecycle of privileged credentials — discovery, vaulting, rotation, monitoring, and decommissioning — ensuring continuous protection.
- *Centralized and secure credential vaulting* → uses enterprise-grade encryption and hardware security modules (HSMs) to protect privileged credentials and secrets from unauthorized disclosure.
- *Automated password and key rotation* → reduces credential exposure by automatically rotating and updating

passwords, API keys, and certificates according to customizable security policies.

- *Just-in-Time (JIT) access control* → eliminates permanent administrative privileges by providing temporary, task-based elevated access, automatically revoked upon completion. Real-time session monitoring and recording → enables full visibility into privileged user actions, with live session control, playback, and forensic evidence for investigations.
- *Command filtering and policy enforcement* → prevents misuse of administrative access by blocking unauthorized commands and enforcing predefined policy rules during active sessions.
- *Integration with Enterprise identity and security systems* → seamlessly connects to IAM, SSO, SIEM, SOAR, and DevOps tools to ensure consistent access control and unified threat visibility.
- *Behavioral analytics and anomaly detection* → uses machine learning models to detect suspicious or abnormal privileged activity, triggering automated alerts and responses. *Strong Authentication and Adaptive Security* → implements MFA, context-based access control, and adaptive authentication to strengthen access security across all privileged sessions.
- *Secure remote access gateway* → provides agentless, credential-free remote access to internal systems through encrypted channels, reducing the risk of credential theft.
- *Scalable cloud-native architecture* → designed for elastic scaling to accommodate growth in users, systems, and sessions, ensuring consistent performance across large deployments.
- *Continuous compliance and reporting* → generates automated reports and dashboards that meet audit and compliance requirements, ensuring continuous adherence to security policies.
- *Multi-tenant and delegated administration support* → enables secure separation of administrative domains for different departments or customers, ideal for managed service providers or large organizations.
- *Resilient and redundant infrastructure* → built on a high-availability architecture with geographic redundancy, automatic failover, and disaster recovery capabilities. Extensive API and Automation Capabilities → exposes APIs for integration with orchestration and ITSM systems, enabling policy automation, credential management, and incident response workflows.

4.3.6 Intrusion Prevention System (IPS) Service

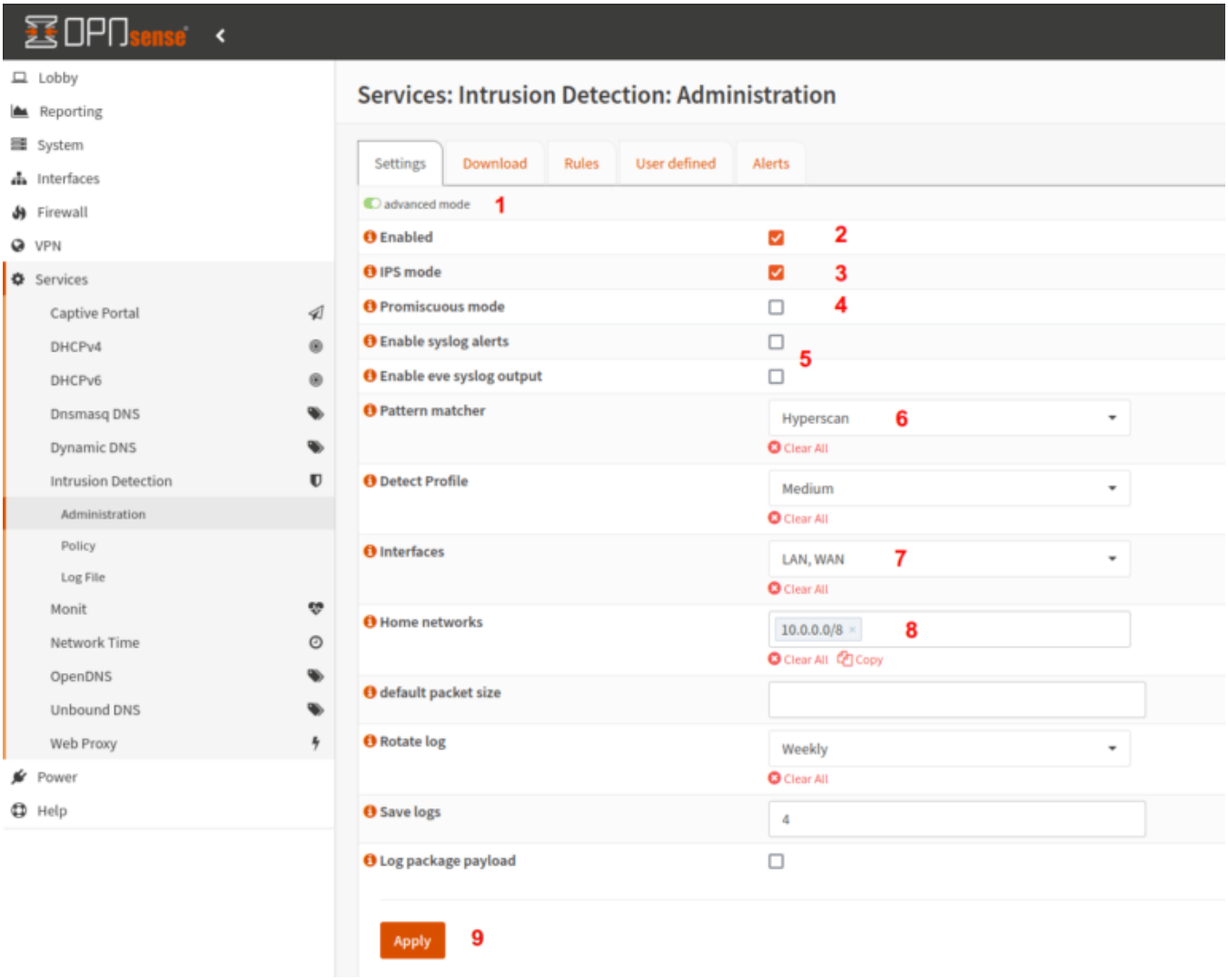


Figura 12 – Intrusion Prevention System (IPS) Service Overview

4.3.6.1 Service Description

Based on OPNsense, the Intrusion Prevention System (IPS) service actively intercepts network traffic for patterns of malicious or abnormal behavior and automatically and proactively blocks such malicious traffic.
The Intrusion Prevention System (IPS) service not only detects but also prevents attacks in real time.
It uses attack signatures and behavioral analysis to identify and block known and unknown threats, protecting the IT infrastructure from potential compromise. Unlike an IDS, an IPS is integrated into the network architecture, at least for mission-critical network flows.

The service is offered with the following unit metric: *1 Gbps of Throughput*.

4.3.6.2 Features and Advantages

The main features and functionalities of the service are:

- *Traffic inspection and analysis* → performs deep packet inspection (dpi) and protocol decoding for inbound, outbound, and east-west traffic. Applies signature-based rules (known attack patterns), anomaly/behavior analysis (baseline deviation), and policy enforcement. Supports real-time blocking of malicious connections and content.
- *Signature and threat intelligence engine* → maintains an updated signature library for known exploits and malicious traffic patterns. Integrates external threat intelligence feeds to identify malicious ips, domains, C2 channels, and exploit kits.
- *Policy-driven prevention and inline blocking* → automates blocking, connection termination, or traffic modification (e.g., reset, drop) when threats are detected. Policy profiles are configurable by severity, traffic zone, protocol, application, and asset criticality.ts.
- *Zone and network segment enforcement* → inspects traffic crossing defined security zones (e.g., lan → dmz, cloud → on-prem) and enforces segmentation rules.
- *Logging, alerting, and reporting* → generates detailed logs of detected intrusions, blocked events, and session information. Provides dashboards and reports for monitoring detection/prevention performance, compliance, and trends.
- *Continuous update and threat intelligence sync* → automatically delivers new signatures, behavioral models, and threat intelligence to all enforcement nodes to keep protection current.

The main components of the service are:

- *Enforcement / data plane nodes* → high-performance inline sensors (virtual or hardware) that inspect and enforce traffic rules, perform dpi, session tracking, and blocking. Deployed across zones (edge, cloud gateway, internal segment).
- *Signature and threat intelligence repository* → stores rule sets, malware and attack signatures, reputation data, ip/domain blacklists, and threat feed aggregations.Regularly updated and distributed to enforcement nodes.
- *Policy engine and configuration repository* → manages configuration of inspection zones, severity thresholds, blocking actions, traffic handling rules, and enforcement workflows.Maintains versioning, audit history, and rollback capabilities.
- *Integration and api gateway* → exposes restful apis and webhooks for integration with siem, soar, orchestration, and other security tools. Supports event export, automation triggers, and third-party tool connectivity.
- *Logging, monitoring, and reporting subsyste*m → collects logs, alerts, session metadata, and traffic flows, storing them in a secure, indexed repository. Provides dashboards, forensic search, export capabilities, and report generation.

The service offers the following advantages:

- *Proactive protection against cyber threats* → prevents network intrusions and exploits in real time, reducing the risk of data breaches and business disruption.Continuously analyzes traffic to identify and stop attacks before they escalate.
- *Reduced operational costs* → eliminates the need for dedicated on-premises intrusion prevention appliances and complex management.Delivered as a cloud-based paas with predictable subscription costs and minimal maintenance overhead.
- *Enhanced business continuity* → blocks disruptive and malicious traffic automatically, ensuring uninterrupted operations.Minimizes downtime and revenue loss caused by security incidents.
- *Improved regulatory and compliance posture* → supports adherence to security standard frameworks Provides continuous monitoring, detailed logs, and auditable reports for compliance verification.
- *Centralized visibility and governance* → provides unified control and visibility over network traffic across cloud, hybrid, and on-premises environments. Simplifies governance and policy enforcement from a single management interface.
- *Scalability and flexibility* → dynamically scales according to traffic load and business needs, adapting to cloud and hybrid deployments.Supports integration with existing soc and siem platforms for extended visibility.
- *Reduced risk exposure and faster incident response* → accelerates threat response through automated blocking and integration with orchestration tools. Shortens mean time to detect (mttd) and mean time to respond (mttr).
- *Improved security posture through continuous updates* → continuously updated with new signatures, threat intelligence, and behavioral models. Ensures up-to-date protection against emerging and zero-day attacks.
- *Advanced detection and prevention capabilities* → combines signature-based, heuristic, and anomaly-based detection techniques for comprehensive threat coverage. Uses deep packet inspection (dpi) for high-precision traffic analysis.
- *Real-time inline prevention* → automatically blocks malicious traffic inline without human intervention. Prevents exploits, denial-of-service attempts, and command-and-control communications in real time.
- *Machine learning and behavioral analytics* → employs machine learning models to identify unknown and evolving threats. Continuously refines detection accuracy through feedback and adaptive learning.
- *Seamless integration with existing infrastructure* → integrates easily with SIEM, SOAR, and SOC systems for centralized monitoring and automated response.Supports api-based integration for custom workflows and automation.
- *High availability and redundancy* → designed for continuous uptime through clustering, failover, and auto-scaling mechanisms. Ensures uninterrupted protection even during maintenance or component failure.
- *Centralized management and policy control* → allows administrators to define, deploy, and manage security policies across distributed environments from a single console. Enables consistent enforcement across multi-cloud and hybrid architectures.

- *Encrypted traffic inspection* → supports ssl/tls decryption and inspection for comprehensive visibility into encrypted traffic streams. Ensures full coverage against hidden or encrypted attacks.
- *Automation and orchestration capabilities* → supports automated remediation workflows for threat containment and isolation. Reduces human workload and response time through integration with orchestration tools.

4.3.7 PaaS Web Application Firewall (WAF)

4.3.7.1 Service Description

The WAF is a fully managed web application firewall service designed to safeguard applications hosted within your environment on the cloud. It provides a protective layer between your public-facing services and the internet, ensuring that malicious traffic is intercepted before it can exploit vulnerabilities. The service is delivered as a turnkey solution, meaning that all necessary components, licenses, and updates are handled by the provider, allowing administrators to focus on their applications rather than the underlying security infrastructure.
The WAF inspects HTTP and HTTPS traffic directed at web applications. It evaluates requests against defined rules to determine whether they are legitimate or potentially harmful. Administrators can adopt either a negative security model, which blocks traffic matching known exploit signatures, or a positive security model, which denies all traffic by default and only allows explicitly permitted requests.
The firewall integrates protection against the most critical threats identified by the OWASP Top 10, including injection attacks, cross-site scripting, and insecure deserialization.

4.3.7.2 Features and Advantages

The WAF leverages OPNsense’s NGINX plugin with NAXSI (Negative Application Security for nginx) to deliver its capabilities.NAXSI is a rule-based engine specifically designed to detect and block malicious web requests.

Rule Types

- Main Rules: These are globally valid and designed to block common attack vectors such as SQL injection, XPath injection, or cross-site scripting attempts.
- Basic Rules: These are used to fine-tune configurations, typically by whitelisting certain requests or creating additional rules for specific application contexts.
- Custom Rule Sets: Administrators can define custom rules to tailor protection to their applications. For example, they may whitelist certain parameters for trusted applications while maintaining strict controls elsewhere.

Logging and Monitoring

Logs are generated in near real time, providing visibility into blocked and allowed requests, and can be dispatched to the centralized log analytics service to analyze traffic patterns and identify potential threats.

OWASP Guidance

Configuration can be guided by OWASP cheat sheets, which provide best practices for securing web applications.

Provisioning the Service

The WAF is provisioned through the Secure Cloud Management Platform, the central portal for managing cloud services. Administrators can deploy the firewall by selecting the WAF option within the platform. Provisioning can also be performed via APIs, enabling integration into automated workflows.
Once deployed, the firewall is automatically patched and maintained by Leonardo, ensuring that the system remains up to date with the latest security fixes.

Configuration and Management

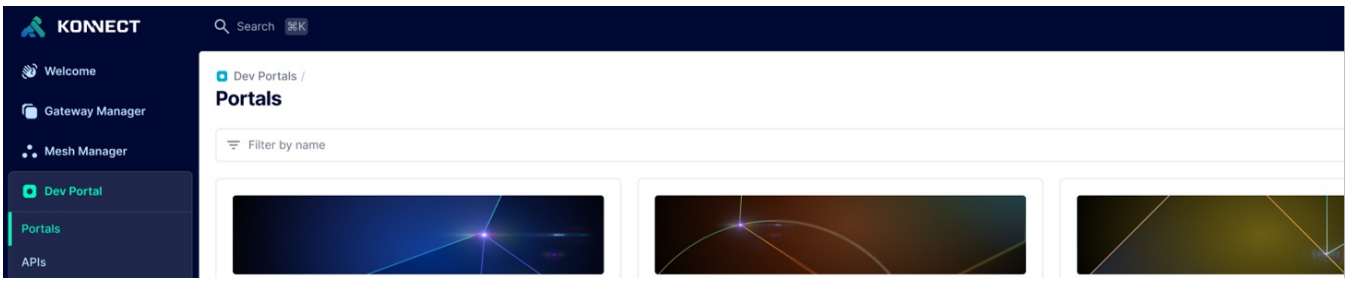
Configuration is performed through the Secure Cloud Management Platform. Administrators can:
- Define rule sets for both negative and positive security models.
- Apply NAXSI main and basic rules to protect against common exploits.
- Customize rules to allow specific traffic patterns while blocking suspicious requests.
- Monitor logs to gain insight into traffic directed at their applications.

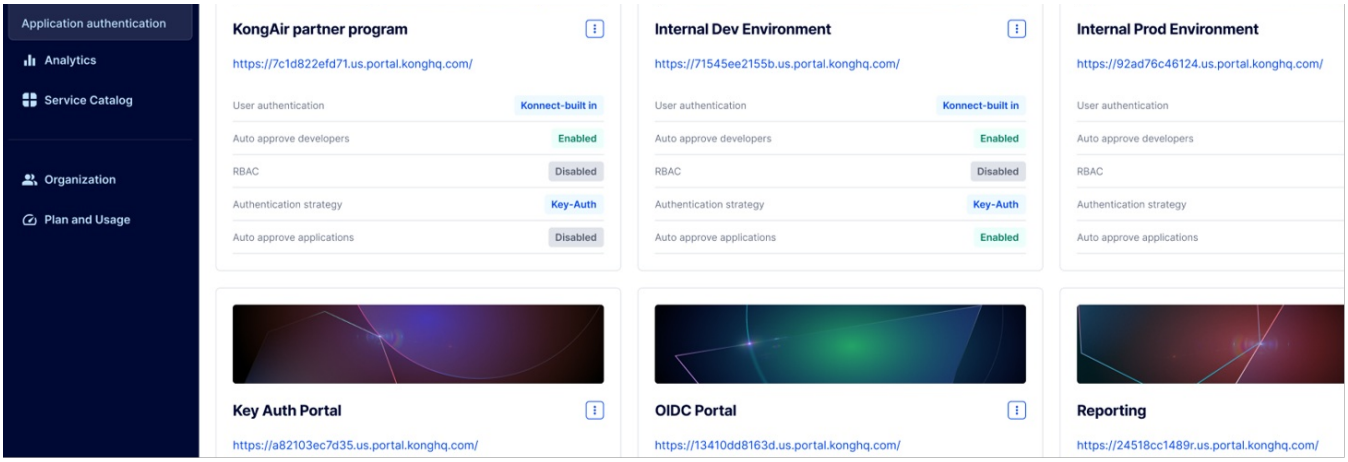
4.4 Middleware Family

Below is the list of services belonging to the Middleware family:

- PaaS API Management
- Functions as a Service (FAAS)
- Jboss as a Service
- Spring boot as a Service
- PaaS Business Process as a Service
- PaaS CMS as a Service
- Semantic Knowledge Search

4.4.1 PaaS API Management





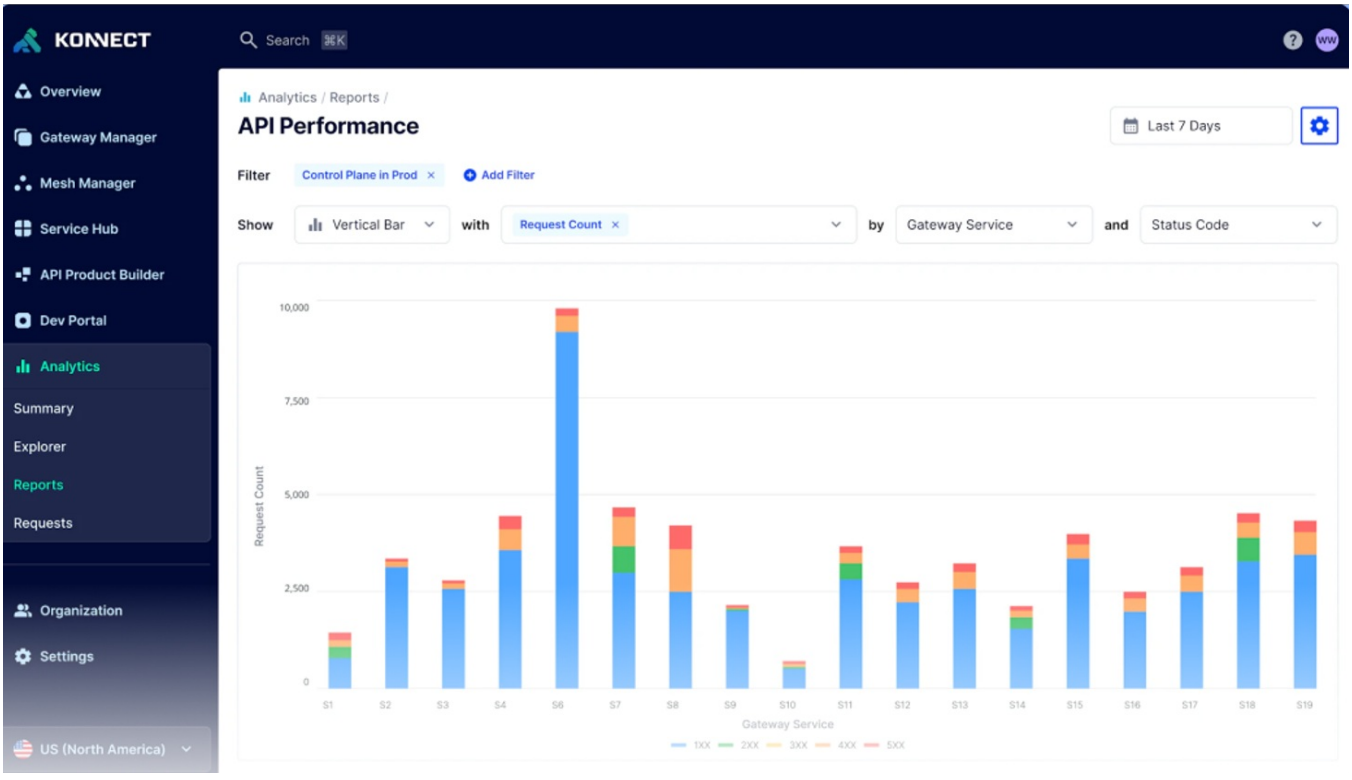


Figura 13 – PaaS API Management

4.4.1.1 Service Description

Based on Kong solution, it is a platform of tools and services that facilitates the management, control, monitoring, and protection of APIs (Application Programming Interfaces) without having to manually implement all the components. The service typically offers:

- API gateways to route and secure traffic;
- Authentication and authorization: Rate limiting and throttling to control consumption;
- Logging and observability: Integration with security and DevOps systems.

The API manager facilitates API lifecycle management, including aspects such as creation, version management, deprecation, and retirement, to ensure backward compatibility, allowing developers to gradually migrate to new versions without disrupting existing applications.
The API manager allows you to define and enforce policies, such as usage limits, quota management, custom authentication, data transformations, and caching. These policies allow you to control API behavior and ensure compliance with security requirements and guidelines.
The API Manager can integrate with other systems and tools, such as identity and access management (IAM) systems, performance monitoring systems, data analytics systems, and security gateways. This integration expands the API Manager's functionality and integrates it into the ecosystem of existing applications and services.

The service is offered for a *unit size of 500 M of API requests* .

4.4.1.2 Features and Advantages

The main features and functionalities of the service are:

- *API Publishing* → the API Manager offers tools for publishing APIs, allowing developers or authorized users to access them. For optimal use, clear and comprehensive documentation is provided describing how to use the APIs, which endpoints are available, which parameters are requested, and how to interpret the responses.
- *Access Control* → the API Manager manages the authentication and authorization of users who wish to use the APIs. This allows you to control who can access the APIs and with what permission levels. The API Manager can adopt authentication mechanisms such as access tokens, API keys, or digital certificates to ensure API security.
- *Monitoring and Analytics* → the API Manager offers tools for monitoring API performance, such as the number of requests, response times, and errors. This information allows developers and administrators to monitor API usage, identify any performance issues, and take corrective action.

The architecture, based on Kong technology, is divided into several key components that interact to provide comprehensive functionality to users:

- *Front-end* → administration clients and graphical interfaces (Admin GUI, Dev Portal) accessible via browser or dedicated applications, which allow users to configure services, manage users, and monitor metrics in real time.
- *Back-end Kong Control Plane* → manages configurations, policies, plugins, and API orchestration.

- *Back-end Data Plane* → routes user requests to back-end services, applying security rules, transformations, caching, and rate limiting. - *Database* → stores configurations, users, roles, statistics, and logs. Supports replication and high availability capabilities to ensure resilience and business continuity
- *Integrations* → supports integrations with development tools, CI/CD, monitoring systems, and project management platforms, allowing Kong to be incorporated into existing enterprise workflows.
- *Security and Authentication* → offers advanced security options, including multi-factor authentication, support for enterprise protocols (OIDC, SAML, LDAP), and granular access control, ensuring data protection and compliance with corporate standards.

The service offers the following advantages:

- *Reduced time to market* → APIs can be published and managed quickly without building the infrastructure from scratch.
- *Flexibility and scalability* → the platform grows with business needs, supporting traffic spikes or new integrations without disruption.
- Reduced operating costs → no hardware or maintenance investments: infrastructure management is delegated to the PaaS provider.
- *API monetization* → ability to create API-driven business models (e.g., exposing APIs to partners or customers with pricing plans).
- *Enhanced security and compliance* → secure management of APIs and traffic between services, with authentication, authorization, and rate limiting policies, protecting the infrastructure from unauthorized access.
- *Open ecosystem* → Facilitates partnerships and innovation thanks to an API-ready and standardized infrastructure.

4.4.2 Functions as a Service (FAAS)

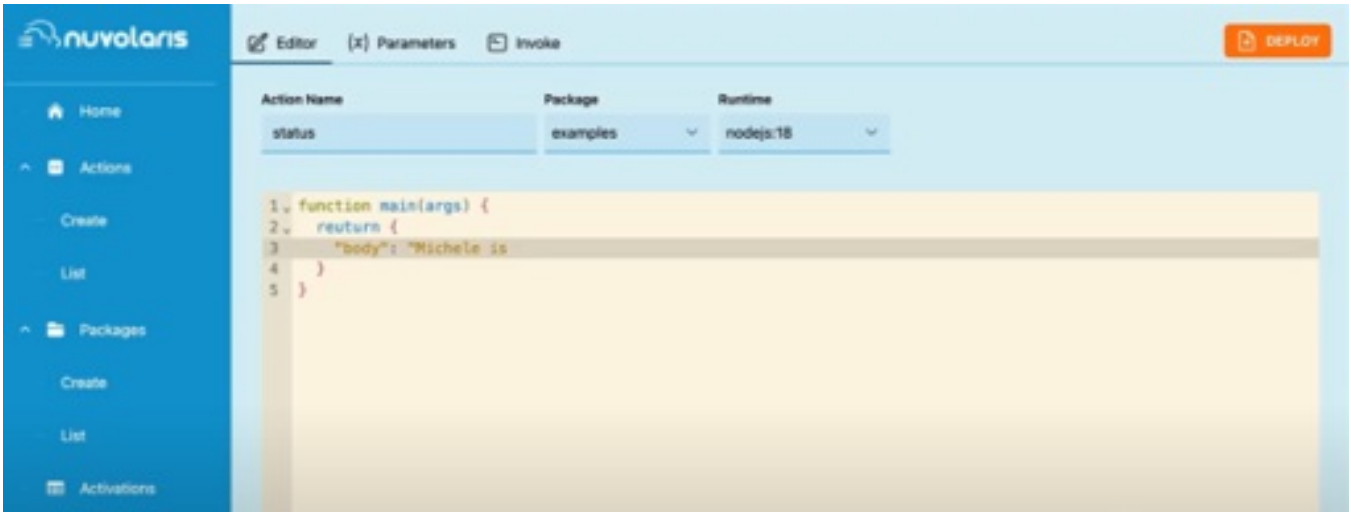


Figura 14 – Functions As a Service (FAAS) Interface

4.4.2.1 Service Description

FaaS (Function as a Service) is an event-driven system design model running on stateless containers, where developers create, deploy, and execute small, independent functions to perform specific tasks without worrying about the underlying infrastructure.
Adopting FaaS allows for standardization of application development and execution by centralizing cross-functional capabilities such as orchestration, automatic provisioning, monitoring, integrated service management, and event-driven flow control.

It offers tools to:

- centrally manage serverless functions;
- automate component lifecycle management.

The FaaS platform provisions and scales the underlying resources based on demand. It is ideal for highly dynamic scenarios with variable workloads and integrates seamlessly with microservices and event-based architectures.

The service is offered with the following metrics: *100 VCPUs*.

4.4.2.2 Features and Advantages

The service goes beyond simply providing an execution engine; it also offers a complete ecosystem, consisting of:

- Serverless execution → stateless functions and event-driven workflows, scalable and available in various programming languages.
- Portability and independence → can run on any Kubernetes cluster, across multiple environments, without lock-in

constraints.

- Security and compliance → data protection and centralized access management.
- The solution enables organizations to adopt a modern and flexible model, reducing operational complexity and benefiting from a standardized and easily accessible service.

The service is delivered through Apache OpenServerless, an open-source, cloud-agnostic serverless platform based on Apache OpenWhisk as a Function-as-a-Service (FaaS) engine.

The service offers the following advantages:

- *Reduced operating costs* → you only pay for the actual use of features.
- *Flexibility and scalability* → resources adapt to demand.
- *Operational efficiency* → eliminating the need to directly manage servers, patches, and updates.
- *High availability* → built-in redundancy and fault tolerance, ensuring high availability of features even in the event of hardware failures or other interruptions.
- *Accelerated time-to-market* → rapid release of new features without worrying about the infrastructure.
- *Agile development* → focus on code and business logic, not server management.
- *Continuous innovation* → rapid experimentation with new, low-cost services. Competitive advantage in cost and speed compared to traditional hosting models.

4.4.3 Jboss as a Service

4.4.3.1 Service Description

The service is based on an open source platform for running and managing Enterprise Java applications, designed to offer reliability, scalability, and flexibility in modern environments. It allows to run Java EE/Jakarta EE applications and microservices, providing a robust environment for business logic, data persistence, and transaction management.
It allows to manage the application lifecycle, including deployment, updates, rollbacks, and centralized configuration, ensuring secure and repeatable processes.
Thanks to its modular architecture, compatibility with cloud environments, and rich integration with automation and security tools, it represents a strategic solution for companies seeking efficiency, innovation, and operational control.

The service is sized per container. Each one consists of:

- 4 VCPUs
- 8 GB of RAM

4.4.3.2 Features and Advantages

JBoss offers a robust, high-performance, and secure environment for developing and managing enterprise applications, providing a stable foundation for the growth and evolution of enterprise systems.
The main features and functionalities of the service are:

- *Security and Compliance* → manages security, authentication, authorization, and data protection.
- *Web Services* → JAX-RS, JAX-WS, creation and management of RESTful and SOAP APIs for service integration.
- *Microservices Management* → MicroProfile, a set of specifications optimized for developing microservices-based applications. Includes features such as configuration, resiliency, monitoring, and metrics.

The architectural components of the service are as follows:

- *Front-end* → administration interfaces (Web Console, CLI) accessible via browser or terminal, which allow administrators to manage configurations, deployment, resources, and monitoring.
- *ack-end* → the server core manages application execution, request processing, resource management (datasources, JMS queues, batch, etc.), and integration with external systems via resource adapters and connectors.
- *Database* → integrates with relational and NoSQL databases via configurable datasources, used by applications for data persistence.
- *Security and Authentication* → offers an advanced security subsystem for authentication, authorization, encryption, and auditing. It supports authentication via LDAP, Kerberos, SSO, and integration with external identity providers, ensuring secure access that complies with corporate standards.

The service offers the following advantages:

- *Reduced time to market* → application lifecycle automation, centralized management, and easy integration with DevOps pipelines reduce development and release times, accelerating response to market needs.
- *Reduced operating costs* → centralized resource management and the platform's modularity optimize the use of existing infrastructure, reducing waste and operating costs.

4.4.4 Spring boot as a Service

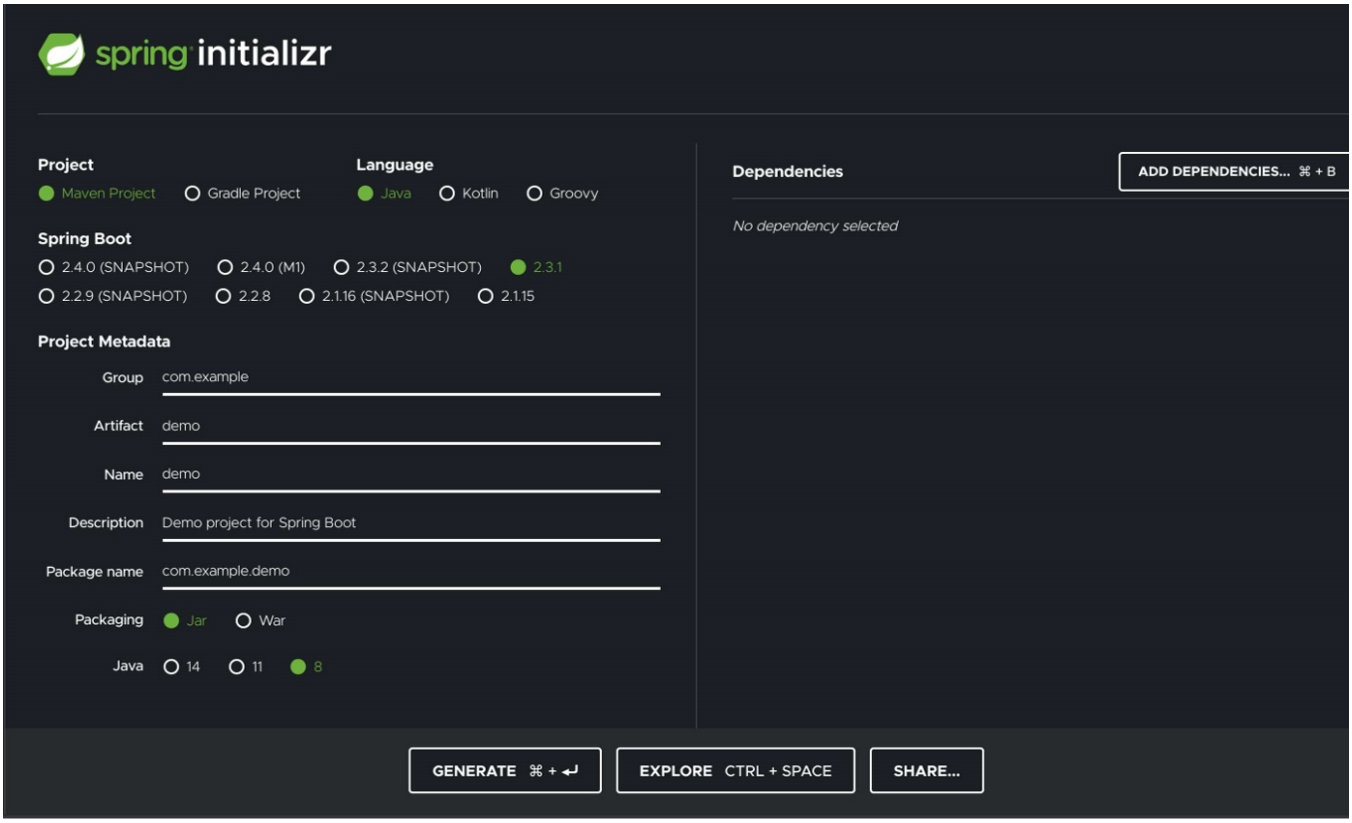


Figura 15 – Spring boot as a Service

4.4.4.1 Service Description

This service allows you to use Spring Boot, an open-source framework for Java application development, as a managed service.
It is designed to simplify the development of production-ready Java applications by providing a platform that eliminates much of the manual configuration required by the traditional Spring framework and reduces the need for server provisioning and dependency management.
With a preconfigured environment optimized for the Spring Boot framework, the service allows teams to focus on developing business features, reducing release times and costs.

The service is sized for single containers. Each container has 16 GB of RAM.

4.4.4.2 Features and Advantages

The main features and functionalities of the service are:

- *Automatic environment provisioning* → automatic configuration of Java runtime (JDK), integrated application server, and Spring Boot framework. No need to manually configure build environments or containers. Simplified

deployment → ability to directly upload a JAR or source code (e.g., via Git, API, or CI/CD pipeline).

- *Scalability* → horizontal (replication) and vertical (CPU/RAM resources) scaling managed by the PaaS based on load.
- *Integrated monitoring and logging* → access to runtime metrics (CPU, memory, latency, throughput); centralized logs (stdout/stderr) accessible via console or API; integration with BI tools (Prometheus, Grafana, etc.).
- *Configuration and secret management* → centralized configuration (environment variables, Spring Cloud Config, or Vault); secure management of credentials, tokens, and keys. Integrated support services → easy connection to managed databases (PostgreSQL, MySQL, MongoDB); support for messaging (RabbitMQ, Kafka), caching (Redis), and storage; automatic service binding via environment variables or injection.
- *Security and isolation* → each application is isolated (namespace, container, or dedicated VM); HTTPS/TLS by default, identity management, and integration with authentication systems (OAuth2, SSO).

The solution is based on the following architectural layers:

- *Infrastructure layer* → provides the hardware and virtual resources needed to run application containers (Compute nodes, Storage, Networking, Security layer); automatic provisioning via IaC (Infrastructure as Code).
- *Orchestration layer* (Platform Runtime) → manages the lifecycle of Spring Boot containers, from deployment to monitoring, ensuring availability, replication, and load balancing
- *Application layer* (Spring Boot Runtime) → Spring Boot runs within a container; supports Actuator endpoints for health checks and metrics; exposes HTTP/REST APIs on predefined and configurable ports
- *Management layer and PaaS services* → web dashboard or CLI to manage applications, versions, and resources. REST API for automation (deployment, scale, logs, metrics). Integration with external logging and monitoring systems.

The service offers the following advantages:

- *Reduced time to market* → Deployment automation and simplified environment management allow applications to be brought into production more quickly.
- *Reduced operating costs* → No hardware or maintenance investments: infrastructure management is handled for the customer.
- *Observability and monitoring* → Preconfigured tools to track performance, errors, and response times.
- *Guaranteed security* → Automatic patch and update management.
- *Environment consistency* → Same environments for development, testing, and production.
- *Microservices support* → Simplified management of distributed architectures.

4.4.5 Business Process as a Service

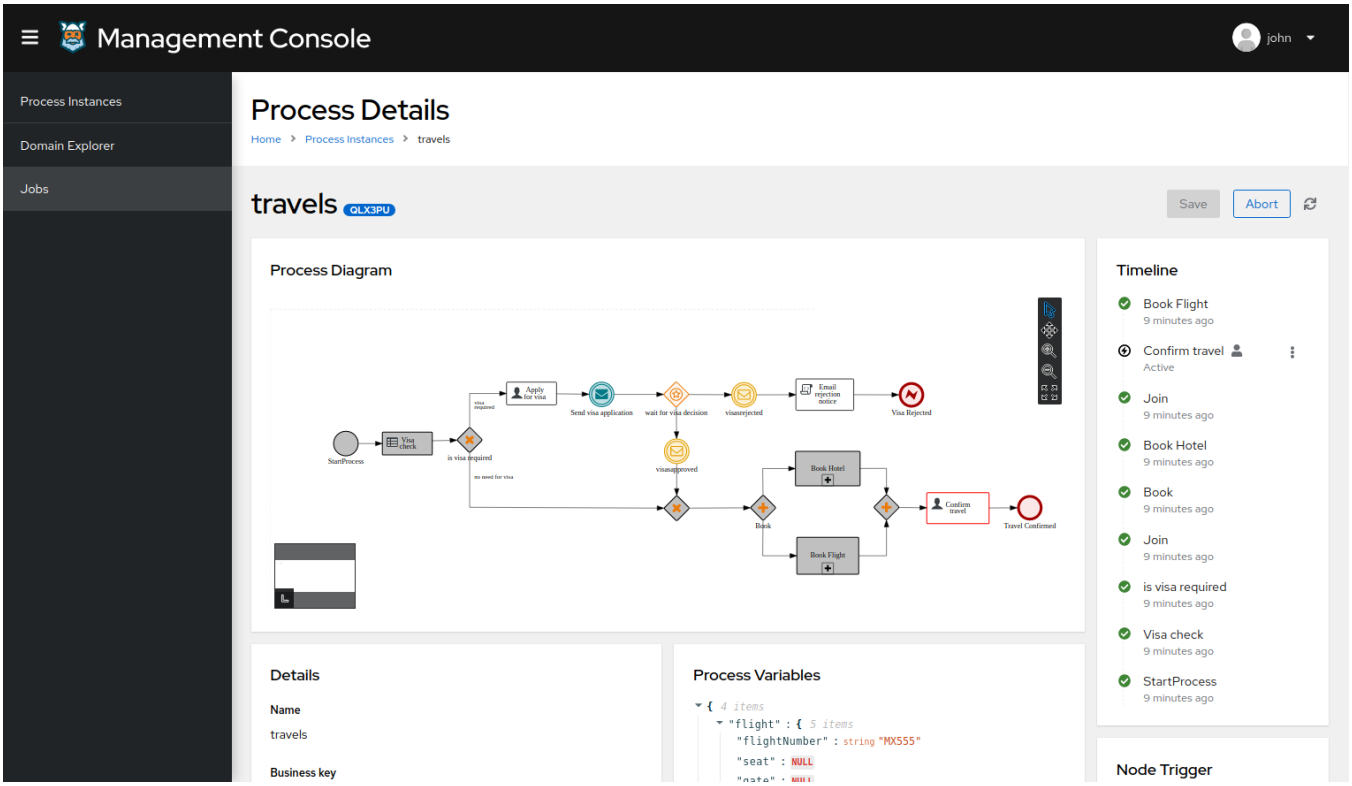


Figura 16 – Business Process as a Service

4.4.5.1 Service Description

Based on Kogito solution, it is a comprehensive Business Process Management (BPM) platform that helps companies model and automate complex processes, improve productivity and service quality, and ensure control, traceability, and flexibility in an integrated and scalable environment.
It combines workflow automation, application integration, and performance monitoring in a single solution. The goal is to improve operational efficiency, reduce execution times, and ensure process consistency across the organization.
It facilitates collaboration between business users and IT during the creation, management, validation, and deployment of customized process and decision automation solutions. Business users can modify business logic and business processes without requiring assistance from IT staff.

The service is sized for istance. Each one consists of:

- 8 VCPUs
- 16 GB of RAM

4.4.5.2 Features and Advantages

The main features and functionalities of the service are:

- *Process Modeling & Simulation* → allows business analysts and developers to collaborate on process definition using a standard language (BPMN 2.0) with drag-and-drop tools.
- *Process Automation & Orchestration* → allows for the automation of repetitive tasks and decision rules.
- *Human Workflow Management* → automatic assignment of tasks based on roles, priorities, and workloads. Intuitive user portal for completing, delegating, or commenting on tasks.
- *Monitoring, Reporting & Optimization* → real-time dashboard for performance analysis based on KPIs and SLAs, reporting, optimization recommendations through predictive analytics, and historical data.
- *Security & Governance* → integrated authentication with LDAP/Active Directory. Granular roles for users and groups (process owner, approver, admin). Complete audit trail for compliance and traceability. Version control and approvals prior to deployment.
- *Cloud & DevOps Integration* → offered as a managed cloud service. Integration with CI/CD pipelines and DevOps tools.

The service, based on IBM technology, is organized into the following integrated modules that cover the entire process lifecycle—from modeling to performance measurement.

- *Process Designer* → Visual process modeling tool.
- *Process Center* → Centralized repository and collaborative environment, allows you to manage multiple versions of processes, reuse common components, and collaborate across multiple teams.
- *Process Server* → Process execution engine. Manages both human and automated tasks.
- *Process Portal* → User portal for receiving, executing, or approving tasks.
- *Performance Data Warehouse (PDW)* → Performance collection and analysis system, stores process execution data and enables historical analysis and real-time monitoring.

The service offers the following advantages:

- • Operational efficiency and cost reduction* → automation and reduction of manual and repetitive tasks, resulting in reduced personnel costs, errors, and inefficiencies.
- *Transparency and control* → end-to-end visibility. Each process is tracked in real time. Increases accountability and control.
- *Quality and standardization* → consistent and compliant processes. Ensures processes are always executed consistently, reducing deviations and variability.
- *Compliance and auditability* → complete traceability for audits and regulatory compliance. Every step and decision is documented, facilitating internal controls and regulatory compliance
- *Monitoring and observability* → integrated dashboards and analytics.

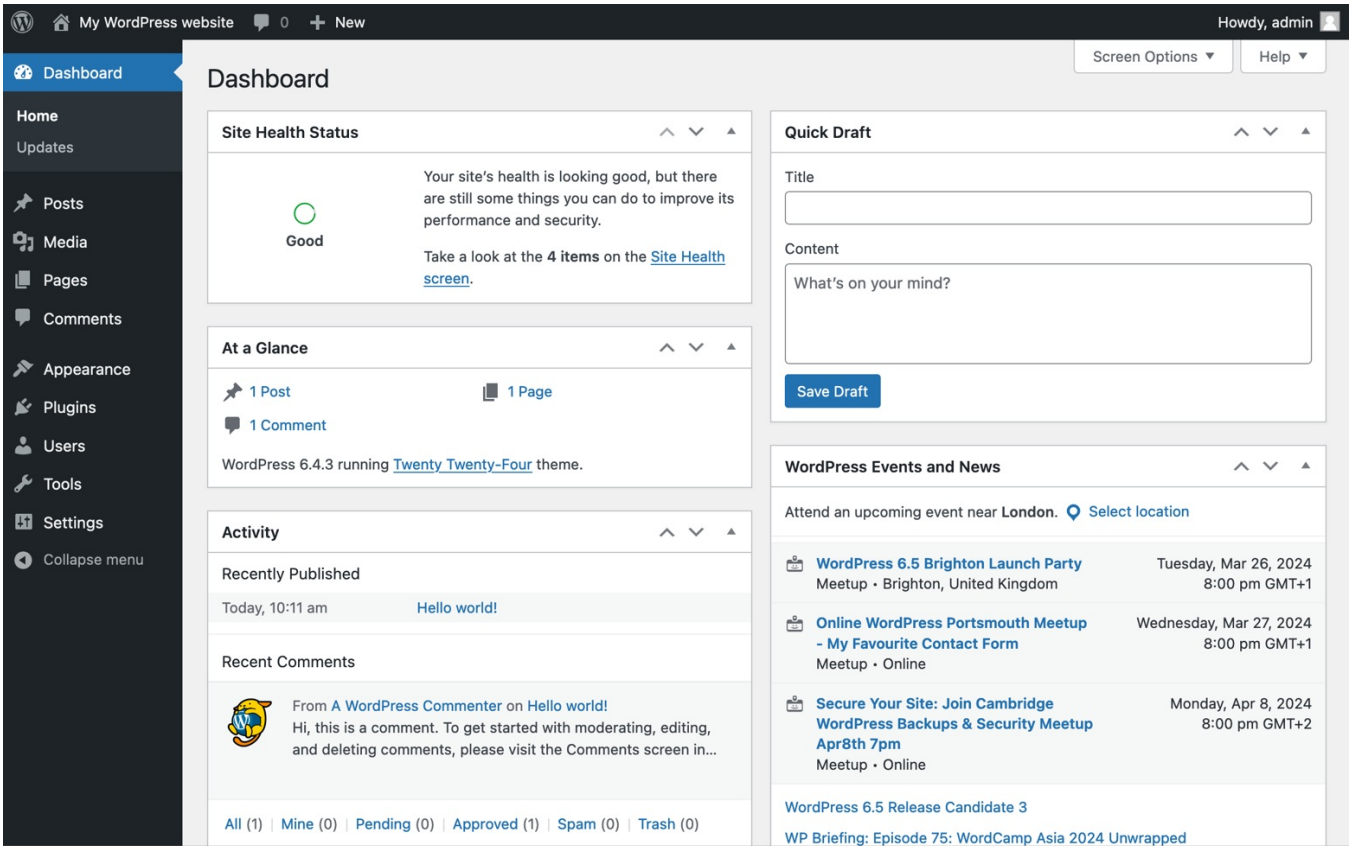
4.4.6 Content Management Systems (CMS) as a Service

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform



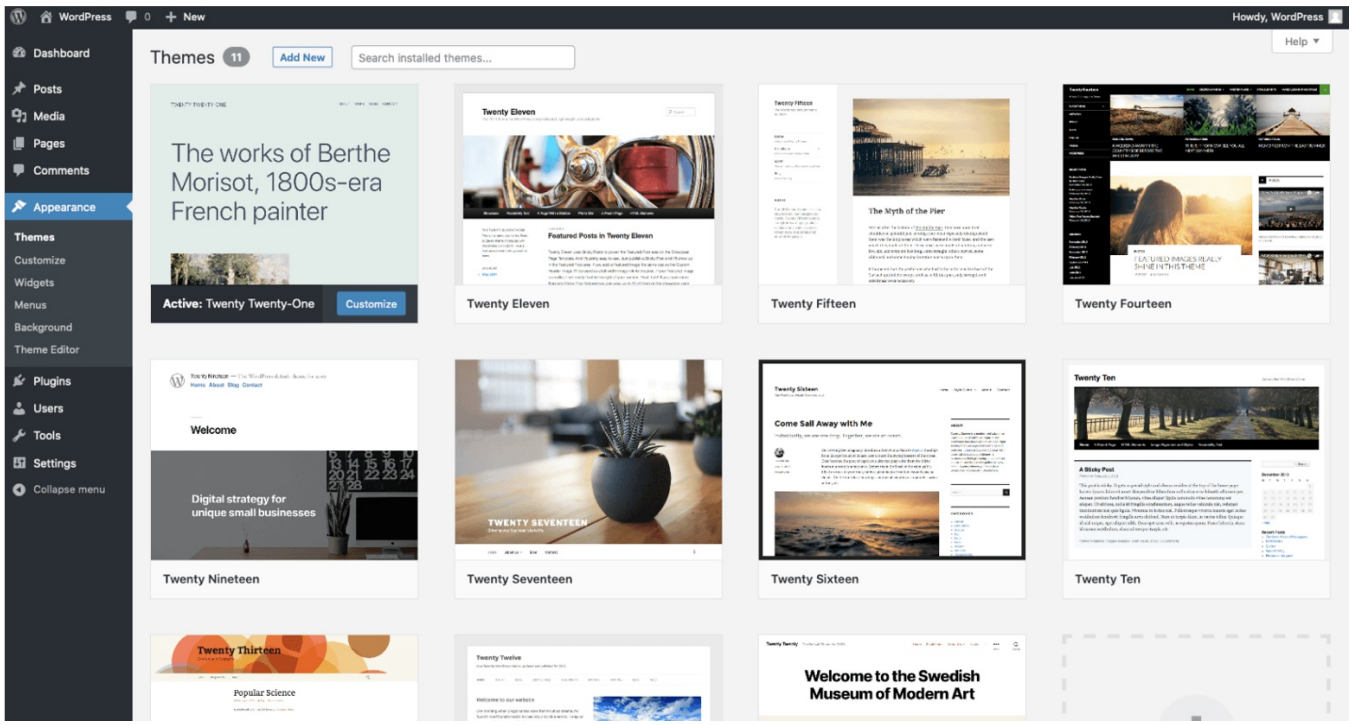


Figura 17 – Content Management Systems (CMS) as a Service

4.4.6.1 Service Description

The service, based on Wordpress, provides comprehensive and versatile tools for creating and managing websites and blogs based on CMS (Content Management System) solutions, which are cloud-based Content Management Systems (CMS) delivered as a service, without having to install or maintain software on your own server.
It offers a centralized system that allows for scalable, integrable, and multi-channel content management, with consumption-based costs and no infrastructure overhead.
This allows users to focus solely on content creation and management, while the platform handles hosting, maintenance, and updates.

The service is offered every 1000 users for unit.

4.4.6.2 Features and Advantages

The main features and functionalities of the service are:

- *Website creation* → content publishing.
- *Content management (CMS)* → ability to create, edit, and delete content.
- *Intuitive user interface* → easy content access.
- *Customization via themes and plugins* → layout management and use of plugins for customization
- *SEO-friendly* → search engine visibility.
- *Flexibility and scalability* → adaptability based on needs.
- *Open Source and Community* → collaboration with the online community.
- *Accessibility* → tools to improve readability, contrast, keyboard navigation, and compliance with accessibility standards for users with disabilities.

The service offers the following advantages:

- *Accelerated time to market* → rapid launch of websites and apps.
- *Reduced operating costs* → no servers or internal maintenance. High availability and resilience.
- *Support for omnichannel strategies* (web, mobile, e-commerce, IoT).
- *Ability to operate in multiple markets* with multilingual websites.
- *Simplified collaboration* for distributed teams.
- *Continuous innovation at no additional cost* → new features released by the provider.
- *Native integration with cloud services* (CRM, analytics, AI, CDN).

- *Front-end/back-end separation* → freedom to use modern frameworks (React, Vue, Angular, etc.).

4.4.7 Semantic Knowledge Search

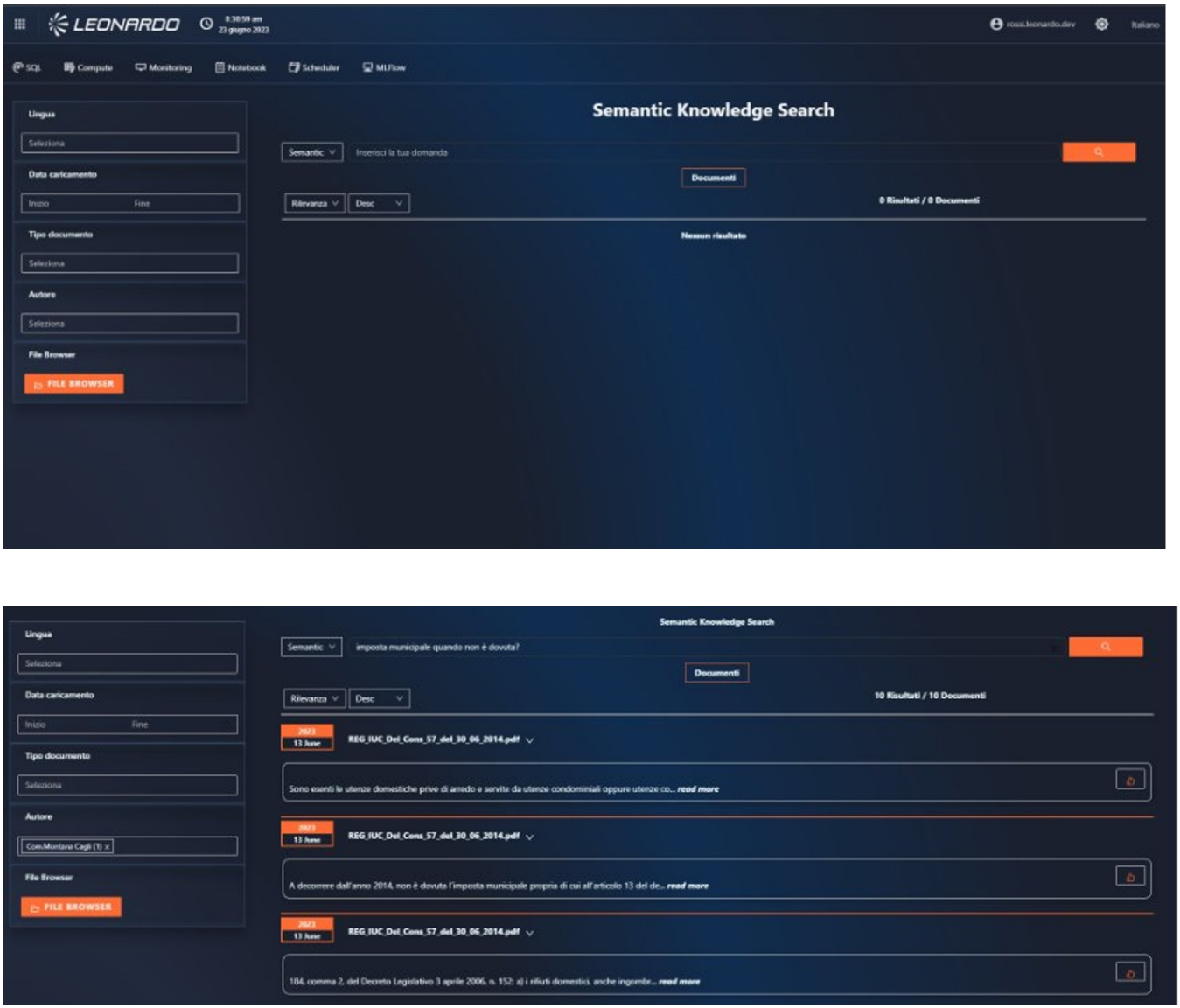


Figura 18 – Semantic Knowledge Search Service

4.4.7.1 Service Description

This service, developed by Leonardo, provides a ready-to-use platform that makes information contained within the information assets easily accessible, using a semantic search engine capable of interpreting natural language queries in different languages.
It considers the search context, word variations, and synonyms to find relevant results from a semantic database for a given domain based on a user's natural language query.
The service allows for the management of content in various formats (Word documents, PDFs, PowerPoint presentations, emails, images, etc.) through an upload service capable of inferring and processing the document type.
The tool is able to filter and select the most relevant information for the user through the use of an NLP (Natural Language Processing) model, also allowing complete navigation of the indexed document. The services are designed to ensure digital sovereignty through deployment on a secure national infrastructure, with a particular focus on latency and optimization of computational resources.
It allows users to enter feedback on individual results returned by the search engine, in order to take into account domain knowledge to better refine the results provided by the system.

The service is sized per container unit. Each container consists of:

- 8 VCPUs
- 16 GB of RAM

4.4.7.2 Features and Advantages

The platform bases its semantic search methodology on a database of carefully selected internal information sources, as well as on feedback from system users.
This way, the results produced will prove significantly more effective, as the output of an IT tool will be combined with the assessments of domain experts.
The platform will allow users to:

- Submit natural language queries in different languages.
- Reduce information search times, which will no longer be based on manual consultation of documentation, but will instead benefit from the efficiency of AI
- Optimize the tool and share the experiences of individual operators through the feedback system.

The main components of the service are:

- *Client App* → user-friendly frontend through which users can interact to submit questions in different languages, find documents relevant to the question, narrow the search field through relevant metadata, submit feedback, and index their documents by uploading one or more files.
- *FastAPI Framework* → modern, fast (high-performance) web framework for creating APIs with Python, based on the OpenAPI and JSON Schema standards.

- *Bidirectional Encoder Representations from Transformers* → pre-trained deep learning models that provide a foundation upon which to build custom versions to address a wide range of tasks. Examples include sentiment analysis, named entity recognition, text engagement (i.e., next sentence prediction), semantic role labeling, text classification, and coreference resolution.
- *Apache Tika* → Software for data extraction, language identification, and content analysis. It can find and extract text and metadata from over a thousand file formats.
- *OpenSearch* → A distributed search engine that provides extremely fast full-text search capabilities and high-performance indexing of all data types. Interaction with the search engine occurs via REST API technology.

The service offers the following advantages:

- *Faster and more informed decisions* → teams have easier access to corporate knowledge, reducing analysis and decision-making time.
- *Better use of information assets* → implicit or distributed knowledge within corporate silos (documents, emails, databases, CRM, etc.) is made searchable and semantically linked, reducing the loss of know-how or information dispersion.
- *Reduced operating costs* → PaaS eliminates the need to manage proprietary infrastructure for indexing, NLP, and data linking.
- *Innovation and competitive advantage* → differentiate products and services with a more intelligent user experience.
- Accelerated time to market → PaaS services are ready to use and easily integrated via API, allowing for the rapid development of new knowledge-driven applications.
- *Simplified scalability and management* → manage provisioning, updates, load balancing, and fault tolerance.
- *Access to advanced AI/NLP technologies* → semantic engines based on embeddings, ontologies, graph search, and machine learning without having to implement them internally. - Continuous updates with the latest developments.
- *Multi-source integration* → Semantic Knowledge Search PaaS allows you to connect structured and unstructured data from multiple sources and supports standard connectors (REST API).
- *Managed security and compliance* → authentication, authorization, and encryption are integrated into the service.

4.5 Data Protection Family

Below is the list of services belonging to Data Protection family:

- Backup Platform

4.5.1 Backup Platform Service

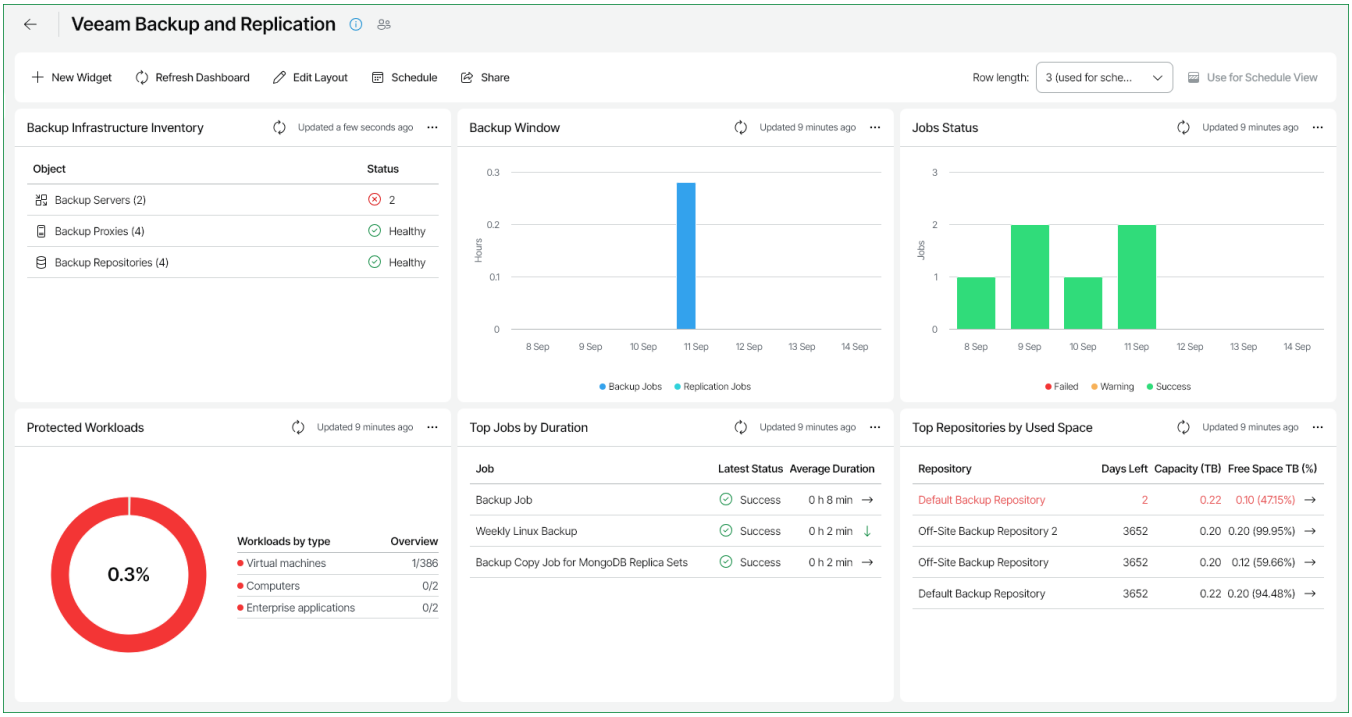


Figura 19 – Backup Service

4.5.1.1 Service Description

The PaaS Backup (Veeam-based solution) is a fully managed platform service that provides automated, secure, and reliable data protection for virtual machines, cloud workloads, and application data.
The service ensures consistent backups, rapid restores, and long-term retention without requiring customers to deploy or maintain backup servers, storage repositories, or complex scheduling policies.
The solution is designed for enterprise-grade data protection, offering backup automation, disaster recovery enablement, policy-based lifecycle management, and secure multi-tenant separation within cloud environments.

The service is offered for single TB sizing.

4.5.1.2 Features and Advantages

The service offers the following key features:

- *Automated VM and cloud resource backup* → Protects: virtual machines, cloud instances, application data, OS and configuration states. Supports image-level and incremental backups for optimal efficiency.
- *Policy-based backup management* → Create backup policies defining: scheduling, retention periods, backup types (full, incremental, differential), storage tiers. Ensures consistent and compliant protection across

environments.

- *Application-consistent backups* → supports VSS-based and application-aware backups for: databases (SQL, Oracle, etc.), Active Directory, file systems, transactional workloads. Guarantees recoverability and data integrity.
- *Multiple restore options* → Full VM restore, instant recovery to cloud infrastructure, file-level recovery, application or database item-level restore, cross-region or cross-environment recovery
- *Backup storage flexibility* → uses managed backup repositories within the cloud. Tiers include: performance storage (for fast restore), capacity storage (for long-term retention), archival storage (optional)
- *Immutable and secure backups* → optional immutability features for ransomware protection. Write-once, read-many (WORM) retention policies. Encrypted transport and encrypted-at-rest repositories.
- *Monitoring and reporting* → dashboards for job success, failures, and SLA compliance. Alerts for - *Disaster recovery integration* → supports replication features for DR strategy. Enables fast failover to cloud environments. Provides restore testing and verification tools.
- *Zero infrastructure management* → No need to deploy backup servers or agents manually. Provider handles: scaling, patching, repository management, backup infrastructure health.

The main components of the service are:

Backup management cluster → centralized system orchestrating all backup operations. Handles scheduling, job execution, and policy enforcement. Highly available and fully managed by the provider. - *Backup proxies and data movers* → distributed components that handle data transfer. Optimize performance by offloading backup/restore workloads. Integrated with cloud virtualization platforms. - *Backup repository layer* → multi-tier repository infrastructure for: short-term storage, long-term retention, immutable storage. Redundant and scalable for large data volumes. - *Control plane* → manages backup policies, job configurations, user permissions and multi-tenancy, SLA definitions, reporting and analytics, API-driven automation. - *Data plane* → responsible for: VM snapshot creation, data extraction and compression, transport - *Security & compliance layer* → encryption in transit and at rest. Tenant isolation at storage and management layers. Compliance with data protection standards (GDPR, ISO, etc.). - *Observability & alerting layer* → real-time monitoring of backup/restore jobs. Alerts on job failures, capacity issues, and SLA violations. Audit logs for operations and access tracking.

The service offers the following advantages:

- *Reliable and consistent data protection* → ensures all virtual machines and data are continuously protected. Reduces risk of data loss and improves operational resilience.
- *Simplified backup management* → fully managed service eliminates infrastructure complexity Policy-based automation ensures compliance and consistency.
- *Fast and flexible recovery* → instant VM recovery dramatically reduces downtime. Granular restore options improve operational efficiency.
- *Ransomware resistance* → immutable backups prevent malicious modification or deletion. Secure repository

design strengthens recovery posture.

- *Cost efficiency* → no need to purchase backup servers, licenses, or storage hardware.
- *High scalability* → handles growing workloads and storage needs. Suitable for expanding cloud environments and hybrid infrastructures.
- *Improved compliance and governance* → detailed reporting supports audits, SLA measurement, and regulatory compliance. Centralized retention policies ensure consistent data handling.
- *Unified protection across hybrid environments* → protects both cloud and on-prem workloads (if extended). Supports modernization and migration scenarios.
- *Reduced operational overhead* → provider manages infrastructure, maintenance, patching, and upgrades. IT teams focus on core applications instead of backup operations.
- *Business continuity enablement* → integrates with replication and DR features. Supports failover during incidents or migrations.

4.6 Infra & Ops Platform Family

Below is the list of services belonging to the Infra & Ops Platform family:

- Multicloud Management Platform
- IT infrastructure Service Operations (Logging & Monitoring)
- PaaS Ticket Management Service
- PaaS Operations Management Service

4.6.1 Multicloud Management Platform

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

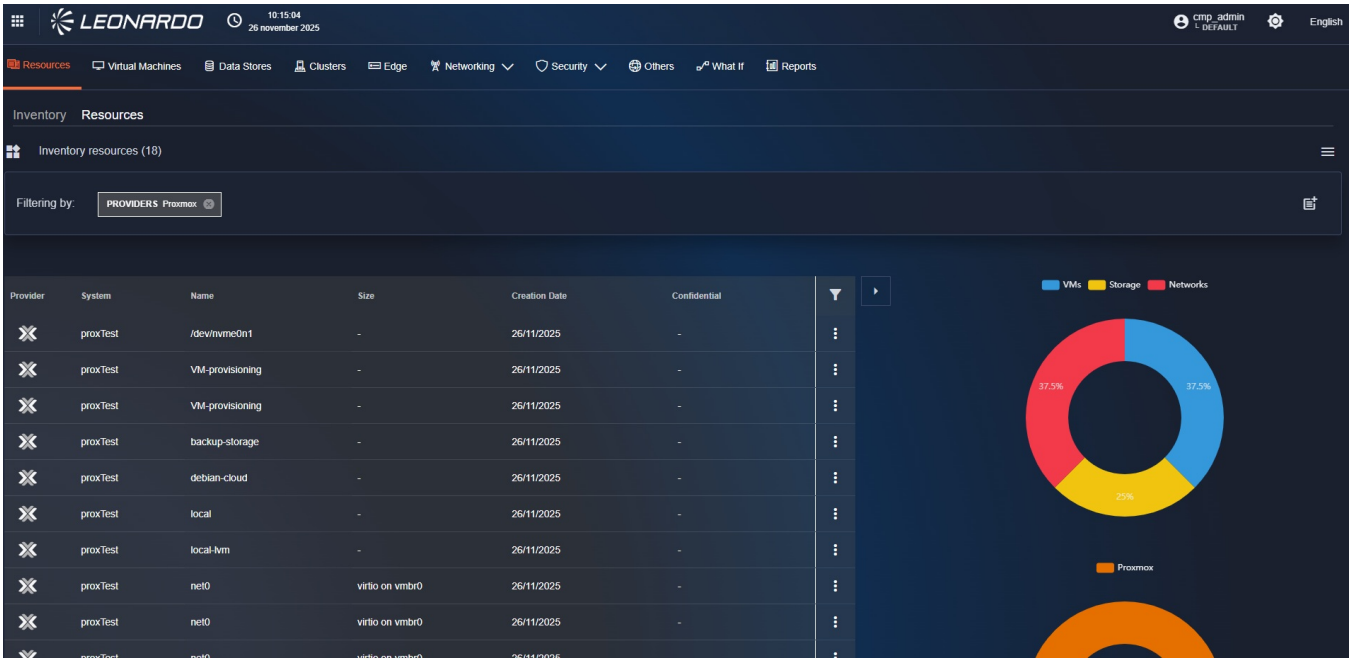


Figura 20 – Leonardo Secure Cloud Management Platform (SCMP) - Inventory interface

Figura 21 – Leonardo Secure Cloud Management Platform (SCMP) - Costs dashboard

4.6.1.1 Service Description

Secure Cloud Management Platform (SCMP) is a Multicloud management software platform, designed by Leonardo, for governance, lifecycle management, brokering, and resource automation in hybrid and multi-cloud environments. It offers a self-service portal with a unified service catalog, governance, and customizable dashboards and reports to monitor infrastructure performance and costs.
The platform allows to orchestrate, monitor, and control usage, costs, and workflow performance in complex or hybrid multi-cloud environments.
It integrates seamlessly with leading Enterprise Cloud Service Providers, On-premise resource virtualization and edge computing systems.
It can also manage self-service provisioning of resources: e.g., virtual machines (VMs), storages, clusters, containers, services, complex applications (such as blueprints), or entire application stacks (IaaS, PaaS, CaaS).

The service is sized and offered based on volumes:

- less than €1.000.000,00 in annual managed resource expenditure for Cloud resources.
- every 5 TB of managed RAM for on-premise or hybrid resources.

4.6.1.2 Features and Advantages

The service offers the following key features:

- *High compatibility and integration* → integration with major CSPs (AWS, Azure, GCP, Oracle, etc.), virtualization and on premise vendors and systems (VMware, OpenStack, HPE, Nutanix, Hyper-V, bare metal, PXE provisioning), and container orchestration systems (Kubernetes). Integration with third-party systems (e.g., ERP) to offer process automation.
- *High level of granularity and customization* → the platform offers various graphical views for monitoring and reporting, to meet the needs of each user and team. You can choose whether to have aggregate views and reports by system/subsystem, or by element type or individual element.
- *Performance and cost monitoring* → through integrated, unified, and intuitive dashboards, users can monitor the current and forecasted status of systems, subsystems, and related resources in terms of resource usage and generated costs. Views can be presented in graphical form with custom tables or graphs, or through the creation of reports, which can be exported in various formats or sent to users periodically. The platform manages the monitoring of aggregate and/or resource/team/cloud costs and enables predictive cost analysis (what-if analysis) to identify waste, comply with recommendations (e.g., resizing, rightsizing), implement budget guardrails, etc.
- *Self-Service Catalog and Item Provisioning* → authorized users can create and manage their own catalog to

orchestrate and manage the various elements within it. For example, an authorized user can deploy new infrastructure resources (e.g., VMs, storage resources, network resources, etc.) to the desired CSPs, launch or modify standard or custom services, pre-configured environments, and blueprints (both proprietary and IaC).

- *Multicloud security monitoring* → thanks to compatibility with existing security systems and appliances (e.g., SIEM, Key Vaults, Remote attestation for confidential computing, etc.), you can centrally manage your organization's security posture, detecting any vulnerabilities, discrepancies, or non-compliance on the systems or resources monitored by the platform.
- *Data and User Security Management* → the platform does not process customer data, but only the use of CSP services and/or resources. Identity and access management (IAM) mechanisms are foreseen with the implementation of MFA and RBAC authentication logics, compliant with the principle of least privilege, to regulate access to IT resources and related information based on roles, responsibilities and authorization levels.

The main components are:

- Abstraction Layer (ABS) → lowest platform layer that executes operational workflows towards integrated CSPs.
- Resource Layer/Manager (RM) → highest platform layer responsible for executing user requests. It is composed of the following modules:
  - Costs: module responsible for managing and displaying resource costs.
  - Security: module responsible for managing and displaying security policies and resource compliance status.
  - Monitoring: module responsible for managing and displaying resource usage metrics.
  - Inventory and Catalog: modules responsible for managing and displaying all allocated and available resources.
  - Provisioning: module responsible for the automation and provisioning logic of resources and other services. Tenant: Module responsible for multi-tenant service management and external operational requests
- Persistence Layer → NoSQL database (MongoDB) used by the RM to store normalized data retrieved from the respective ABS submodules.
- Integration and Communication Layer → facilitates and orchestrates asynchronous information communication between the ABS and RM modules of the system; allows the ABS submodules to interact with the various APIs of the respective CSPs and external systems
- Security and Authentication Layer → access management and encryption of sensitive data from provider systems.

The service offers the following advantages:

- *Simplify the management of heterogeneous and complex IT infrastructures* → centralizes resource management across multiple clouds or hybrid infrastructures, simplifying visibility, management, and control of distributed resources.
- *Scalability and flexibility* → identifies the most suitable IT services and resources at the time, continuously adapting to business needs.

- *Cloud expense optimization* → enables constant monitoring and optimization of current and forecasted IT infrastructure expenses.
- *Agility and speed* → on-demand resource allocation and automation of daily operations (e.g., resource management, configuration, scaling) reduces provisioning times and the workload for IT groups.
- *Faster and more informed decisions* → guides IT development strategy with a data-driven approach.
- *Reduced time to market* → reduces the time required to develop and deploy new applications, improving time to market and accelerating response to market needs.
- *Improves the reliability of services and processes* → governance, security, and compliance policies can be centrally managed, ensuring that Resources are protected and regulations are complied with.
- *IT Operations Support* → can be integrated with IT service management (ITSM) and IT operations automation tools (such as Ansible, Chef, SaltStack), improving service quality and reducing manual errors.

4.6.2 IT infrastructure Service Operations (Logging & Monitoring)

Figura 22 – IT infrastructure Service Operations (Logging & Monitoring) interface

4.6.2.1 Service Description

Developed by Leonardo, this is an Application Performance Monitoring (APM) service that monitors and controls infrastructure performance supporting applications (e.g., latency, errors, service availability) and workloads deployed in the Cloud environment.
It provides centralized collection and analysis across various infrastructure elements: Servers and VMs, Containers and orchestrators, Cloud providers, and Network.

The service is offered per 1 GB of data storage.

4.6.2.2 Features and Advantages

The Log & Audit service built on OpenTelemetry provides a unified and vendor-neutral way to collect, process, and export observability data. Its core capabilities include:

The service offers the following main features:

- *Log collection & aggregation* → vaptures application logs, system logs, and security-relevant audit trails. Supports structured logging for consistent and machine-readable data.
- *Audit trail generation* → tracks user actions, configuration changes, and security-sensitive operations. Ensures immutability and integrity through standardized data formats and export pipelines.
- *Distributed tracing* → enables end-to-end traceability across microservices. Helps correlate logs, metrics, and traces for full-context auditability.
- *Metrics and performance data* → collects operational and performance metrics (CPU, memory, network, API latency). Correlates metrics with logs and traces for accurate diagnostics.
- *Policy-driven data processing* → allows filtering, sampling, redaction, and enrichment through OpenTelemetry Collectors. Ensures sensitive information is processed according to compliance policies.
- *Multi-destination export* → exports data to SIEM platforms, log analytics tools, data lakes, or object storage. Supports Elasticsearch, Splunk, Loki, BigQuery, and more.

The main components of the service are:

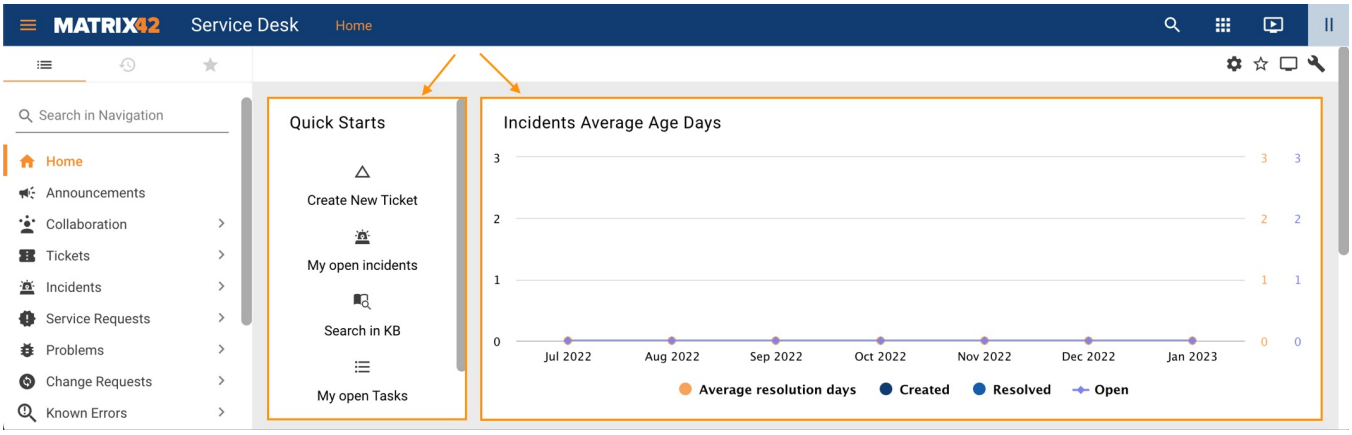
- *Instrumentation Layer* → applications and services instrumented using OpenTelemetry SDKs and auto-instrumentation agents. Generates logs, metrics, and traces in a standardized OTLP format.
- *OpenTelemetry collector* → central component responsible for: receiving data (logs, metrics, traces); processing/enriching it; exporting it to one or more backends.
  Can run as: a sidecar in Kubernetes, a daemonset on each node, a centralized collector cluster.
- *Export & storage layer* → observability and security data coud be sent to: log storage (Elasticsearch, Loki, Cloud logging platforms); SIEM systems (Elastic SIEM, Splunk, Azure Sentinel); Audit archives (S3, GCS, object storage).
- *Visualization & analytics* → dashboards and visual tools (Grafana).

- Support centralized log analysis, auditing, forensics, and compliance reporting.

The service offers the following advantages:

- *Improved security & compliance* → centralized audit trails simplify compliance with standards (ISO 27001, SOC2, GDPR). Enhanced visibility into user actions and critical events reduces risk.
- *Reduced vendors Lock-in* → OpenTelemetry is vendor-neutral, enabling freedom to switch backends without re-instrumenting code.
- *Better decision-making* → unified observability data supports data-driven product and business insights. Helps organizations identify usage patterns, performance bottlenecks, and customer-impacting issues.
- *Cost optimization* → policy-driven sampling and data routing help reduce storage and licensing costs. Ability to send different data types to cost-efficient storage tiers.
- *Unified observability pipeline* → Single consistent pipeline for logs, metrics, and traces reduces operational complexity.
- *Improved troubleshooting* → correlation of logs, metrics, and traces dramatically speeds up root cause analysis. Reduces MTTR (Mean Time To Repair).
- *Scalability & flexibility* → the OpenTelemetry Collector can be scaled horizontally to handle high data volumes. Supports multi-cloud and hybrid architectures natively.
- *Standardization across teams* → developers, SREs, and security teams use a common telemetry standard. Simplifies onboarding and reduces friction in cross-team operations.
- *Extensibility* → pluggable components allow integration with new tools or pipelines without redesigning the system.

4.6.3 PaaS Ticket Management Service



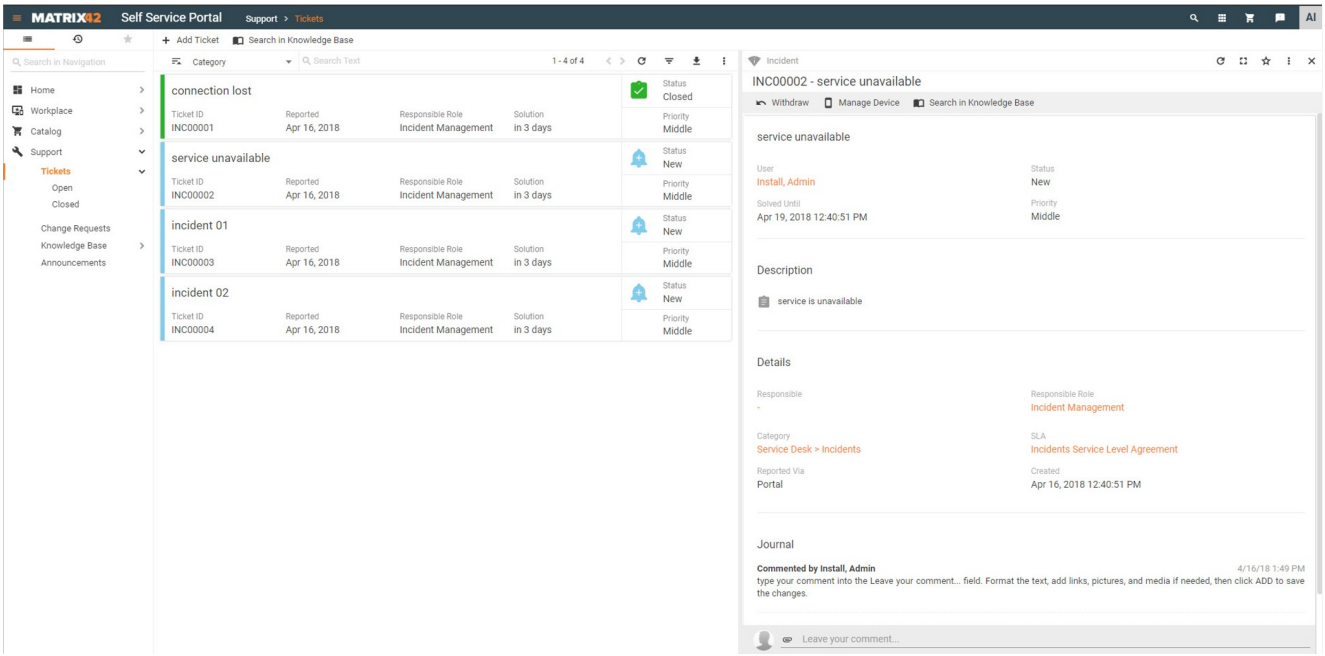


Figura 23 – Ticket Management Service interface

4.6.3.1 Service Description

The service offers tools for managing user requests, incidents, related problems, and the entire ticketing cycle.
Intelligent automation: integrated AI functions (classification, knowledge suggestion, sentiment, and draft generation) reduce manual workload and speed up resolution.
Self-service and multi-channel: users can open tickets via the portal or email and view their status. This promotes a good user experience.
Integration with assets, services, and configuration: It can connect to the service catalog, CMDB, and asset management, making ticketing part of a broader IT management ecosystem.

The service is offered for a number of Service Desk operators. Each subscription is for 50 operators.

4.6.3.2 Features and Advantages

The service, based on Matrix42, features a modular architecture, with components covering the user interface, workflow/automation engine, integration with external systems, databases, and reporting. It offers the following main features:

- *Incident and Service Request Management* → allows for the logging, classification, and resolution of incidents and service requests via a portal, email robot, or Service Desk agent.
- *Self-Service Portal and Service Catalog* → the portal allows users to request services, check ticket status, view announcements, and view knowledge/FAQs. Workflow, Automation, and Low-Code Platform → offers a visual workflow builder (drag & drop) with no coding required to automate processes such as approvals, escalations, and ticket assignment.
- *Integrated Artificial Intelligence* → the "AI Assist" module automatically suggests ticket category, impact, and urgency, analyzes user sentiment ("user mood"), and suggests knowledge base articles or similar tickets ("resolution helper").
- *SLA Monitoring, Reporting, and Dashboards* → analyzes support processes, KPIs, and provides visibility into service desk performance.
- *Customization, Roles, and Permissions* → Supports the definition of user roles, granular permissions, filters, custom views, and dedicated dashboards. agents/managers.

The main components of the service are:

- *UUX (Unified User Experience)*: the platform's UI component, which unifies the web interface ("low-code solution") for users, agents, and administrators.
- SolutionBuilder: A low-code/"no-code" module for configuring/modifying layouts, views, data models, and interfaces. Allows interface and data customization without (much) code. - *Workflow Studio / Designer / Worker Engine*: components for defining, managing, and executing workflows and automations.
- Database and storage: the platform uses multiple databases (e.g., "Master" database for operational data, "Data Warehouse" for analysis/reporting, "History Database" for logs and change history), typically on Microsoft SQL

Server + Analysis Services + Reporting Services.

- *Integration / API / Data providers*: the platform supports integration with Active Directory/Azure AD, external databases, REST API, SOAP, flat files, and SQL for reading/writing.
- *Flexible deployment*: it can be delivered on-premise, in a public cloud, a private cloud, or a hybrid ("Cloud your way") to adapt to compliance, scalability, and geographic requirements.

The service offers the following advantages:

- *Reduced operating costs* → thanks to process automation and a reduction in manual tasks, fewer repetitive interventions and a lower cost per ticket. Increased support team productivity → thanks to workflow automation, the use of AI (for automatic classification, suggestions, pre-populated responses), and self-remediation, the manual burden on IT operators is reduced. The self-service portal and knowledge base enable self-resolution of many user issues.
- *Support for business decisions* → integrated reports and dashboards provide KPIs on average response times, resolution, ticket volumes by category, and seasonal trends.
- *Improved user experience* → users can open tickets, monitor status, and find solutions independently, reducing frustration and wait times. Furthermore, it fosters a collaborative and efficient environment between users and support teams, with agents viewing the same status in real time.
- *Improved control and governance of IT services* → provides a comprehensive view of assets, users, and services, supporting regulatory compliance and service level agreement (SLA) monitoring in a documented and traceable manner.
- *Native integration with the IT ecosystem* → possible integrations with SSO systems (e.g., Active Directory/Azure AD), UEM, Asset Management, Change Management, IT monitoring, HR systems, and others via API, reducing information silos and improving data quality.

4.6.4 PaaS Operations Management

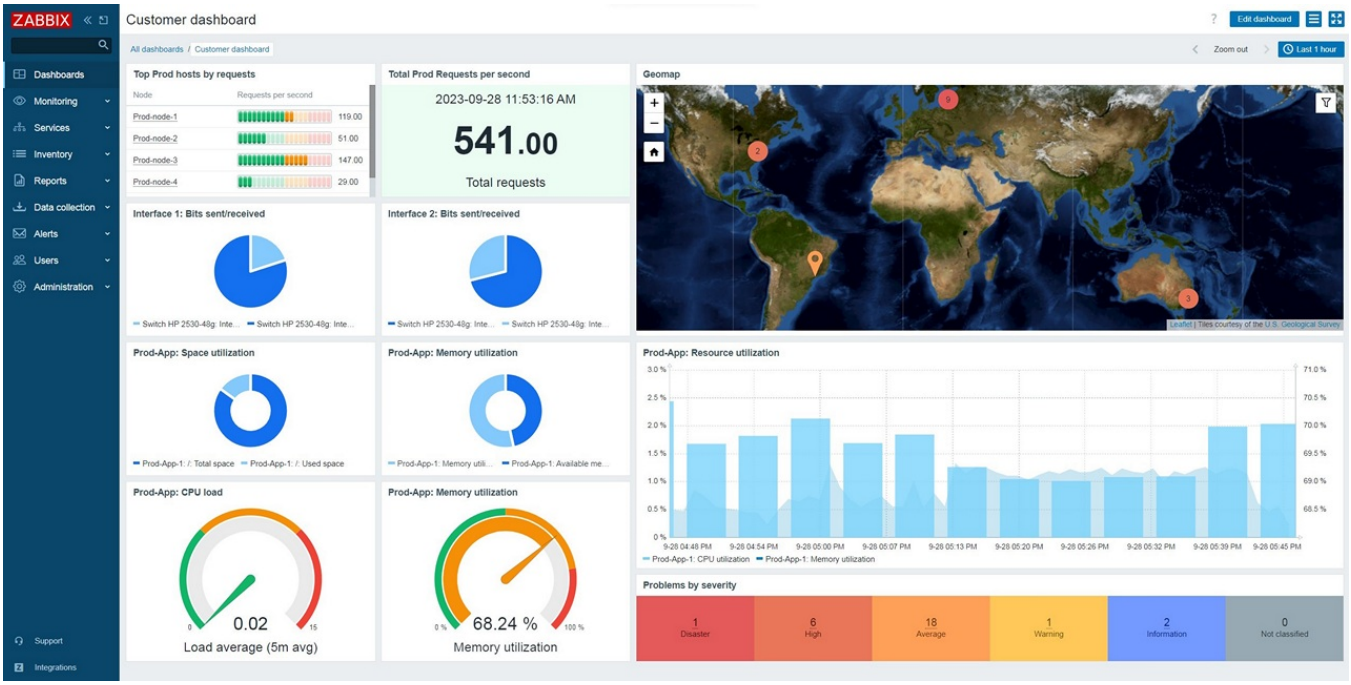


Figura 24 – PaaS Operations Management Overview

4.6.4.1 Service Description

The PaaS Operations Management service provides a fully managed platform for monitoring, observability, incident detection, and operational oversight of IT infrastructures and applications.
Based on Zabbix and NetEye, the service delivers enterprise-grade monitoring capabilities—such as telemetry collection, alerting, performance analytics, and event correlation—without requiring customers to deploy or maintain monitoring servers, databases, or agents.
Designed for hybrid and cloud-native environments, the service centralizes monitoring for compute, network, storage, security, and application layers, ensuring full visibility and operational continuity.

The service is offered and sized for every 25 concurrent users.

4.6.4.2 Features and Advantages

The service offers the following main features:

- *Comprehensive infrastructure & application monitoring* → tracks the health and performance of: VMs, containers, hosts, and cloud resources, networks, firewalls, and load balancers, storage systems and databases, application services and APIs. Supports agent-based and agentless checks.
- *Centralized metrics, logs, and telemetry collection* → consolidates metrics, ping checks, SNMP data, application logs, and custom KPIs. Ensures unified observability across heterogeneous environments. Retains historical data

for trend analysis.

- *Intelligent alerting & notifications* → event-driven alerts based on thresholds, anomalies, or dependency rules. Multi-channel notifications (email, SMS, webhook, ITSM integration). Avoids alert noise through suppression, deduplication, and escalation rules.
- *Event correlation and root cause analysis* → NetEye's correlation engine groups related events. Identifies probable root causes across interconnected systems. Reduces mean time to detect (MTTD) and mean time to repair (MTTR).
- *Dashboards and visualization* → customizable dashboards for operations, NOC screens, and business KPIs. Visual representations of system health, topology maps, and SLA views.
- *SLA monitoring and reporting* → tracks service availability against SLA targets. Generates performance, capacity, and downtime reports. Supports compliance audits and service management.
- *Automated discovery* → auto-detects new cloud resources, VMs, hosts, network devices, and services. Automatically assigns monitoring templates. Keeps monitoring configuration aligned with dynamic environments.
- *Integration with ITSM and automation tools* → supports integration with ticketing systems (ServiceNow, Jira, etc.). Exposes APIs for orchestration and automated remediation workflows.
- *Zero infrastructure management* → no monitoring servers, databases, or scaling logic to manage. The provider handlespatching, backup, capacity, and high-availability.

The main components of the service are:

- *Zabbix monitoring cluster* → distributed monitoring cluster for data collection and event processing. Supports high availability and horizontal scaling. Responsible for metrics ingestion, - *NetEye observability and correlation layer* → enhances Zabbix data with event correlation and analytics. Adds long-term storage, dashboards, reporting, and advanced alerts. Integrates with log management and SIEM modules if required.
- *Data collection layer* → supports multiple collection methods: Zabbix agents, SNMP collector, API polling, log ingestion, push gateway metrics, cloud-native exporters. Ensures flexibility across heterogeneous environments.
- *Storage layer* → time-series storage for metrics (TSDB). Log and event indexing engines. Redundant and scalable architecture for long-term data retention.
- *Control plane* → manages: template management, alert rules, agent policies, discovery rules, user and permissions configuration, integrations and webhooks
- *Data plane* → collects telemetry from monitored systems. Processes events, evaluates triggers, and generates alerts. Streams metrics to dashboards and correlation modules.
- Visualization & reporting layer → provides dashboards, SLA reports, historical charts, and heatmaps. UI tailored for NOC operations and technical teams.
- *Security & multitenancy* → segregated monitoring domains per tenant or project. Secure role-based access

controls (RBAC). Encrypted communication between monitoring agents and servers.

The service offers the following advantages:

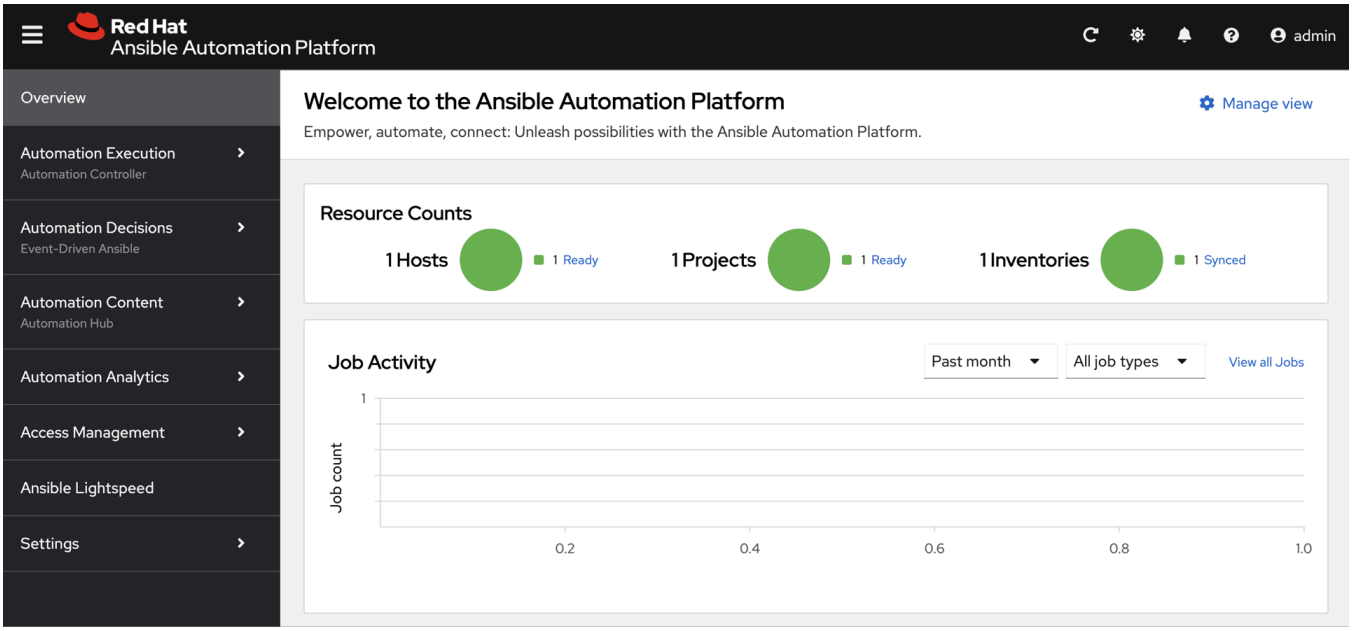
- *End-to-end visibility* → unified monitoring across cloud, on-prem, and hybrid environments. Central view of all operational metrics and services.
- *Faster detection and resolution* → intelligent alerts and event correlation reduce noise and improve detection. Lower MTTR thanks to root cause analysis and detailed telemetry.
- *No Infrastructure to manage* → fully managed service—no servers, DBs, or upgrades to maintain. Reduces operational burden on IT and DevOps teams.
- *Enhanced reliability and SLA compliance* → continuous monitoring ensures proactive issue identification. Supports SLA tracking and reporting for internal/external services.
- *Scalability and performance* → handles thousands of checks per second. Automatically adapts to growing or dynamic infrastructures.
- *Cost efficiency* → avoids the cost of deploying, licensing, and maintaining monitoring platforms.
- *Enterprise-grade security* → isolated tenant environments. Encrypted agent communications and secure data storage.
- *Improved operations and governance* → supports audit requirements with historical logs and performance reports. Ensures transparency and accountability in service operations.
- *Integration with ITSM and automation* → automatic ticket creation for incidents. Enables self-healing workflows and auto-remediation.
- *Better user and customer experience* → early detection prevents service degradation. Ensures smooth, predictable operation of business-critical applications.

4.7 DevSecOps Family

Below is the list of services belonging to the DevSecOps family:

- Configuration Manager
- Test Automation
- Quality Code Analysis
- DevSecOps As A Service
- Qualizer DevSecOps

4.7.1 Configuration Manager



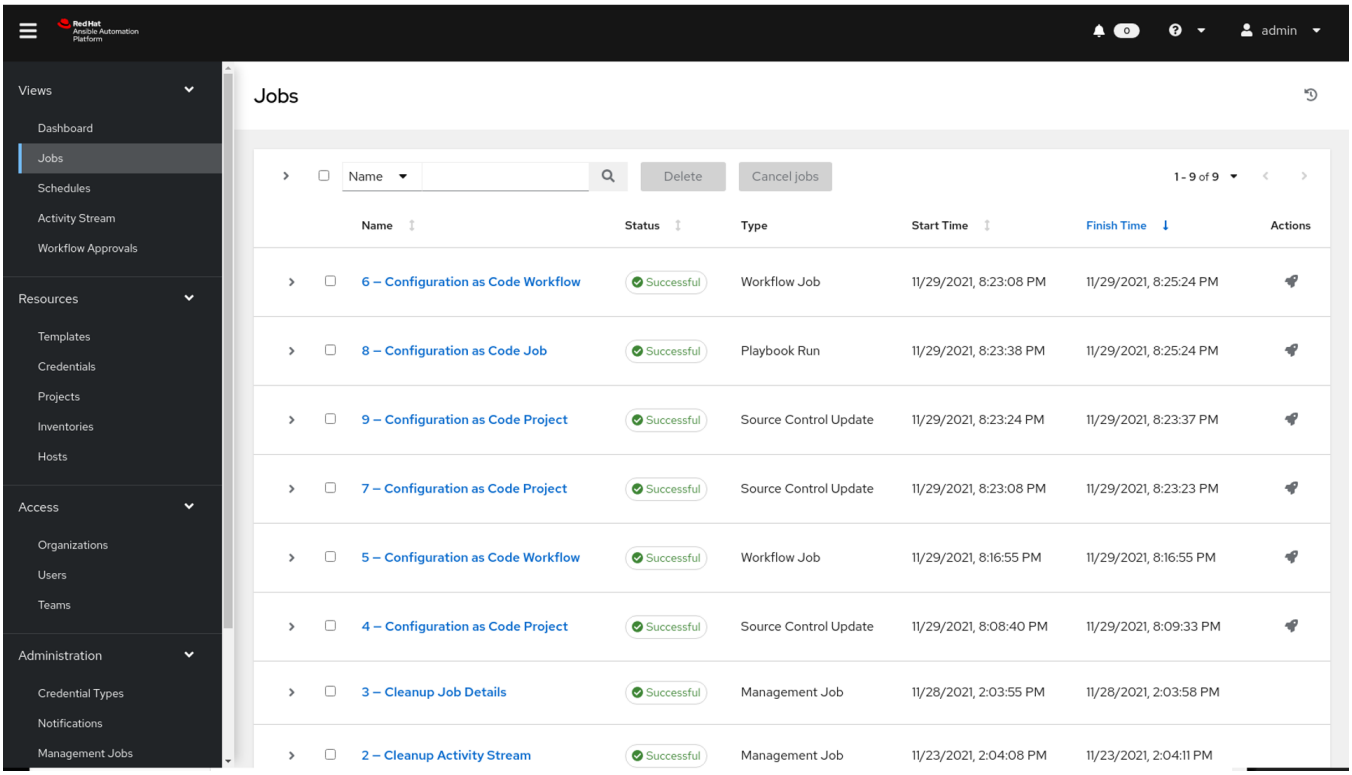


Figura 25 – Configuration Manager Service interface

4.7.1.1 Service Description

The service, based on Red Hat Ansible Automation Platform, is a comprehensive automation solution for managing IT infrastructure, simplifying operations, and accelerating development and deployment processes.
It is a platform that acts as a powerful and flexible configuration manager, helping organizations automate repetitive or manual tasks, implement complex configurations, and orchestrate workflows centrally and securely through a declarative and automated approach, ensuring consistency and improving overall operational efficiency and compliance.

The service is offered and sized in units of 25 Managed workers.

4.7.1.2 Features and Advantages

The service offers the following main features:

- *Declarative automation* → use of playbooks to clearly describe the desired state of resources. Support for role-based automation, reuse, and modular configurations.
- *Centralized execution management* → task orchestration via Ansible Controller with scheduling, auditing, and notifications. Dashboards and reporting for real-time monitoring of automations.
- *Integration with DevOps pipelines* → support for CI/CD tools (Jenkins, GitLab, GitHub Actions, OpenShift Pipelines). Automatic execution of playbooks in response to events or code commits. Credential and secret management. Integration with Red Hat Ansible Vault, CyberArk, HashiCorp Vault, and other secret managers.
- *Scalability and multi-tenancy* → support for multi-organization environments with role and access segregation. Distributed execution via containerized Automation Execution Environments.
- *Compliance and security* → full operation logging and Role-Based Access Control (RBAC)-based access control. Compliance with corporate and regulatory security standards.

The service uses an agentless architecture and YAML-based playbooks to define, deploy, and maintain desired system states across various infrastructure components, including servers, networks, storage, and cloud resources. The main components of the service are:

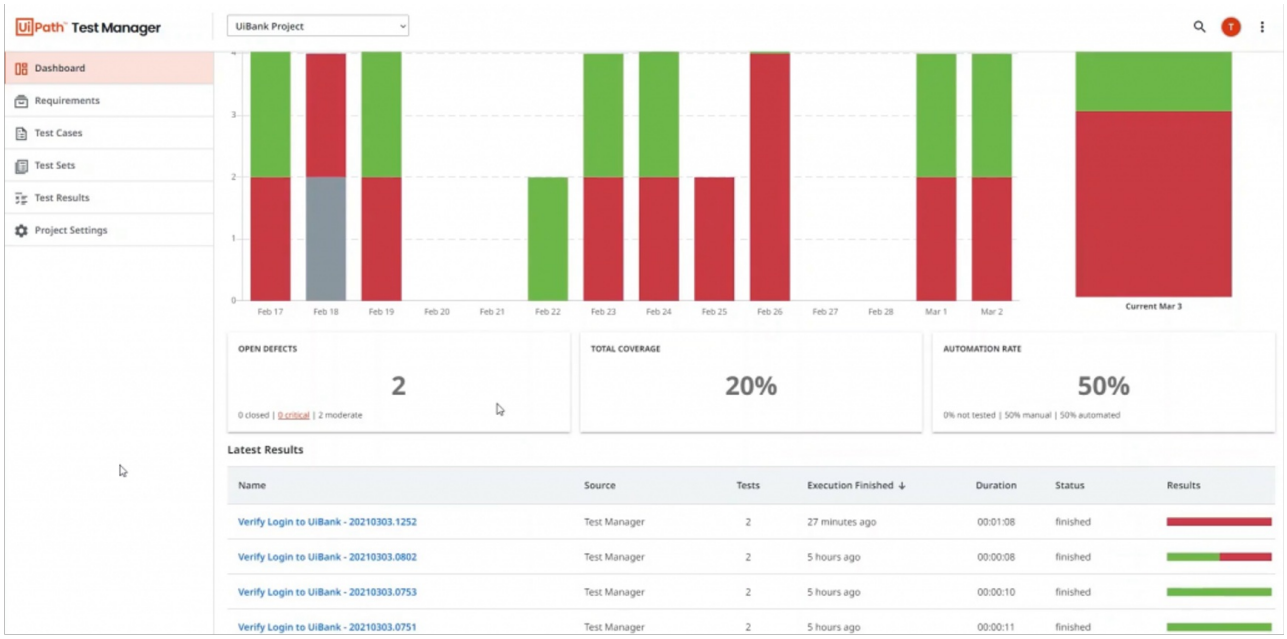
- *Automation Controller* → Web interface and REST API for centralized automation management. Orchestration engine that coordinates playbook execution.
- *Automation Execution Environments (EE)* → standardized containers containing the Ansible runtime, modules, plugins, and specific dependencies. They enable portability and consistency of execution across different environments.
- *Automation Hub* → private repository for distributing content collections (modules, roles, plugins). It promotes reuse and version control of Ansible content.
- *Automation Mesh* → distributed architecture for scalable job execution on remote nodes or in the cloud. Ensures reliability and load balancing of automations

- *Inventory and Credential Store* → defines target systems (servers, VMs, containers, network devices, cloud services). Securely manages access credentials for each target or environment. *APIs and Integrations* → RESTful API for integration with external monitoring, ticketing, or orchestration systems.

The service offers the following advantages:

- *Reduced operating costs* → automating repetitive and manual tasks reduces the time spent on system management and maintenance.
- *Increased reliability and service quality* → standardized and automated configurations reduce inconsistencies between environments (dev, test, prod).
- *Scalability of IT business* → the platform grows with the organization, managing hundreds or thousands of nodes without linear staff growth.
- *Improved IT compliance and governance* → all changes are tracked and documented, ensuring transparency and compliance with regulations and corporate policies.
- *Increased productivity and collaboration* → DevOps, IT Operations, and Security teams can work on a single shared platform, reducing organizational silos.
- *End-to-end automation* → from operating system configuration to application deployment, patch management, and ongoing maintenance.
- *Standardization and repeatability* → playbooks ensure consistent configurations and easy reuse of automation code.
- *Centralized and secure management* → a single interface (Controller) for orchestrating jobs, managing inventories, credentials, and access policies (RBAC). Secure management of credentials and secrets (Vault), centralized auditing, and support for enterprise authentication (LDAP, SSO, OAuth).
- *Distributed scalability* → job execution can be distributed across multiple nodes, improving performance and resilience.
- *Complete visibility and traceability* → dashboards and analytical reports allow you to monitor the effectiveness of automations and resource usage.

4.7.2 Test Automation



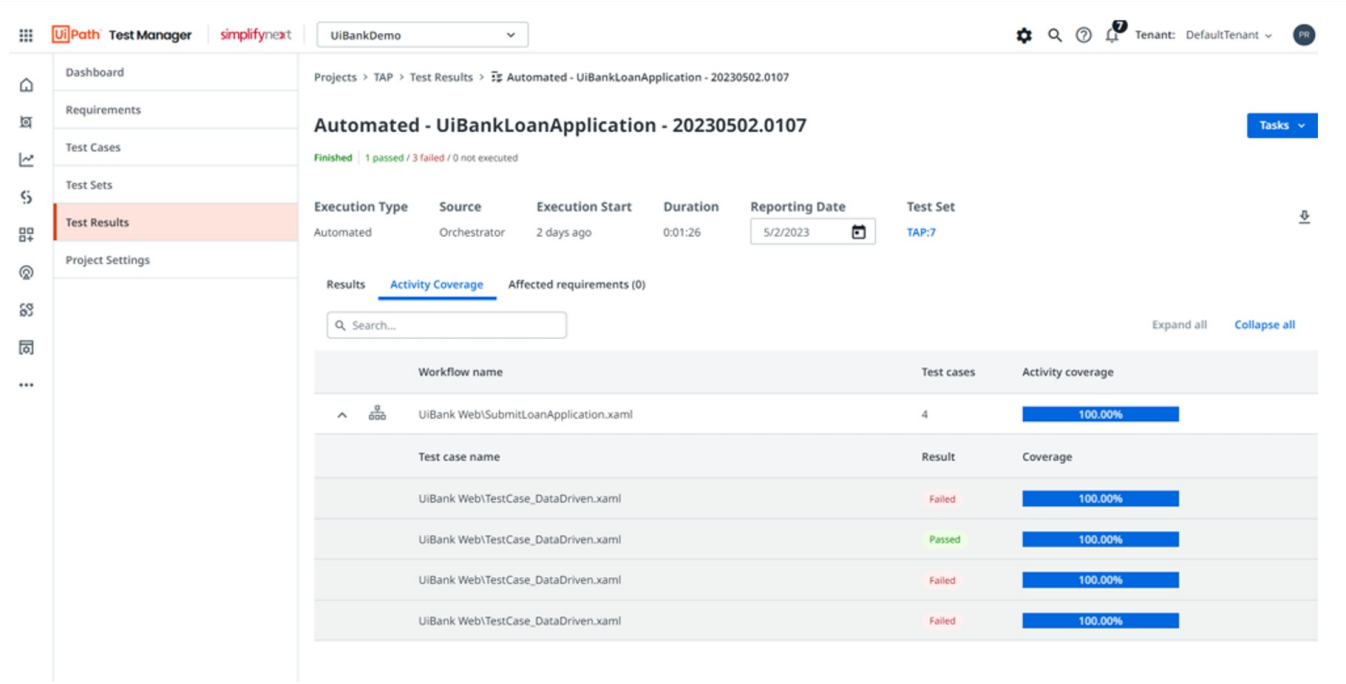


Figura 26 – Test Automation Service

4.7.2.1 Service Description

The service is designed to automate software testing activities, with the goal of improving quality, reducing release times, and increasing development process efficiency.
The solution uses the UiPath RPA (Robotic Process Automation) platform to automate software testing (functional, regression, API, user interface).
It was created to support both IT and business teams in the continuous validation of applications, digital processes, and RPA robots to increase testing efficiency and ensure software integrity.
It supports Agile and DevOps approaches with Continuous Testing to ensure code changes do not introduce new defects.
Centralized monitoring: Test results are collected and displayed in a single interface, facilitating monitoring and analysis via UiPath Test Manager and extensible with dashboards on UiPath Insights.

The service is sized and offered per user units. Each unit is consists of: 10 automation testers -concurrent, 5 Robots.

4.7.2.2 Features and Advantages

The service offers the following main features:

- *Test automation for applications* → test automation for web, desktop, mobile, and API applications. Support for cross-browser and cross-platform testing. Reuse of RPA components → automations developed in UiPath Studio can be reused as test cases. This reduces test creation time and costs.
- *Test Manager* → centralized tool for planning, executing, and monitoring tests. Dashboard with KPIs and integrated reporting.
- *DevOps Integration* → integration with CI/CD tools (Azure DevOps, Jenkins, GitLab, etc.). Ability to run tests in software release pipelines.
- *Scalability* → tests can be deployed to UiPath robots in parallel, reducing execution times.
- *Automated Continuous Testing* → "Shift-left" approach: quality is validated from the early stages of development. Ensures fewer bugs in production.

The main components of the service are:

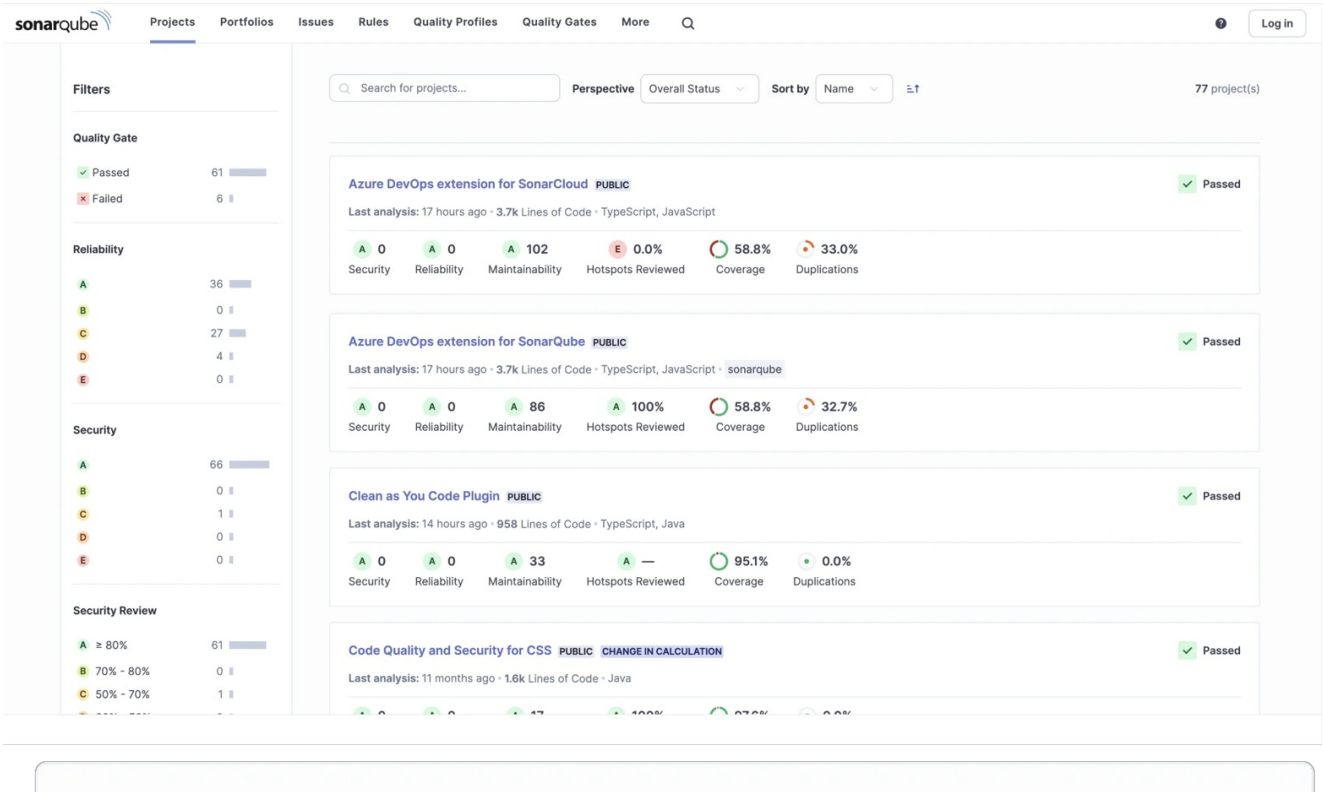
- *Studio / Studio Pro* → Development environment (IDE) for creating automated tests, similar to creating RPA workflows.
- *Orchestrator* → for scheduling, deploying, and running tests at scale.
- *Test Manager* → for managing requirements, organizing test suites, collecting metrics and reporting.
- *Robotic Test Execution* → UiPath robots become "digital testers," running tests autonomously.
- *Testing Robots* → Specialized test execution robots; support testing frameworks such as NUnit, MSTest, and Junit.
- *Insights* → Manages the creation of dashboards for monitoring various testing processes; allows you to calculate

the return on investment of initiatives.

The service offers the following advantages:

- *Reduced software release times* → thanks to faster and more continuous testing cycles.
- *Improved software quality* → fewer bugs in production and reduced maintenance costs.
- *Reduced manual testing costs* → less time spent on manual testing and more focus on strategic testing.
- *High Return on Investment (ROI)* → thanks to a single automation and testing platform.
- *IT-business alignment* → greater reliability and traceability of results.
- *Support for Agile and DevOps CI/CD approaches* with continuous validation.
- *Reduced risk of regressions* → more confident release of new features.
- *Multi-level test automation* (UI, API, mobile, desktop, SAP, Salesforce).
- *Controlled scalability* → assigned resources can be scaled horizontally or vertically to meet performance and operational needs.
- *Multi-platform support* (Web, Mobile, Mainframe, API, Enterprise systems).

4.7.3 Quality Code Analysis



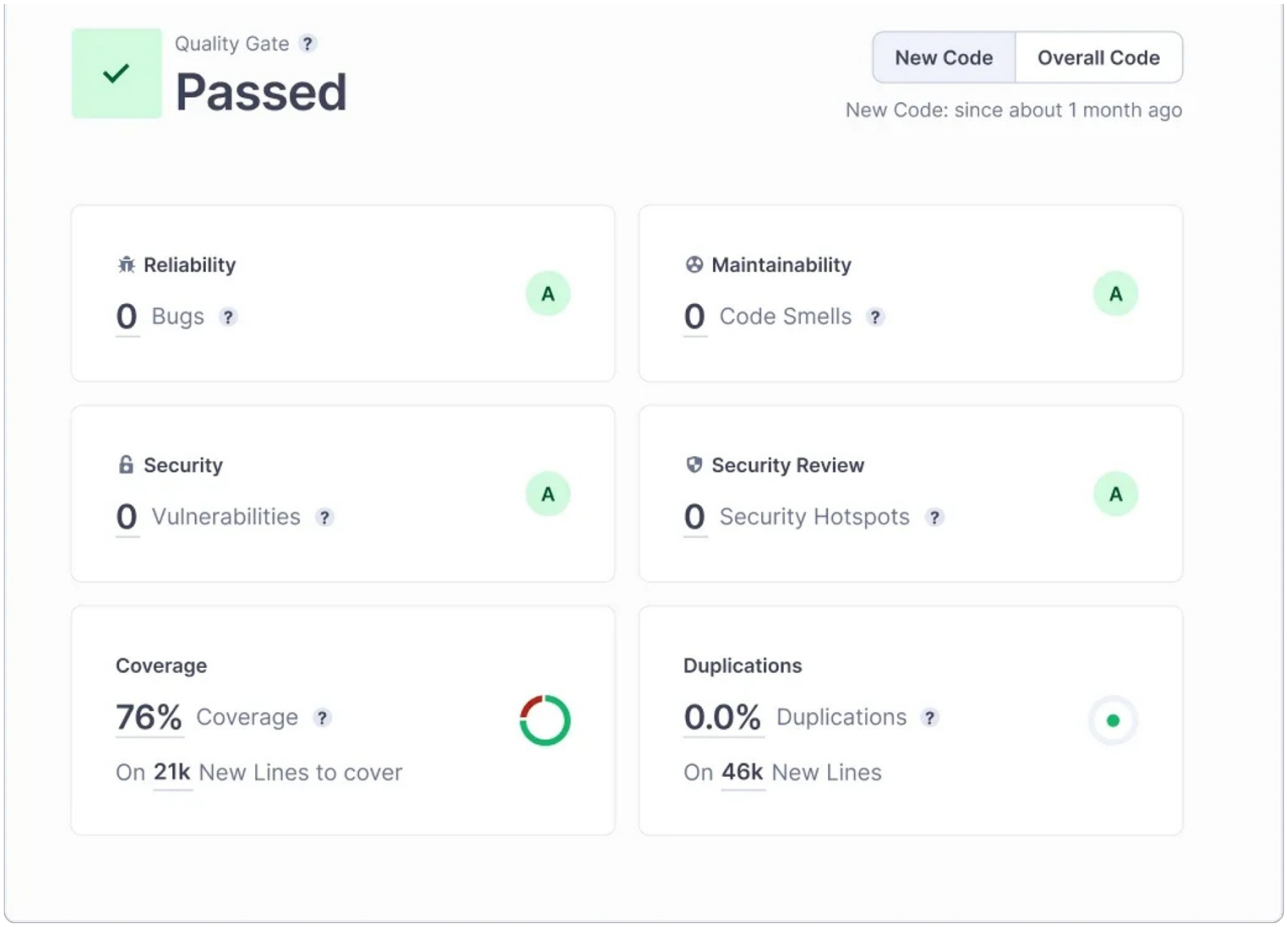


Figura 27 – Quality Code Analysis Service

4.7.3.1 Service Description

The service, based on SonarQube, offer a robust static code analysis tool, supporting software quality and integration into CI/CD processes.
Thanks to its architecture and ability to integrate into the continuous development and analysis cycle, it enables the development of high-quality software and fully supports DevSecOps initiatives. The service also enables in-depth source code security analysis, detecting known vulnerabilities, injections, poor cryptographic practices, uncontrolled access, and potential exploits.
Integrating directly into CI/CD pipelines or through supported DevOps platforms, it analyzes source code against a broad set of quality rules, covering aspects such as code maintainability, software reliability, and application security.

The service is offered per unit of line of codes. Each unit consists of 1 M lines of codes.

4.7.3.2 Features and Advantages

The service offers the following main features:

- *Static code analysis* → automatically scans source code with over 5,000 predefined or customizable rules. Supports over 30 languages.
- *Quality gates* → defines minimum quality thresholds (e.g., zero critical bugs, zero vulnerabilities, code coverage > 80%). If the code does not meet the criteria, the build is blocked, preventing the release of "dirty" software.
- *Bug and vulnerability Detection* → highlights issues that could cause runtime errors or security risks. Integration with OWASP Top 10, CWE, and SANS security rules.
- *Code smells & debt* → identify development practices that reduce readability or increase technical debt. Calculates an indicator of the time required to "clean up" the code.
- *Test coverage* → measures the percentage of code covered by unit tests. Helps identify critical untested areas.
- *DevOps integration* → can be integrated into CI/CD processes. Provides immediate feedback to developers throughout the development cycle
- *Reporting and dashboards* → interactive dashboards with KPIs on quality, security, and maintainability. Historical trends to monitor code quality evolution over time
- *Multi-branch & Pull request analysis* → analysis of specific branches and pull requests for immediate feedback before merging.

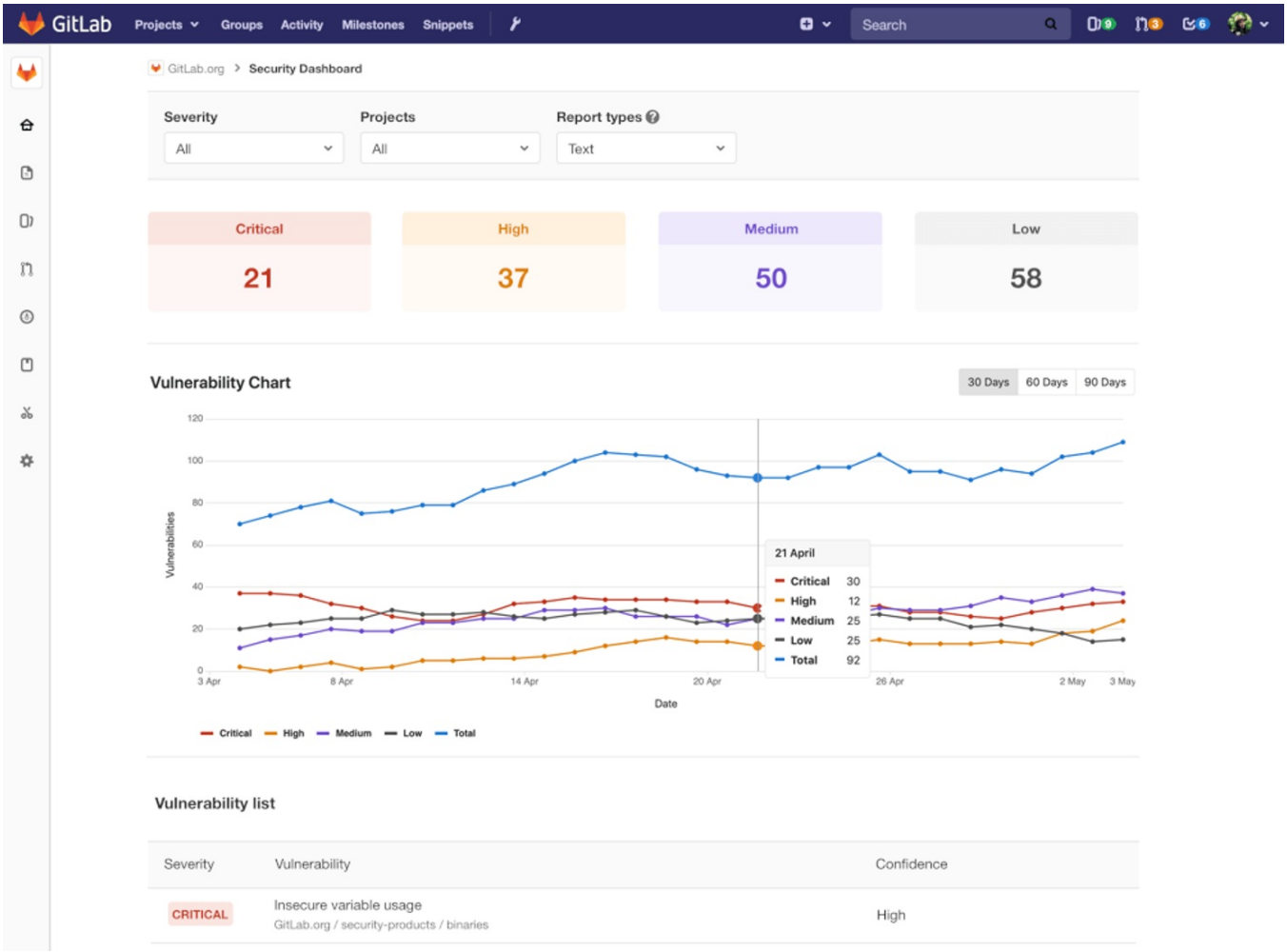
The main components of the service are:

- *SonarQube server* → core module of the service, responsible for running analyses, applying static verification rules, and centralized results management. It includes: analysis engine, quality gate engine, rule repository, user and permissions management, and RESTful APIs.
- *Database* → stores analysis results, active rules, and project history. Supports PostgreSQL, Oracle, SQL Server, and MySQL.
- *SonarScanner* → code analysis tool. It can be run locally by developers or integrated into CI/CD pipelines.
- *CI/CD Integration* → plugins and APIs available for Jenkins, Azure DevOps, GitLab CI, GitHub Actions, Bamboo, and TeamCity.
- *Security and Governance* → Authentication via LDAP, Active Directory, SAML, and OAuth. Granular roles (Admin, Project Admin, Developer, and Viewer).
- *Web portal* → browser-accessible user interface that allows developers, QA, team leaders, and analysts to view detailed project metrics and quality indicators, consult and manage Quality Gates, and view aggregated dashboards and reports at the project portfolio level. The portal is secure, multi-user, and configurable via granular roles and permissions.

The service offers the following advantages:

- *Lower risk of bugs in production and reduced maintenance costs* → more reliable and stable software, cleaner and more maintainable code.
- Compliance with security standards → regulatory and audit support.
- *Increased customer/stakeholder trust* → software perceived as more secure and robust.
- *Long-term Return On Investment (ROI)* → less time and resources spent on late fixes.
- *Increased team productivity* → less rework, more focus on new features.
- *Support for Agile and DevOps approaches* → the service enables the Clean as You Code approach and automates quality and security checks, reducing time to remediation thanks to immediate feedback to developers.
- *Improved software quality* → through the systematic application of quality rules, the service helps improve code maintainability and readability. Technical debt management → estimate the time to fix issues.

4.7.4 DevSecOps As A Service



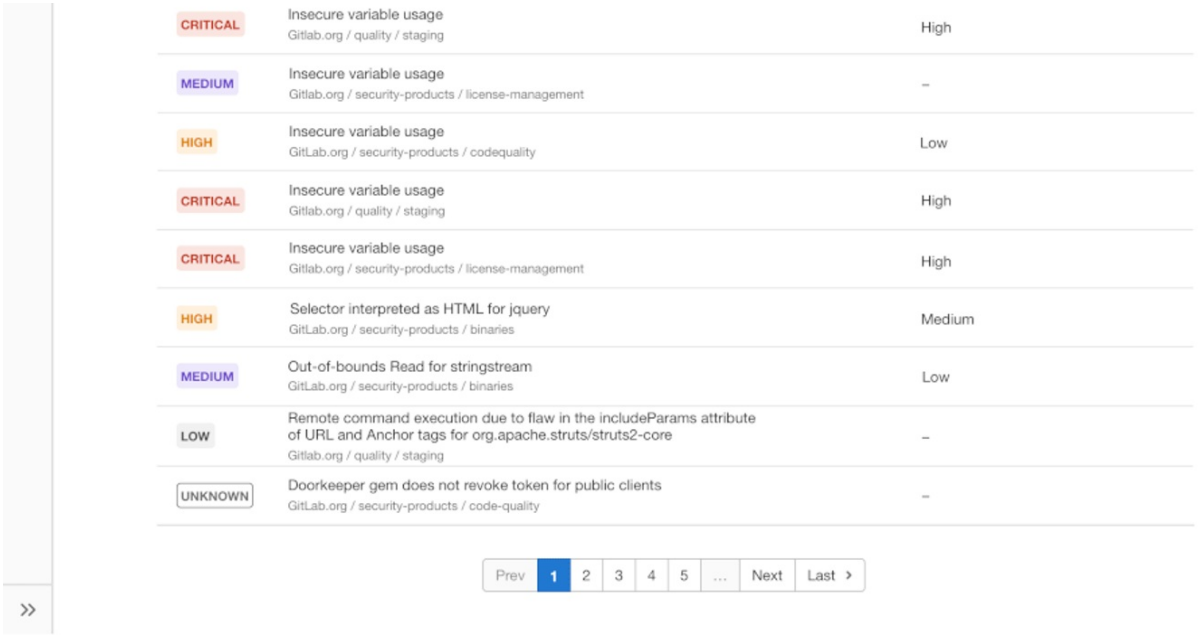


Figura 28 – DevSecOps As A Service

4.7.4.1 Service Description

The service, based on Gitlab, offers an integrated environment for the complete management of the software development lifecycle according to the DevSecOps approach and practices, providing the tools needed for collaboration, development, testing, security, and software release in a single integrated environment.
The service aims to support organizations in introducing application development, release, and management processes characterized by automation, security, and compliance, thus promoting the creation of reliable digital solutions aligned with required quality standards.
It allows you to manage projects and repositories, control source code versions, automate CI/CD pipelines, and collaborate efficiently with development teams.

The service is offered per user unit in the following options: 100 Users Ultimate/500 Users premium/2000 Free.

4.7.4.2 Features and Advantages

The service offers the following main features:

- *Git repositories* → represent the collection point for source code. They enable versioning, change tracking, and collaboration across multiple development teams.
- *CI/CD pipeline* → automation of build, test, and release phases. They reduce manual errors, speed delivery times, and ensure process repeatability.
- *Security Integration (DevSecOps)* → automatic scans of code (SAST), dependencies (SCA), container images,

and infrastructure configurations. Early identification of vulnerabilities and tracking of remediation directly within development workflows.

- *Artifact and Container Management* → centralized storage of build artifacts and container images. Support for secure and controlled deployment across the various phases of the environment (development, testing, production).
- *Monitoring and governance* → dashboards to view code quality, security, and project status. Role-based access controls and integration with identity management systems to ensure compliance and accountability.

The main components of the service are:

- *GitLab core platform* → this is the core of the platform and encompasses its main features: a web interface, API, database, and team collaboration tools.
- *Git repository* → a service dedicated to managing Git repositories. It handles code versioning and timely tracking of all changes.
- *CI/CD Engine GitLab Runner* → a service responsible for executing CI/CD jobs defined within pipelines, automating build, test, and deployment processes.
- *Artifact registry* → a module dedicated to managing and archiving artifacts generated during CI/CD pipelines, such as packages, container images, and libraries. It ensures traceability, security, and reuse of software components.
- *Test Management* → a component that supports the structured management of testing activities, enabling the planning, execution, and monitoring of test cases to ensure software quality throughout the development lifecycle.

The service offers the following advantages:

- *Reduced time to market* → thanks to automation and integrated pipelines.
- *Reduced operating costs* → a single platform instead of multiple separate tools.
- *Increased team productivity* → thanks to centralized collaboration.
- *High Return On Investment (ROI)* → reduced rework and post-release remediation.
- *Increased stakeholder trust* → more secure code and faster releases.
- *Native security integration* → integrated DevSecOps capabilities. Ensures compliance with corporate and regulatory policies.
- *Integrate project management with native tools* (issue boards, milestones, etc.).
- *Centralize source code and CI/CD pipeline management*.
- *Foster collaboration between technical and project teams*.
- *Increase team productivity* through process automation.

4.7.5 Qualizer DevSecOps

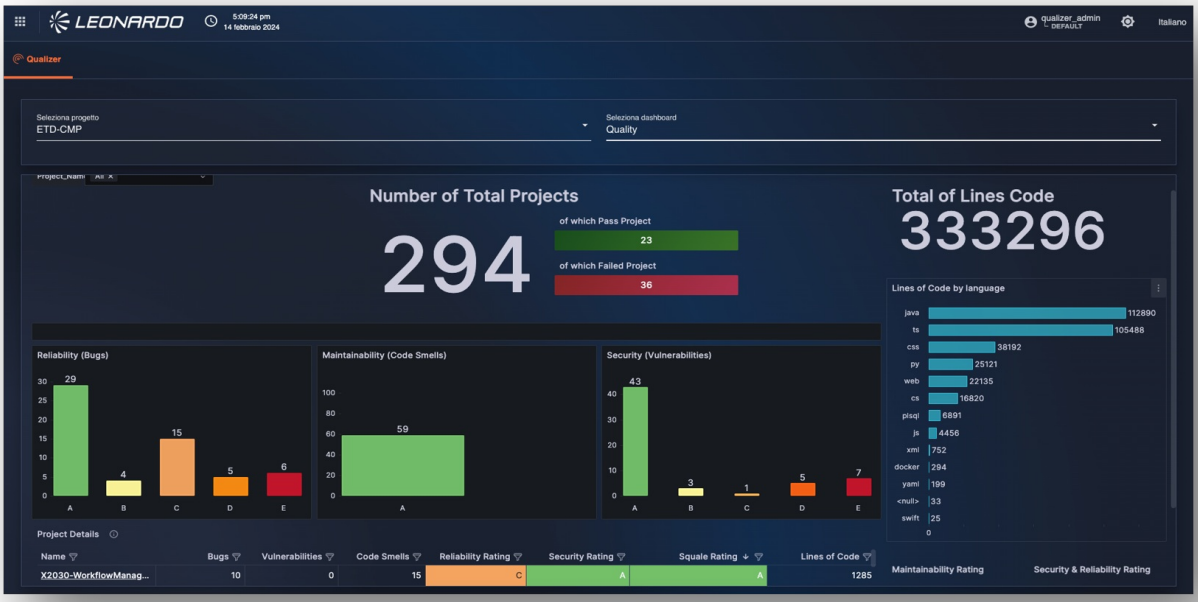


Figura 29 – Qualizer DevSecOps Service

4.7.5.1 Service Description

The Leonardo's Qualizer service is a platform designed to meet the needs for visibility, control, and continuous improvement of the software lifecycle throughout the development cycle, in accordance with the DevSecOps and Agile approach.
It offers a centralized tool for analyzing, observability, and governance of software quality.
The service allows you to aggregate data from various sources, security, monitoring, and testing tools, integrating them into a user dashboard (portal) that clearly and graphically displays various interactive metrics and insights.

The service is sized and offered per project unit. Each unit consists of 10 projects.

4.7.5.2 Features and Advantages

The service offers the following main features:

- *Ingestion* → automatically collects data from the main tools used in development processes, such as code management systems, continuous integration tools, and software quality and security analysis. The collected data is processed and made available for consultation and analysis.
- *Data processing* → processes the data collected by the ingestion module, normalizes it, and extracts key metrics. The data is structured and made highly accessible via dashboards.
- *Project management* → this module allows you to configure and organize projects within the service. It allows organizations to specify which products, pipelines, and tools they wish to monitor and associate useful information for navigation and management with each project.
- *Analytics engine* → the service provides summary and analytical views that aggregate the collected information and present it clearly and understandably (e.g., DevOps performance metrics; code security status; code quality; number of tests performed; percentage of tests passed).
- *Presentation layer* → data is made available through dashboards that allow for the analysis and continuous monitoring of key metrics.

The Qualizer service is cloud-native and based on a containerized microservices system. This architecture allows Qualizer to be flexible, resilient and secure, with the ability to adapt to different technological scenarios.
At a logical level, the architecture is divided into the following main components:

- *Core modules* → each service module (e.g., ingestion, project management, data processing) is implemented as an independent microservice, orchestrated in a Kubernetes/OpenShift environment to ensure high availability and functional isolation.
- *Database for storing collected data* → data acquired from external systems is stored in a centralized database, which is then processed and normalized to support efficient metrics processing, interactive consultation, and dashboard generation.

- *Integration via REST API* → the service interacts with external platforms through standard APIs, enabling continuous data collection.
- *Messaging broker* → the service uses a Kafka-based messaging system to ensure decoupling between modules, support high event loads, and facilitate horizontal scalability.

The service offers the following advantages:

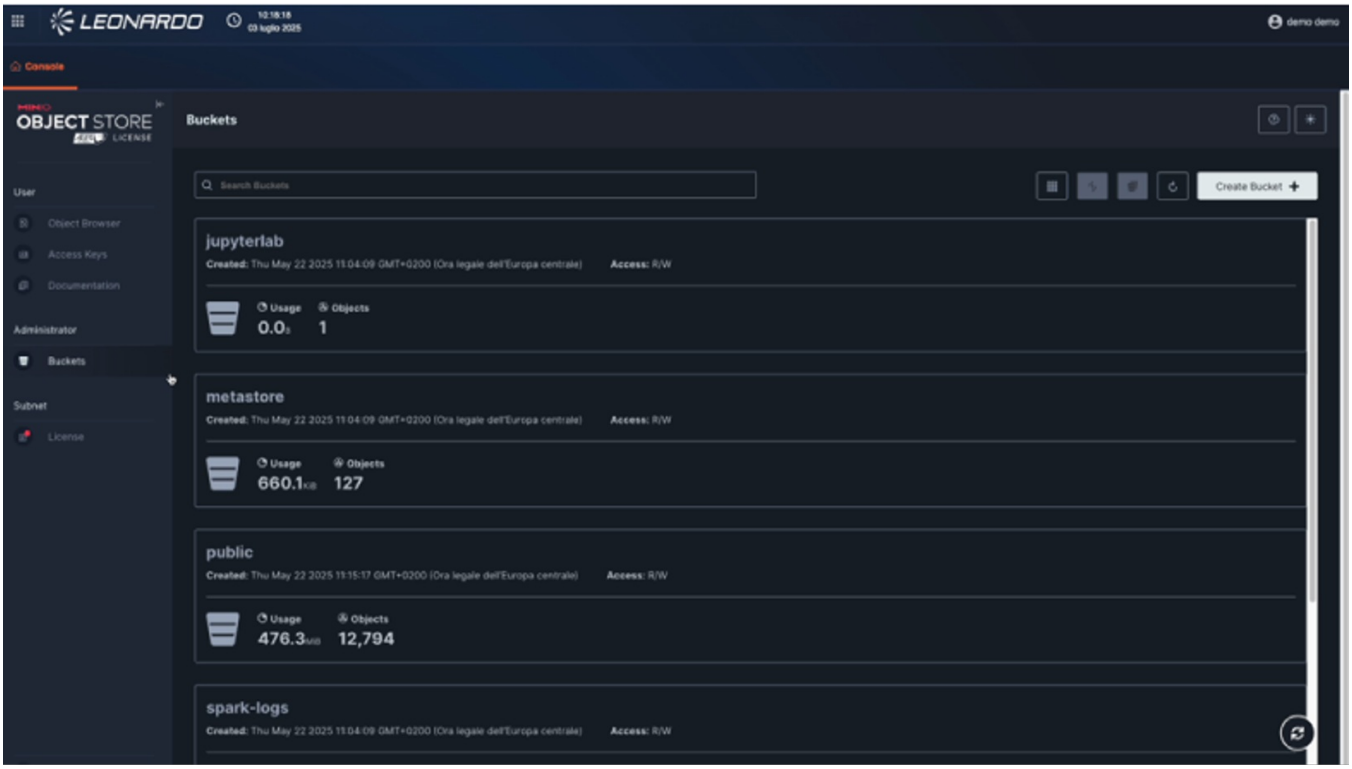
- *Reduced time to market* → thanks to automation and integrated pipelines.
- *Reduced operating costs* → a single platform instead of multiple separate tools.
- *Increased team productivity* → thanks to collaboration between developers and security specialists, aligning objectives and timelines.
- *High Return On Investment (ROI)* → reduced rework and post-release remediation.
- *Increased stakeholder trust* → more secure code and faster releases.
- *Centralized security management* → vulnerabilities detected by various scanning tools are collected, normalized, and tracked in a single location, facilitating the work of security teams and reducing the risk of omissions.
- *Reduced remediation time* → thanks to immediate visibility of vulnerabilities, Qualizer accelerates the process of taking charge and resolving issues. - *Continuous improvement based on collected metrics* → through standardized dashboards and indicators, the service allows you to objectively measure team and project performance.
- *Unified dashboard* for quality, security, and deployment monitoring.

4.8 Big Data Family

Below is the list of services belonging to the Big Data family:

- Data Lake
- Business Intelligence
- Batch/Real time Processing
- Event Message
- Data Governance

4.8.1 Data Lake



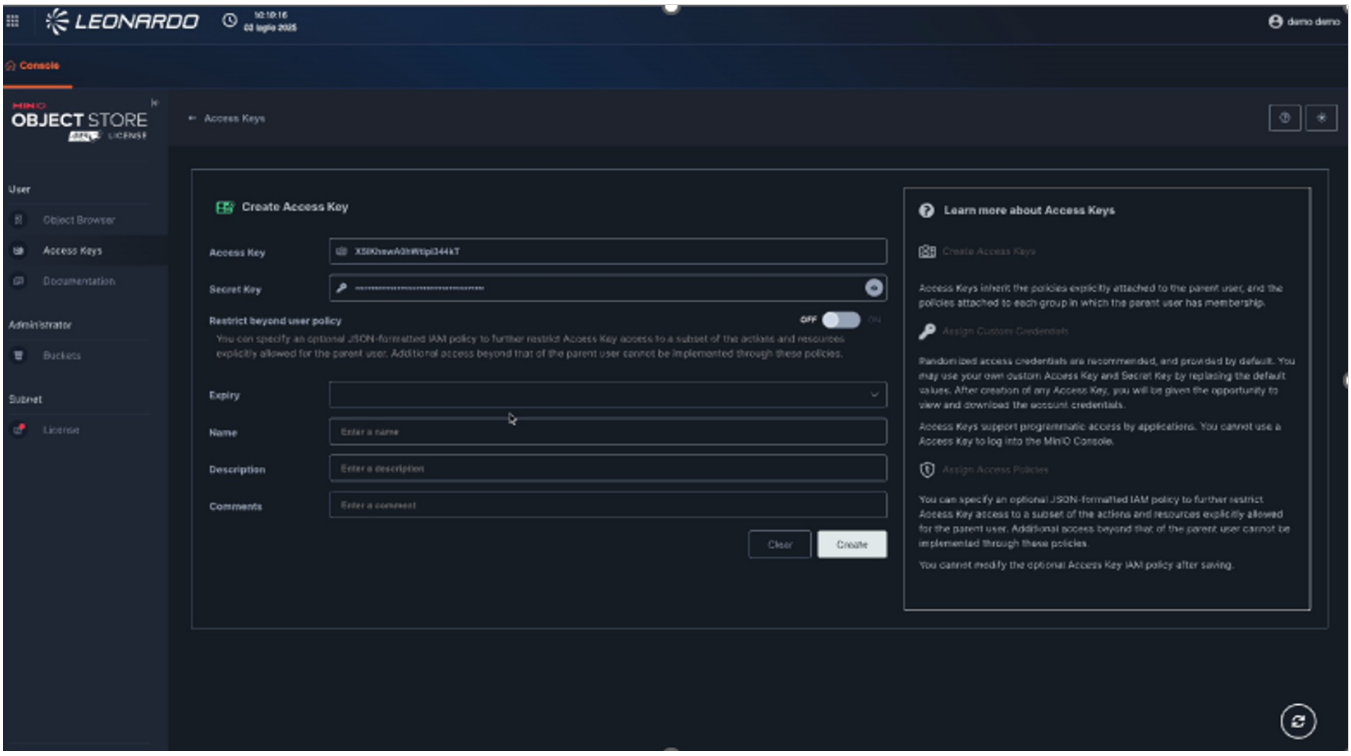


Figura 30 – Data Lake Service

4.8.1.1 Service Description

Developed by Leonardo, it provides a ready-to-use platform that has all the features developers, data scientists, and analysts need to easily archive data of all sizes, shapes, and velocities.
It allows for the ingestion of a wide range of heterogeneous data sources (structured, semi-structured, and unstructured), from various internal and external sources within the organizations (relational databases, files, web applications, cloud, web services, etc.), and of various classification types.
It integrates with the Processing/ETL module for accessing data and metadata for the necessary processing or normalization, and with the Data Governance module for managing data access and managing data security and protection.

The service is sized and offered per storage unit. Each unit contains 1 TB.

4.8.1.2 Features and Advantages

Data Lake is the foundation for all Big Data services; without it, other services cannot be activated.
It was designed based on, and with full wire-protocol compatibility with, Amazon's renowned cloud storage product (Simple Storage Service). This enables the scalability needed to manage data volumes in the petabyte range (and beyond) typical of the Big Data world, while ensuring maximum interoperability and compatibility with languages, libraries, and products compatible with the S3 protocol.
Data Lake's capabilities are based on a horizontally scalable infrastructure, capable of supporting heavy read and write loads, ensuring consistent performance even in scenarios characterized by large amounts of data and intensive throughput.

The development technology is based on MinIO, an object storage solution fully compatible with the S3 protocol.
The application layer is built on distributed object storage, which in turn relies on an underlying block storage layer, which can be implemented either bare metal or using software-defined solutions.
The overall architecture is based on containers orchestrated by a resource manager based on an enterprise-class Kubernetes distribution.

The service offers the following advantages:

- *Compliance and governance* → supports versioning, auditing, encryption (AES-256), and integration with identity management systems.
- *Flexibility and scalability* → supports horizontal scalability; ideal for companies with rapidly growing data or multi-petabyte storage needs.
- *Rapid time to market* → allows you to quickly deploy new analytical applications or data pipelines without worrying about underlying management.
- *Simplified management* → teams don't need to worry about technical maintenance. There's no need to configure clusters, load balancers, manual replication, or complex monitoring; it offers native monitoring and alerting tools.

- *Reduced operating costs* → the service is built with open source standards and compatible with S3, thus reducing licensing costs compared to proprietary solutions.
- *High availability and resilience* → integrated replication and support for erasure coding ensure data resilience and business continuity.
- *Optimized performance* → designed for high-performance object storage, with high throughput and low latency. Ideal for real-time analytics and intensive ML/AI workloads.
- *Interoperability* → S3 API compatibility allows for easy integration of existing applications. Supports multi-protocol access.
- *Automation and DevOps-friendly* → it enables continuous updates without downtime and simplified backup management.

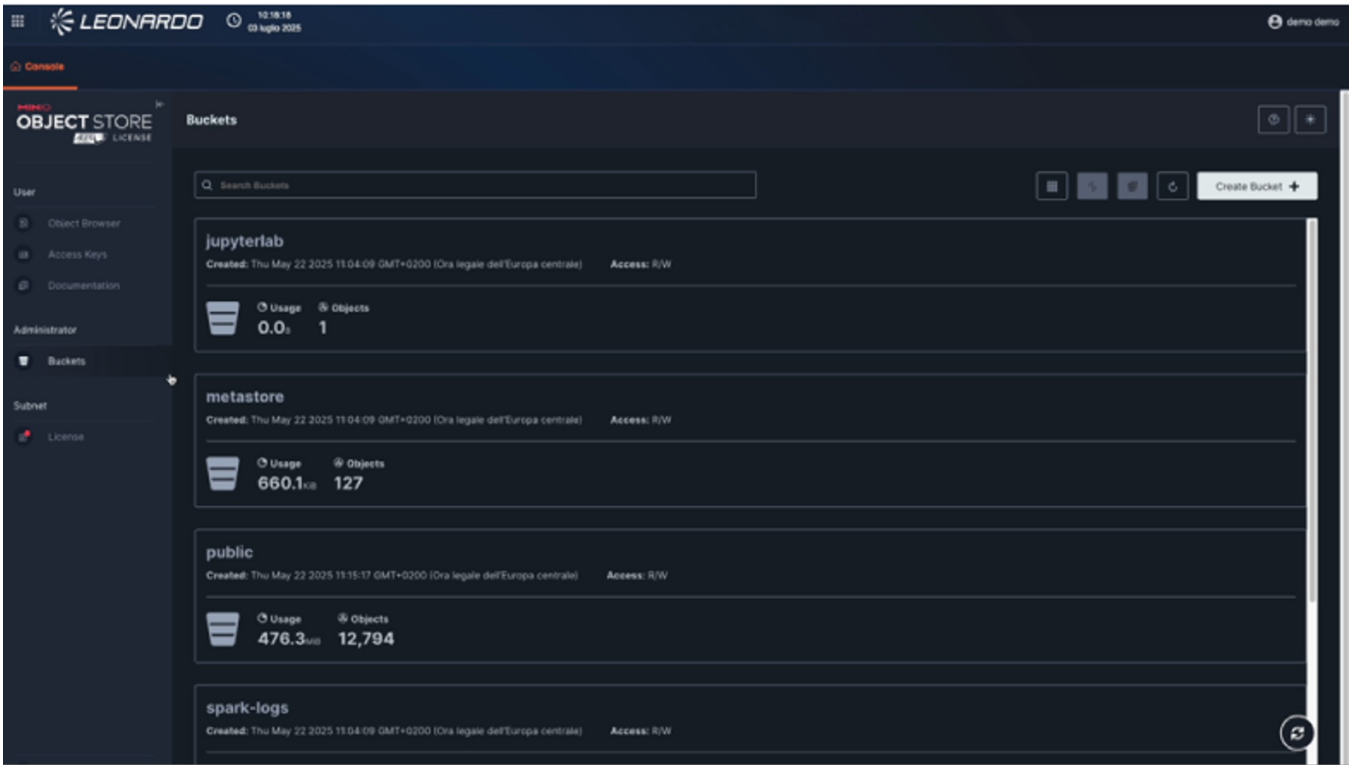
4.8.1.3 Disaster Recovery (DR) architecture

Data replication within MinIO Object Storage is managed directly at the application level.
The solution provides Site Replication capabilities that enable native management of data distributed across multiple Data Centers (DCs), synchronizing buckets, objects, access policies, and encryption configurations.
Typically, data availability and resilience in distributed object storage systems is achieved through deployment across multiple physical locations. In this architecture, MinIO clusters are deployed in geographically separate data centers to provide disaster recovery capabilities. Replication between MinIO sites can be configured:

- as synchronous inside the same Region for HA configuration.
- as asynchronous beetween different Regions for DR configuration.

In this deployment, thanks to the high bandwidth and low latency connections available between data centers, synchronous Site Replication was adopted between clusters, ensuring data consistency across locations.
Access to the different clusters can be achieved either via direct addressing or through a load balancer, depending on architectural and operational needs.From an internal management perspective, MinIO automatically organizes storage units into erasure sets, which are logical groups that form the foundation of system availability and resilience. To ensure uniform distribution, MinIO applies a striping mechanism for erasure sets across the various nodes in the pool, avoiding load concentrations or single points of failure. Objects are then divided into data blocks and parity blocks, which are distributed within the erasure sets, ensuring redundancy, fault tolerance, and operational continuity.

4.8.2 Data Lake-Cold



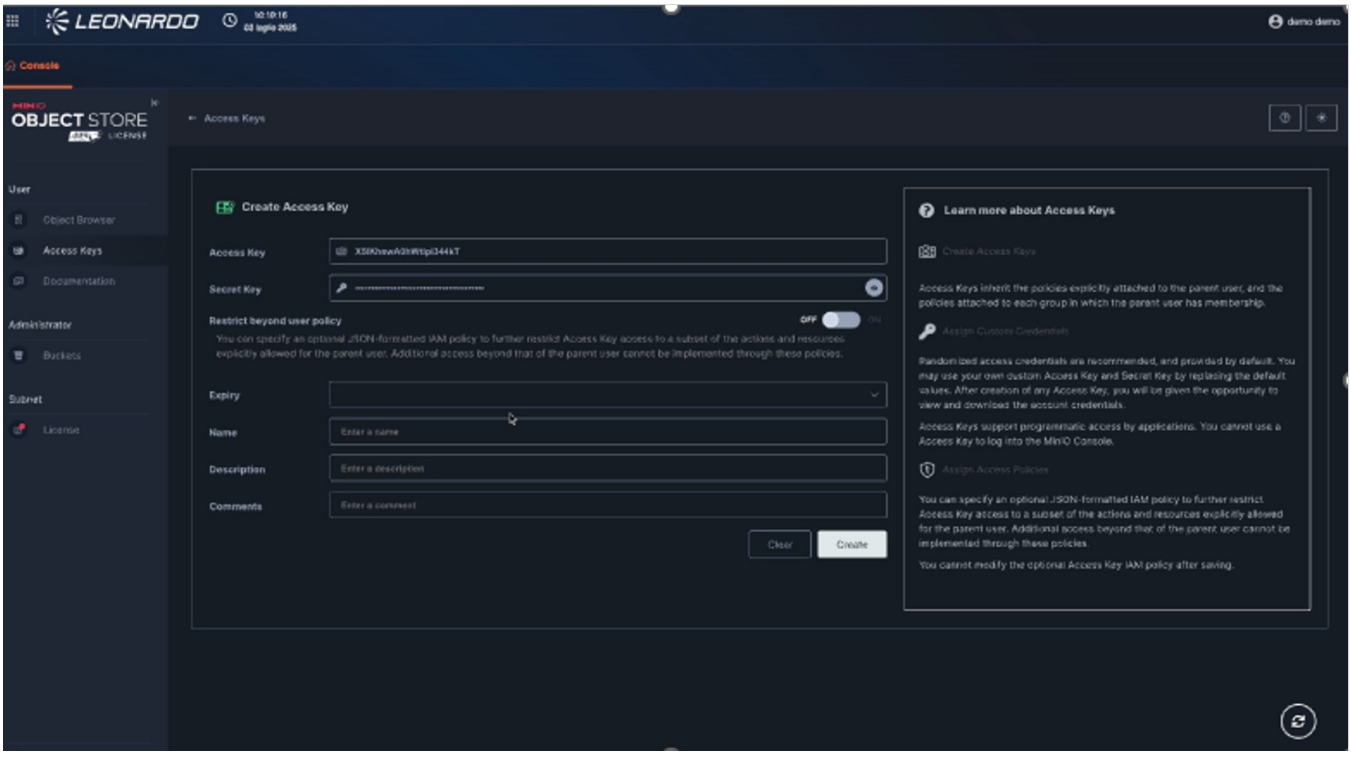


Figura 31 – Data Lake Service

4.8.2.1 Service Description

This is the same technology and architectural solution as the previous Data Lake service, adapted for cold storage scenarios, i.e., data that is rarely used and accessed slowly.

This implies the following features:

- Much less frequent data access
- Slower data recovery times
- Lower storage costs
- Used for historical data, old logs, and long-term backups

4.8.2.2 Features and Advantages

For features, components, and benefits, see the full service offering Data Lake.

4.8.3 Business Intelligence

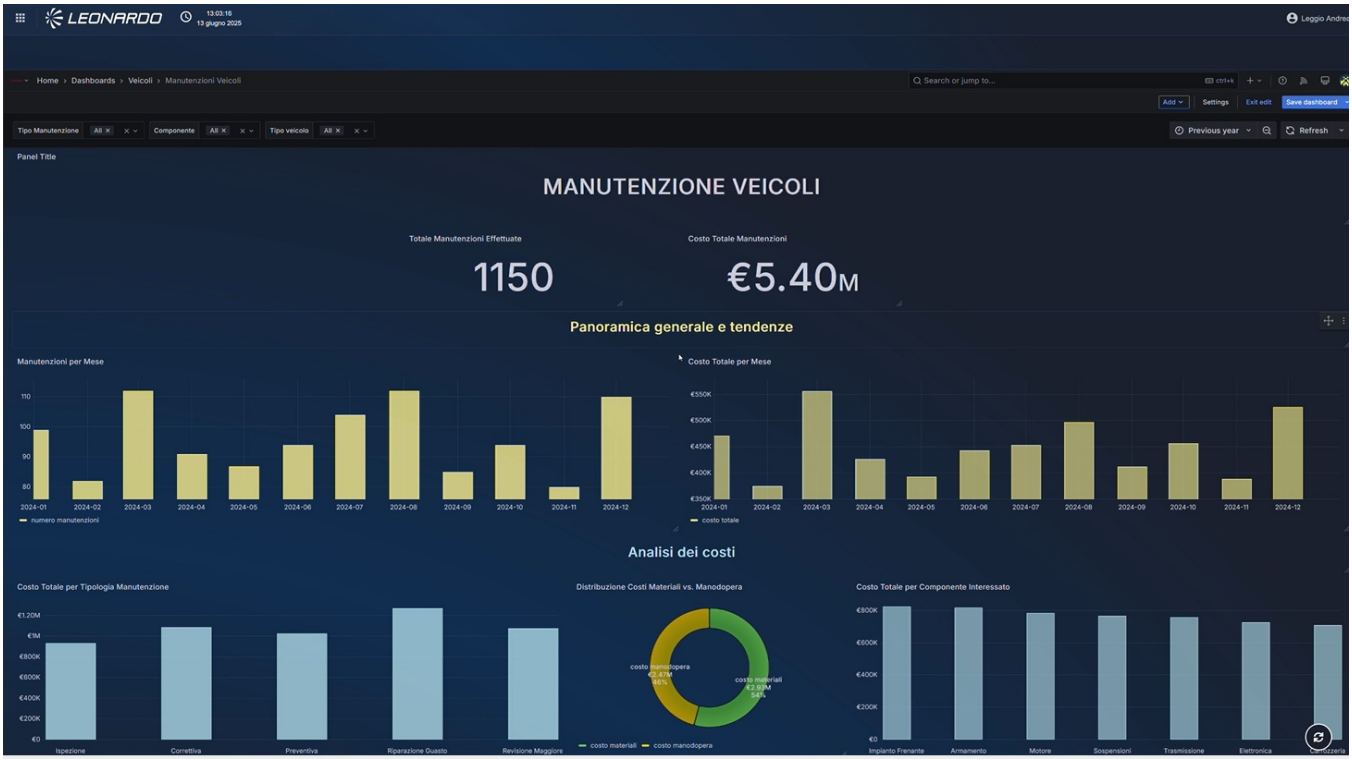


Figura 32 – Business Intelligence Service

4.8.3.1 Service Description

Developed by Leonardo with Grafana technology, the Business Intelligence Service is a platform with an analytics environment designed to provide real-time, interactive data visualization and monitoring capabilities.
It centralizes data ingestion, transformation, storage, and dashboarding within a scalable service that eliminates the need for organizations to maintain on-premises analytics infrastructure.
Built on the Grafana visualization engine, the platform empowers users to explore metrics, logs, and business KPIs through intuitive dashboards while integrating seamlessly with diverse data sources across cloud and hybrid ecosystems.

The service is sized and offered per user unit. Each unit consists of 100 users.

4.8.3.2 Features and Advantages

The service offers the following main features:

- *Unified Data Visualization* – Provides dynamic, customizable dashboards that consolidate operational, financial, and business performance data from multiple sources.
- *Multi-source Connectors* – Supports native integration with SQL databases, time-series platforms, cloud storage, IoT systems, and third-party analytics services.
- *Real-time Monitoring* – Enables continuous tracking of business and operational metrics with live updates, alert rules, and automated notifications.
- *Role-based Access Control (RBAC)* – Ensures secure, granular access to dashboards, data, and administrative functions based on user roles and permissions. Advanced Querying and Exploration – Offers powerful query capabilities, including support for SQL, PromQL, InfluxQL, and other engine-specific languages.
- *Alerts and Anomaly Detection* – Provides rule-based alerts, thresholds, and pattern detection to identify anomalies or performance issues across business workflows.
- *White-labeling and Custom Branding* – Allows organizations to apply their own visual identity to dashboards, reports, and portal interfaces.
- *API and Automation Support* – Facilitates integration with third-party systems through APIs, webhooks, and automation workflows.

The main components of the service are:

- *Visualization Layer* – The dashboard engine that renders interactive charts, tables, alerts, and analytics views.
- *Data Source Integration Layer* – Connectors and plugins enabling ingestion from databases, cloud platforms, streaming services, logs, and monitoring tools.
- Data Processing Pipeline – Optional ETL/ELT engines for cleaning, transforming, and aggregating raw data prior to visualization.

- *Time-Series and Analytical Storage* – Managed storage solutions (e.g., Prometheus, Loki, InfluxDB, Elasticsearch, SQL warehouses) optimized for real-time queries.
- *User and Access Management* – Centralized identity integration with SSO, LDAP, OAuth2, or corporate IAM platforms
- *Alerting and Notification Engine* – Framework that triggers alerts via email, Slack, Teams, PagerDuty, or SMS based on metric conditions.
- *Management and Administration Console* – Web interface for configuring data sources, managing tenants, provisioning resources, and monitoring platform health.
- *API Gateway* – Provides programmatic access for provisioning dashboards, exporting data, managing alerts, and embedding visuals.

The service offers the following advantages:

- *Faster and better decisions* → real-time or near-real-time access to data, intuitive visualizations, and drill-down into information, enabling more informed decisions.
- *Increased productivity and speed of insight* → automated creation/reporting, self-service dashboards, and easy sharing enable business users to act faster.
- *Reduced total cost of ownership (TCO) and lower costs* → managed infrastructure and reduced need for on-premise infrastructure reduce overall costs.
- *Increased collaboration and a data-driven culture* → dashboard sharing, integration with other tools, and ease of use promote adoption among non-technical users.
- *Access anywhere and from different devices* → availability via cloud, mobile apps, and remote access allows users to work on the move or from different locations.
- *Extensive data integration* → support for numerous connectors to on-premise and cloud sources, enabling consolidation of disparate data.
- *Efficient data preparation and modeling* → integrated tools enable ETL, modeling, and complex calculations.
- *Interactive and self-service visualization* → intuitive, drag-and-drop interface and pre-built templates allow non-technical users to build reports independently.
- *Security, governance, and compliance* → Features such as encryption and auditing support access control and compliance. Infrastructure scalability and flexibility.

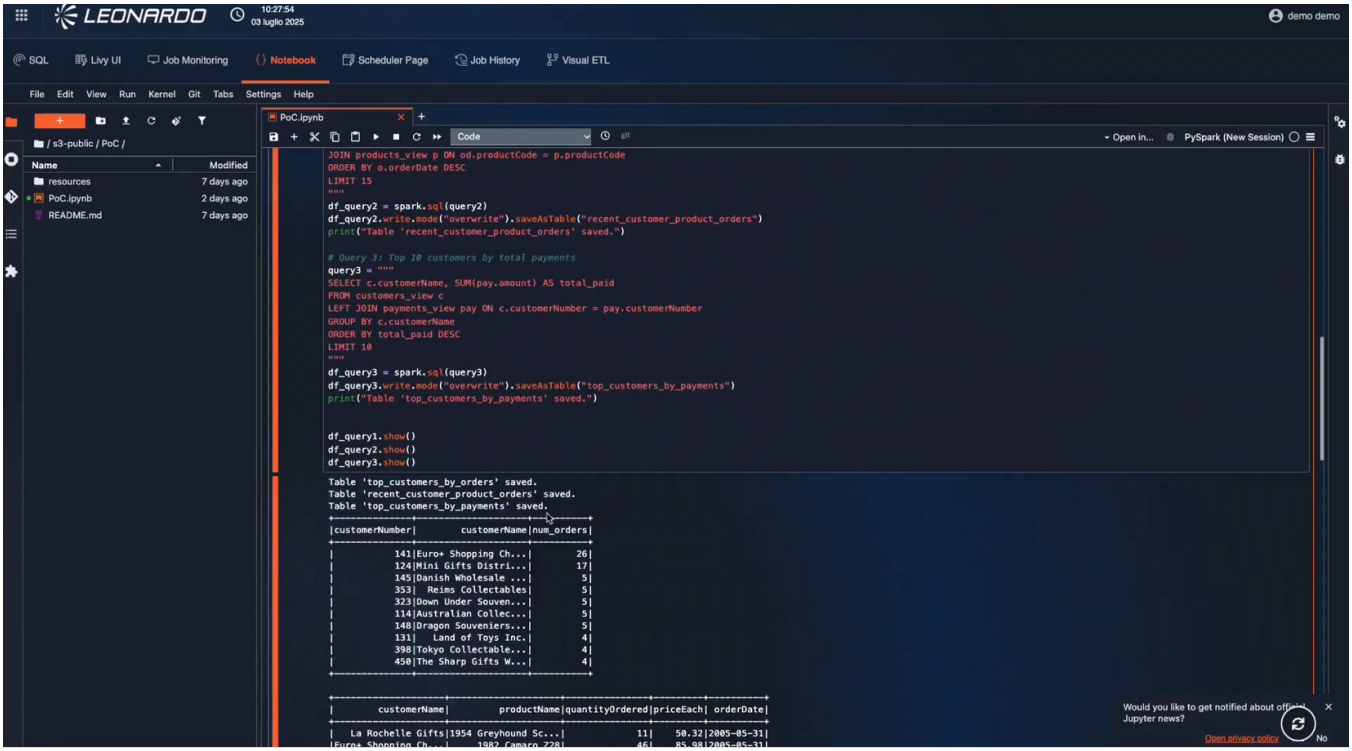
4.8.4 PaaS ETL - Batch/Real time Processing

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform



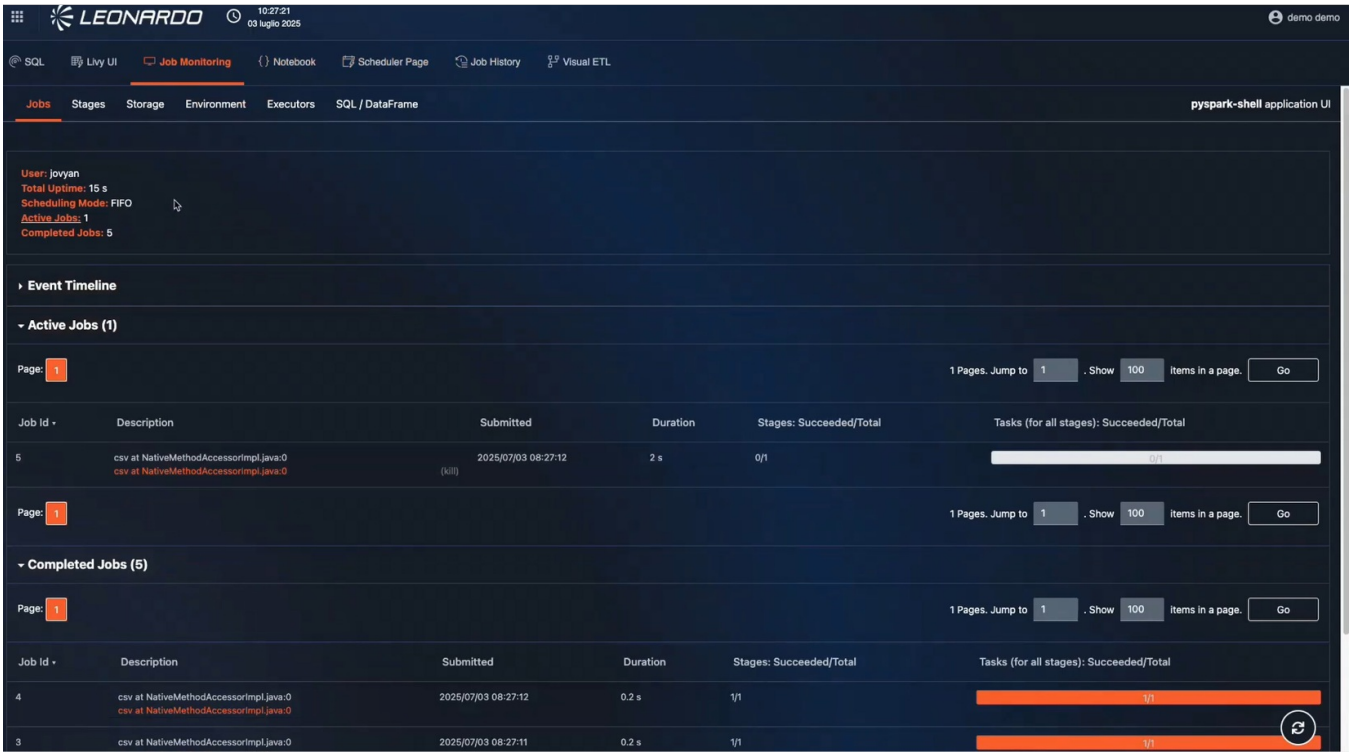


Figura 33 – PaaS ETL - Batch/Real

time Processing

4.8.4.1 Service Description

It is a platform that provides a set of tools for processing, integrating, quality-checking, and preparing data from heterogeneous sources stored in the Data Lake, both in real time and in batch mode.
It offers a user-friendly graphical interface for designing and implementing data integration workflows using a visual approach, following the ETL (Extract – Transform – Load) approach. This reduces the complexity of data integration and allows users to focus on business logic rather than programming code.
It supports a wide range of data sources, including relational databases, files, web applications, cloud, web services, and more. This makes it extremely flexible for data integration in a variety of contexts.
It also offers data quality management tools, allowing users to clean, standardize, and enrich their data to ensure its accuracy and reliability.

The service is sized and offered per worker node. Each worker consists of:

- 16vCPU
- 128 GB of RAM

4.8.4.2 Features and Advantages

The main features and functionalities of the service are:

- *Heterogeneous and large-scale data processing* → It supports a large number of data sources in batch and streaming mode (for example, datasets stored on HDFS, S3, ADLS Gen2, and GCS in CSV, Parquet, Avro, and other formats, as well as RDBMS via JDBC or all popular NoSQL, Apache Kafka, and more).
- *It is natively integrated* with the Data Lake and Batch/Real-Time Processing PaaS of the Big Data family.
- *It allows to implement complex data pipelines* → leveraging the parallel and distributed computing capacity provided by a Spark cluster.
- *It provides an interactive mode* to debug flows and explore data easily and intuitively.
- *It guarantees the maximum scalability* necessary to meet the needs of organizations of any size, from small businesses to large enterprises.

The main architectural components of the service are as follows:

- *Visual ETL Architecture* → provides various blocks that allow you to visually design an ETL, ELT, and ELL pipeline. It allows you to read, write, and modify data from different sources, interfacing with the Data Lake and Monitoring module, and can use the Processing module for data-intensive processing.
- *Apache Spark* → Open-source parallel processing framework that supports in-memory processing to improve the performance of applications that analyze Big Data.

- *JupyterLab* → Interactive notebook-based development environment designed primarily for working with data, scientific calculations, and machine learning. It supports writing and executing interactive code in languages such as Python, R, or Julia.
- *NodeRed* → Visual, low-code development environment for creating applications that connect devices, web services, APIs, and systems.

The service offers the following advantages:

- *Support for data-driven strategies, faster and more informed decisions* → centralized data for service customization (e.g., real-time analytics for marketing, IoT, e-commerce, etc.) and ready-to-use pipelines without complex development.
- *Greater focus on core business* → development and IT teams do not have to worry about technical maintenance, as it is managed. - *Reduced operating costs and service scalability* → no infrastructure to manage; support for large data volumes (batch) or continuous flows (streaming); automation of extraction, transformation, and loading processes with real-time scheduling or triggers; same framework for historical data and real-time flows.
- *Integration with cloud ecosystem* (data warehouse, data lake, BI, AI/ML).
- *Guaranteed security and compliance* (encryption, access, audit logs).
- *Integrated monitoring* → metrics, alerts, and centralized logging for ETL pipelines.

4.8.5 Event Message

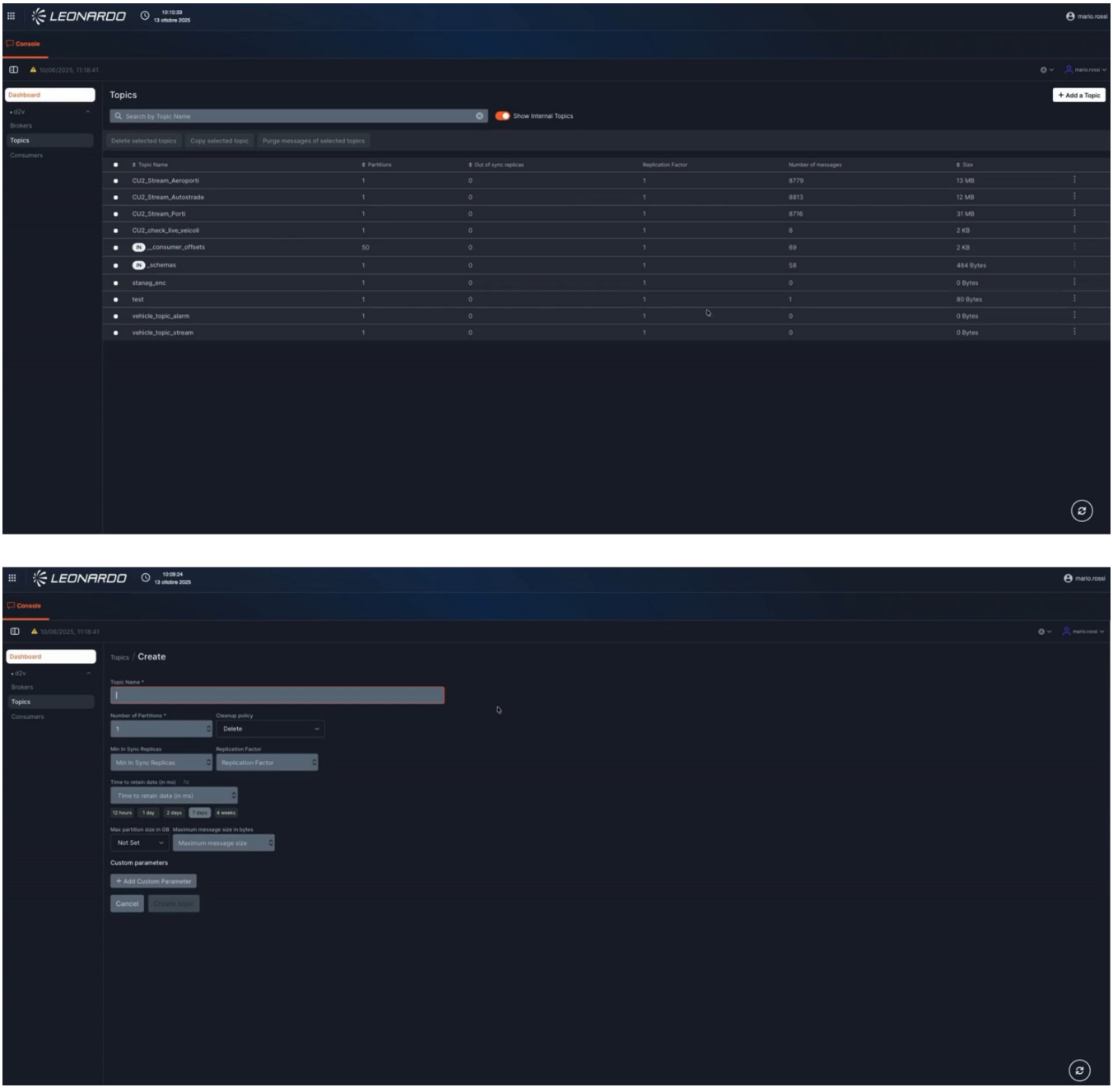


Figura 34 – Event Message Service

4.8.5.1 Service Description

It provides a platform developed by Leonardo for developing real-time applications and data pipelines and acts as a message broker, providing publish-subscribe functionality.
It increases the scalability and resilience of existing applications by decoupling architectural components using a reactive approach based on asynchronous interactions.
The platform can scale horizontally and provide ordered message delivery capabilities. Like other Big Data PaaS modules, the solution is based on containerized resources orchestrated via Kubernetes.
It enables near-real-time analytical processes through streaming and facilitates the implementation of IoT use cases.

The service is sized and offered per worker node. Each worker consists of: - 16 vCPU - 128 GB of RAM

4.8.5.2 Features and Advantages

The service offers the following main features:

- A useful tool for implementing reliable data exchanges between different components.
- Ability to partition messaging workloads as application requirements change.
- Real-time streaming for data processing.
- Native support for data/message playback.
- Integration with the Batch/Stream Processing module.
- Web interface for monitoring: Brokers Topics/Messages, Consumers, ACLs.

The main components of the service are:

- *Apache Kafka-based solution* → publish-subscribe messaging platform built to manage real-time data exchange for streaming, distributed pipelining, and replay of data feeds for fast, scalable operations.
- *Broker-based solution* that operates by maintaining data streams as records within a cluster of servers.
- *Topic* → addressable abstraction used to show interest in a given data stream (series of records/messages).
- *Partitions* → topics can be divided into a series of order queues called partitions.
- *Persistence* → server clusters that durably maintain records/messages as they are published.
- *Producers* → defines which topic/partition a given record/message should be published to.
- *Consumers* → entities that process records/messages.

The service offers the following advantages:

- *Faster time-to-market* → New applications can be integrated rapidly via events, accelerating the development of new products and features.
- *Greater agility* → Facilitates the creation of modular and scalable services without major changes to the existing system.

- *Reduced risk of operational failures* → PaaS often includes SLAs, monitoring, backup, and redundancy, reducing the risk of downtime or data loss.
- *Faster, more informed decisions* → Real-time analytics for marketing, IoT, and e-commerce.
- *Predictable costs* → Reduces the risk of over-provisioning or unexpected maintenance costs.
- *Scalability* → Support for large event volumes without performance degradation
- *High availability and fault tolerance*
- *Simplified management* → No need to manage clusters, patches, software upgrades, or complex configurations
- *Optimized Performance and Latency* → Compression, batching, and automatic topic management improve performance
- *Security and Compliance* → Authentication, authorization, and encryption in transit and at rest are managed by the provider.

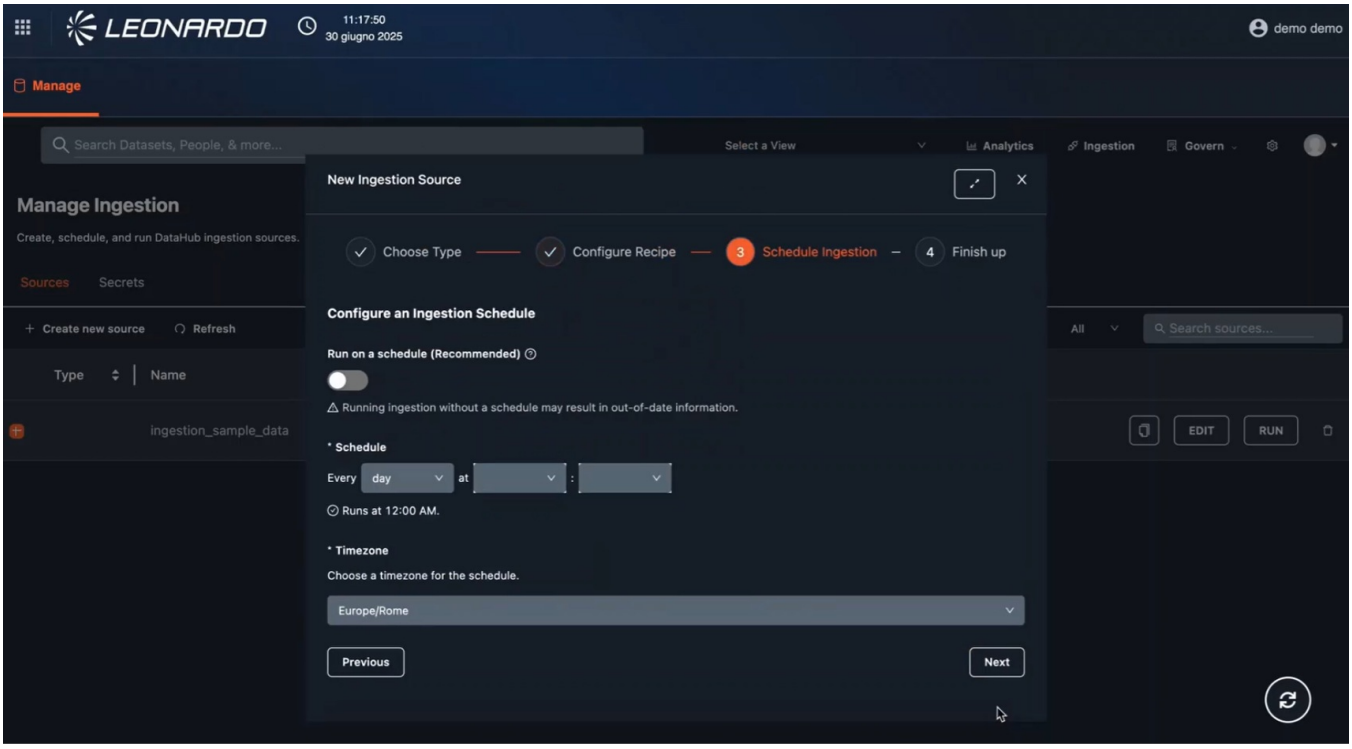
4.8.6 Data Governance

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform



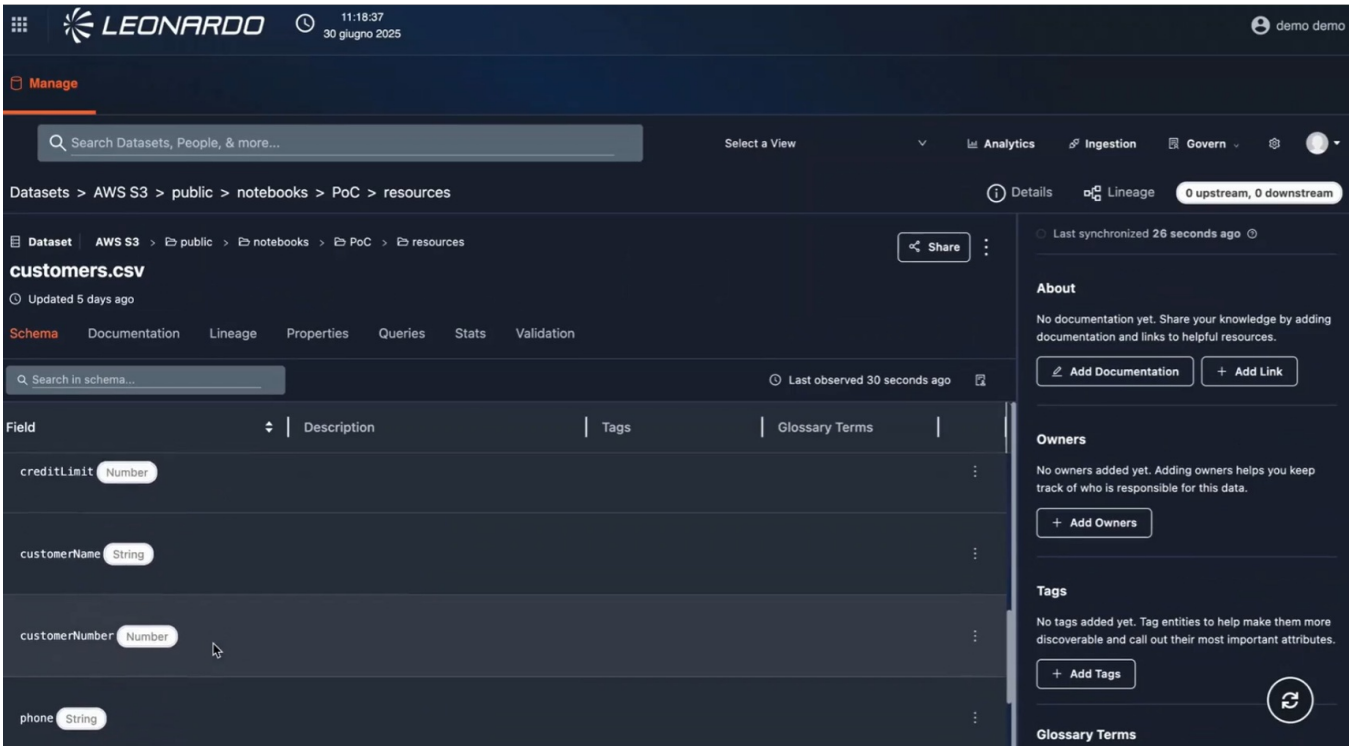


Figura 35 – Data Governance Service

4.8.6.1 Service Description

A service developed by Leonardo that provides a platform with a single, secure, and centralized point of reference for data control. Leveraging search and discovery tools and connectors to extract metadata from any data source, it simplifies data protection, analysis, and pipeline management, as well as accelerating ETL processes.
It allows you to automatically analyze, profile, organize, link, and enrich all metadata, implement algorithms for automatic metadata and relationship extraction, and support regulatory and data privacy compliance with intelligent data lineage tracking and compliance monitoring.
It simplifies data search and access and verifies its validity before sharing it with other users.
It enables the production of data quality data (a measure of data condition based on factors such as accuracy, completeness, consistency, and reliability).
It allows you to oversee data error resolution efforts and maintain compliance with internal audits and external regulations.
It provides immediate support for the detection and classification of personal data and other sensitive data.

The service is sized and offered each 10 users.

4.8.6.2 Features and Advantages

The service offers the following main features:

- *Data Search & Discovery* → Automatic exploration of Data Lake datasets for (meta)data that can enrich or deepen knowledge of the information held.
- *Data & Metadata Catalog* → Extraction of information that makes the data searchable.
- *Data Lineage* → Tracking the entire data lifecycle, from source to destination.
- *CL/Audit* → Allows for robust granular data access permission management and auditing of data usage (this means being able to answer the question "Who accessed what data and when?" at any time).

The service use a tool of Data Hub that extends the concept of a data catalog by offering data discovery, data observability, and data governance functions.
It integrates natively with other architecture components, adding all the features that are particularly useful for achieving compliance objectives, such as privacy, security, and process quality management.
This tool allows you to verify changes made to data within the catalog over time, distinguishing the various sources that have populated the Data Lake, the type of data entered (personal data, financial data, etc.), and identifying data that is sensitive to specific laws or compliance procedures, whether internal or external to the organization. Data integration within DataHub occurs primarily in two ways: - PUSH → automatically within third-party applications such as Airflow, Apache Spark, Great Expectations, etc. - PULL → manually by the developer prior to loading the data into the data lake via dedicated REST APIs.

The service offers the following advantages:

- *Improved governance and compliance* → Complete data traceability ("data lineage") to demonstrate compliance with GDPR, ISO, or industry regulations.
- *Increased data trust* → Certainty about the data's provenance, how it has been transformed, and how up-to-date it is.
- *Reduced risks and operational costs* → Fewer duplications, inconsistencies, and "orphaned" datasets. Reduced time wasted searching or validating data.
- *Accelerating time to market* → Easily discover and reuse existing datasets, reducing reliance on technical teams.
- *Greater focus on core business* → Teams no longer need to worry about technical maintenance.
- *Centralized catalog and metadata* → Provides an active data catalog with technical and operational metadata. Automatically integrate with Big Data systems (Kafka, Hive, Spark, Databricks, etc.).
- *Automated Data Lineage* → Automatically tracks end-to-end data flows from ingestion to transformations, all the way to consumption (dashboard, API, ML).
- *Native APIs and integrations* → Exposes APIs and plugins for continuous integration with orchestration, observability, quality, and security tools.
- *Access and Security Policy Management* → Centralizes access policies based on roles and classifications. Improves data security without fragmenting rules across services.
- *Automation and Self-Service* → Fosters a self-service data discovery model for data engineers and data scientists.
- *Scalability and modern architecture* → Microservices architecture and Metadata Graph.

4.9 Artificial Intelligence (AI) Family

Below is the list of services belonging to the Artificial Intelligence (AI) family:

- Speech to Text
- AI Audio & Video Analytics
- OCR
- Text Analytics/NLP
- Translation
- AI Search - RAG
- AI Platform
- AI SLM/LLM

4.9.1 Speech to Text

4.9.1.1 Service Description

This service provides an advanced speech-to-text model for transcribing audio files into text, trained on a vast dataset of audio and text in various languages using neural AI (deep learning) models specialized in automatic speech recognition (ASR).
The service is optimized for English transcription, but can also recognize and transcribe speech in other languages, still returning the text in English. Furthermore, it can automatically identify the spoken language and supports automatic speech translation.
It is useful for automatically transcribing conversations, interviews, meetings, call centers, podcasts, or videos; supporting chatbots and voice assistants, translating voice into text understandable by NLP or AI systems; indexing and analyzing audio content (semantic search, sentiment analysis, data mining); and digitizing voice archives and official minutes, ensuring accuracy and traceability.

The service is sized and offered per GPU. Each GPU consists of one NVIDIA H200 partition.

4.9.1.2 Features and Advantages

This is a Whisper-based service that provides an API layer and an SDK for integration with existing applications. All tasks are represented as a sequence of tokens that the model predicts, unifying and optimizing the speech processing pipeline.

The service offers the following main features:

- *Automatic Speech Recognition (ASR)* → converts speech to text in real time or from audio files (WAV, MP3, MP4, FLAC, etc.). Multilingual support. *Advanced Neural Accuracy* → uses sequence-to-sequence Transformer models, trained for a wide range of speech processing tasks, such as multilingual speech recognition, speech translation, and language identification.
- *Multilingual Recognition and Machine Translation*
- *Real-time Transcription (Streaming) Batch Processing*
- *Temporal Segmentation* → returns start/end timestamps to synchronize text and audio (useful for subtitles or editing).
- *Text Cleanup and Normalization* → automatically corrects punctuation, capitalization, and formatting.
- *Accent and Ambient Noise Support* → is robust against background noise, poor microphones, and natural (non-studio) speech.

The main components of the service are:

- *Whisper engine (ASR Core)* → transformer neural model trained on millions of hours of audio-text data.

- *Language detection module* → automatically identifies the language of the speech.
- *Post-processing & text normalization* → corrects the transcription, inserts punctuation, and adds consistent formatting.
- *Optional translation layer* → uses a Neural Machine Translation (NMT) model to translate the transcription into another language.
- *Storage and logging* → stores results, metadata, and logs for auditing and analysis.
- *Integration layer (API / SDK)* → interface for external apps, dashboards, or AI pipelines.

The service offers the following advantages:

- *Reduced operating costs* → automate the transcription of audio, meetings, interviews, and minutes without requiring dedicated staff.
- *Increased staff productivity* → automatic transcription saves hours of work.
- *Accelerated document processes* → minutes, interviews, meetings, or consultations can be transcribed and distributed in real time, improving administrative efficiency.
- *Accessibility and inclusion* → generate subtitles and text from audio/video content, improving accessibility for people with hearing impairments and multilingual communication.
- *Data-driven decisions (Voice Analytics)* → voice transcriptions become analyzeable text data, supporting data-driven decisions.
- *Improved customer experience* → chatbots, contact centers, and digital assistants become more effective by recognizing voice and responding naturally.
- *High linguistic accuracy* → the service, based on Transformer architecture, guarantees more precise transcriptions even in the presence of accents, noise, or natural speech.
- *Structured and interoperable output* → output in standard formats (JSON, TXT, SRT, VTT, DOCX) easily integrated with databases or document workflows.
- *Model updates* → managed and ongoing model updates, improving accuracy and reducing errors over time.
- *High performance and low latency* → processing in milliseconds for live streams, seconds for large files.
- *Multimodal AI support* → can be combined with Text Analytics, Translation, and Text-to-Speech services to create complete speech pipelines (e.g., transcription + translation + synthesis).
- *Service scalability* → allows you to simultaneously manage thousands of speech streams by providing and managing the necessary infrastructure.

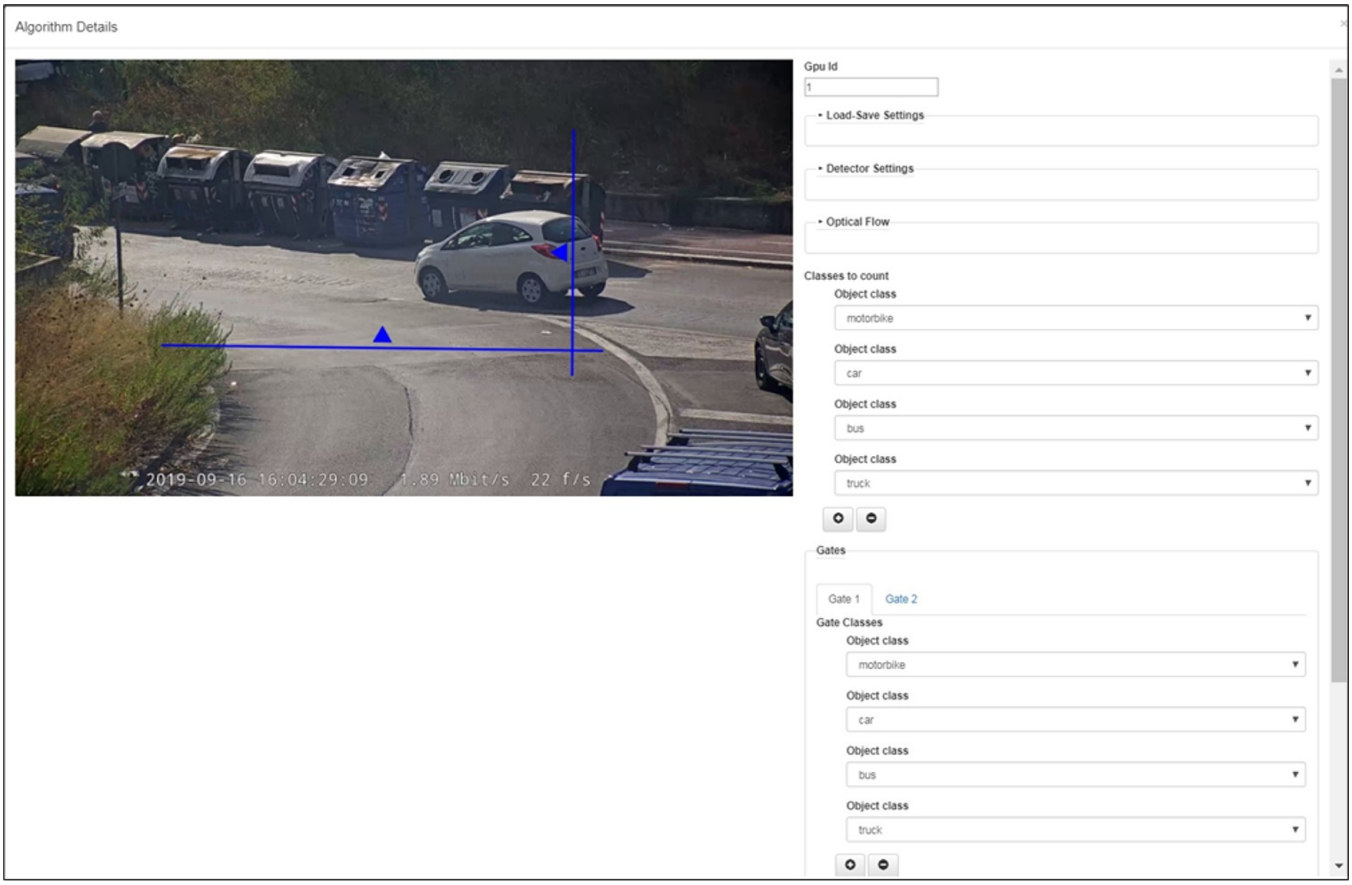
4.9.2 AI Audio & Video Analytics

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform



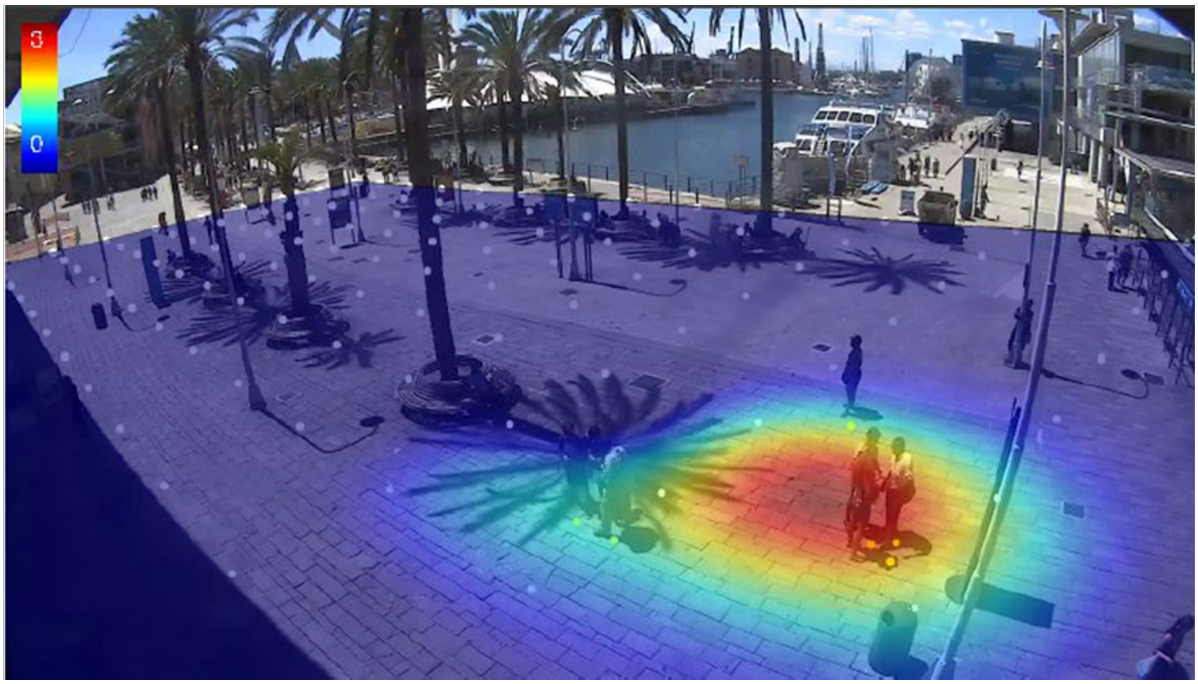


Figura 36 – AI Audio & Video Analytics Services

4.9.2.1 Services Description

These are two services, separate but integrable when necessary, developed by Leonardo.

The *AI Audio Analytics PaaS* provides a ready-to-use platform that, thanks to AI-based algorithms on audio sources, allows the identification of unique features from audio streams using preloaded AI models. These features allow the identification of a person's voice, noises, and possible anomalies in the monitored environment.

The *AI Video Analytics PaaS* is a ready-to-use platform with pre-trained algorithms that leverage computer vision techniques, capable of processing and understanding visual information present in two-dimensional images or video sequences.

The Audio and Video analytics services are sized and offered for GPU unit, specifically:

- for audio analytics: 1 partition H200 GPU per unit
- for video analytics: 1 H200 GPU per unit

4.9.2.2 Features and Advantages

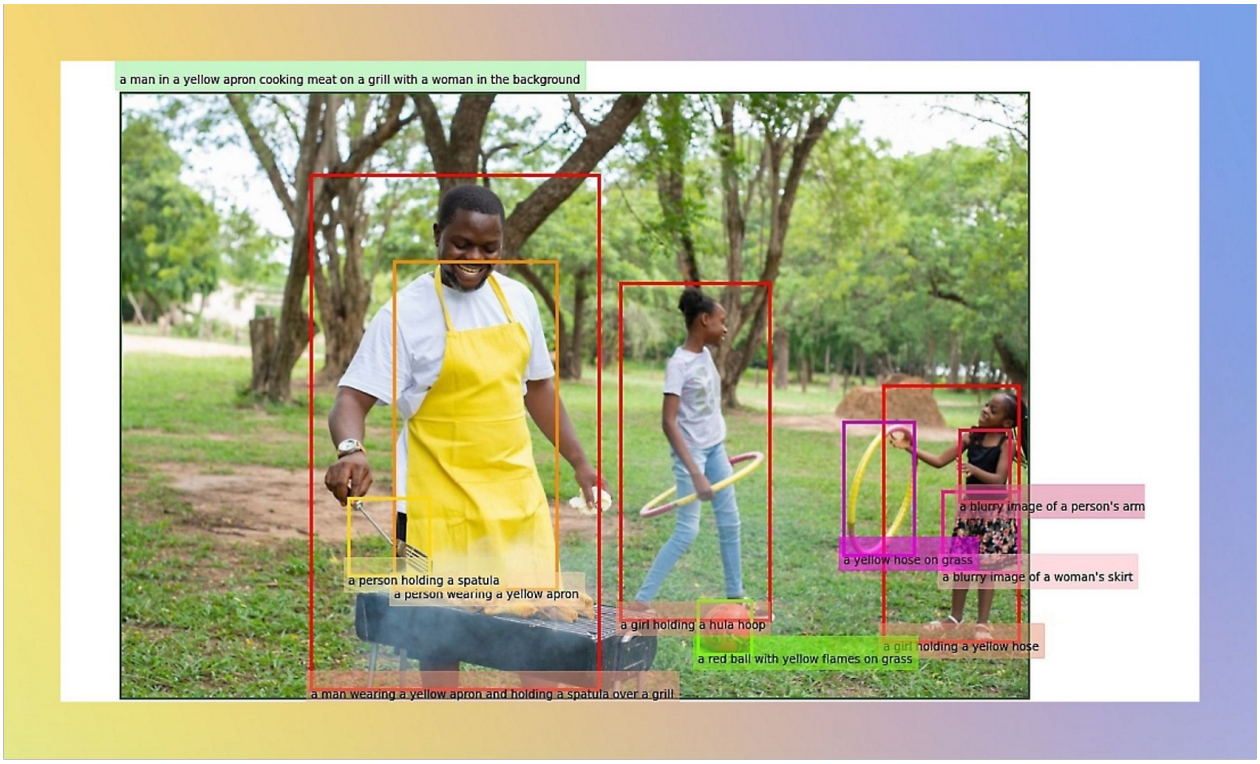
The *AI Audio Analytics platform* can work with signals produced in the field from various audio sources, overcoming the "curse of dimensionality" problem caused by the high-dimensionality of the phenomenon through the use of unsupervised and supervised approaches. These approaches dynamically identify an optimal set of features to identify similarities between signals for the same event/process and differences between signals for different events/processes. The output of these processes can then be treated as characteristics in statistical detection methods, but they rely heavily on the analyst's understanding of a possible link between the signal and the process/event being detected.
The AI Audio Analytics solution is primarily composed of the following tools: - *Swagger UI* → a collection of HTML, CSS, and JavaScript assets automatically generated from the documentation, which must comply with the OpenAPI standard. - *ML models* → algorithms for extracting information from audio sources for: - Speaker identification: an ML model capable of identifying the speaker using voice characteristics. - Audio anomaly insight: an ML model capable of detecting sound anomalies in production or cyclical systems. - Environment classification: an ML model capable of identifying and classifying audio tracks. - *FastAPI framework* → a modern, fast (high-performance) web framework for building APIs with Python.

The *AI Video Analytics* platform includes subsystems: preprocessing, image analysis, and image interpretation. The service can perform video analysis while optimizing computation time through the use of single-pass convoluted networks, which analyze all parts of the image in parallel and simultaneously, eliminating the need for sliding windows.
The AI Video Analytics solution is primarily composed of the following tools: - *ML models* → algorithms for extracting information from video sources. - Object detector: recognizes and locates people and objects within a given frame by extracting metadata containing classification and spatial location - Spacial counter: an extension of the Object Detector model, it can also process a single-shot counting for each object class for each frame - Object counter: capable of both locating people and objects and obtaining a count of the detected objects.

The service offers the following advantages:

- *Improved security and compliance* → automatic detection of anomalous behavior, intrusions, or risky situations. Support for compliance policies and audits based on video/audio evidence.
- *Improved customer experience* → analysis of tone of voice, emotions, and wait times for improved quality of service and customer interactions.
- *Reduced operating costs* → automated continuous monitoring of environments, processes, and media flows, resulting in optimized human resources and response times.
- *Data-driven decisions* → media content becomes a source of structured and analyzable data for visual and audio insights that can be integrated into Business Intelligence systems.
- *Innovation and new business models* → enable new services such as retail analytics, behavioral marketing, intelligent security, and event monitoring for competitive advantage and market differentiation.
- *Scalability and simplified management* → management of resources, workloads, and updates.
- *Integrated advanced analytics* → ready-to-use features, e.g. Facial recognition, object detection, speech-to-text, voice sentiment, anomaly detection.
- *Real-time and batch processing* → analysis of live streams or recorded media archives, thanks to the integration of Processing PaaS.
- *Multi-format and multi-source support* → compatibility with various formats (MP4, AVI, WAV, RTSP, etc.) and heterogeneous devices (cameras, microphones, sensors).
- *Integrated security and privacy* → stream encryption, access control.
- *Operational monitoring and insights*.

4.9.3 Optical Character Recognition (OCR)



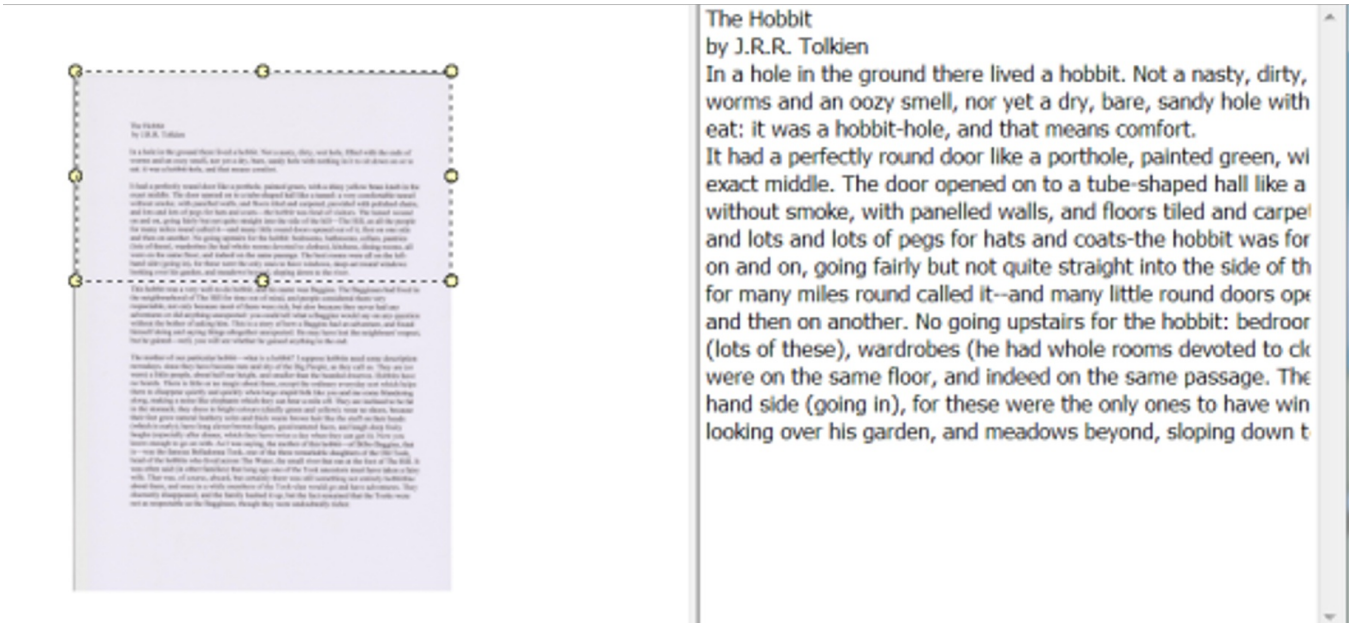


Figura 37 – Optical Character Recognition (OCR) Service

4.9.3.1 Services Description

The services offer innovative computer vision capabilities, enabling the transformation of visual content containing text into processable digital content.
It is useful for analyzing images, reading text, and detecting faces with predefined image tagging, text extraction with Optical Character Recognition (OCR), and responsible facial recognition.
The OCR component (reading printed or handwritten text) is integrated as a REST API or client library that allows you to send images/documents and obtain text extraction from them.
It is useful in multiple scenarios: automatic text extraction from images and vice versa, document processing (e.g., scanning PDFs, form images, extracting written or printed text), and process automation (e.g., data acquisition from forms, invoices, intelligent archiving, full-text search in image content).
The service is offered using open soource OCR technologies with container-based sizing.
Each container consists of 16 GB of RAM.

4.9.3.2 Features and Advantages

The main features of the service are:

- *Text recognition* → recognizes printed or written text in over 100 languages
- *Multi-language models* → can process mixed languages (e.g., English + numbers + symbols)
- *Multiple image input* → supports PNG, JPEG, TIFF, BMP, PDF (via external libraries such as pdfimages).
- *Page layout analysis* → recognizes text blocks, columns, paragraphs, direction, and orientation. Multiple output formats.
- *Model training & fine-tuning* → ability to train models on specific fonts or languages (with dedicated datasets).
- *Image enhancement* → supports skew correction, binarization, thresholding, and deskewing.

The main components of service are:

- *API Layer* → Exposes REST endpoints for loading images or URLs.
- *Compute Layer* → Runs the Tesseract engine in scalable containers.
- *Storage Layer* → Stores image input and text output.
- *Processing Layer* → OCR engine and image management.
- *API Layer* → Exposes REST endpoints for loading images or URLs.
- *Monitoring & Logging* → Performance monitoring and call logging.
- *Security Layer* → API and data protection.

The service offers the following advantages:

- *Lower document management costs* → fewer staff dedicated to data entry and fewer errors that generate correction costs or disputes.

- *Paperless transformation* → enables the complete digitalization of archives and paper flows, reducing paper consumption and physical space.
- *Faster and more traceable workflows* → Scanned documents become immediately accessible data and can be integrated into management systems.
- *Traceability and compliant archiving* → Facilitates compliant digital archiving, improving compliance management (GDPR, electronic preservation).
- *Extensive support* → Native support for dozens of languages and formats (e.g., PDF, JPEG, PNG, TIFF, scanned documents).
- *Standard formats* → The extracted text is immediately usable in management or analytics systems.
- *Real-time and batch processing* → Analysis of live streaming or recorded multimedia archives, thanks to the integration of Processing PaaS.
- *Managed maintenance and updates* → the infrastructure, security, and updates of AI models are managed.

4.9.4 Text Analytics/NLP

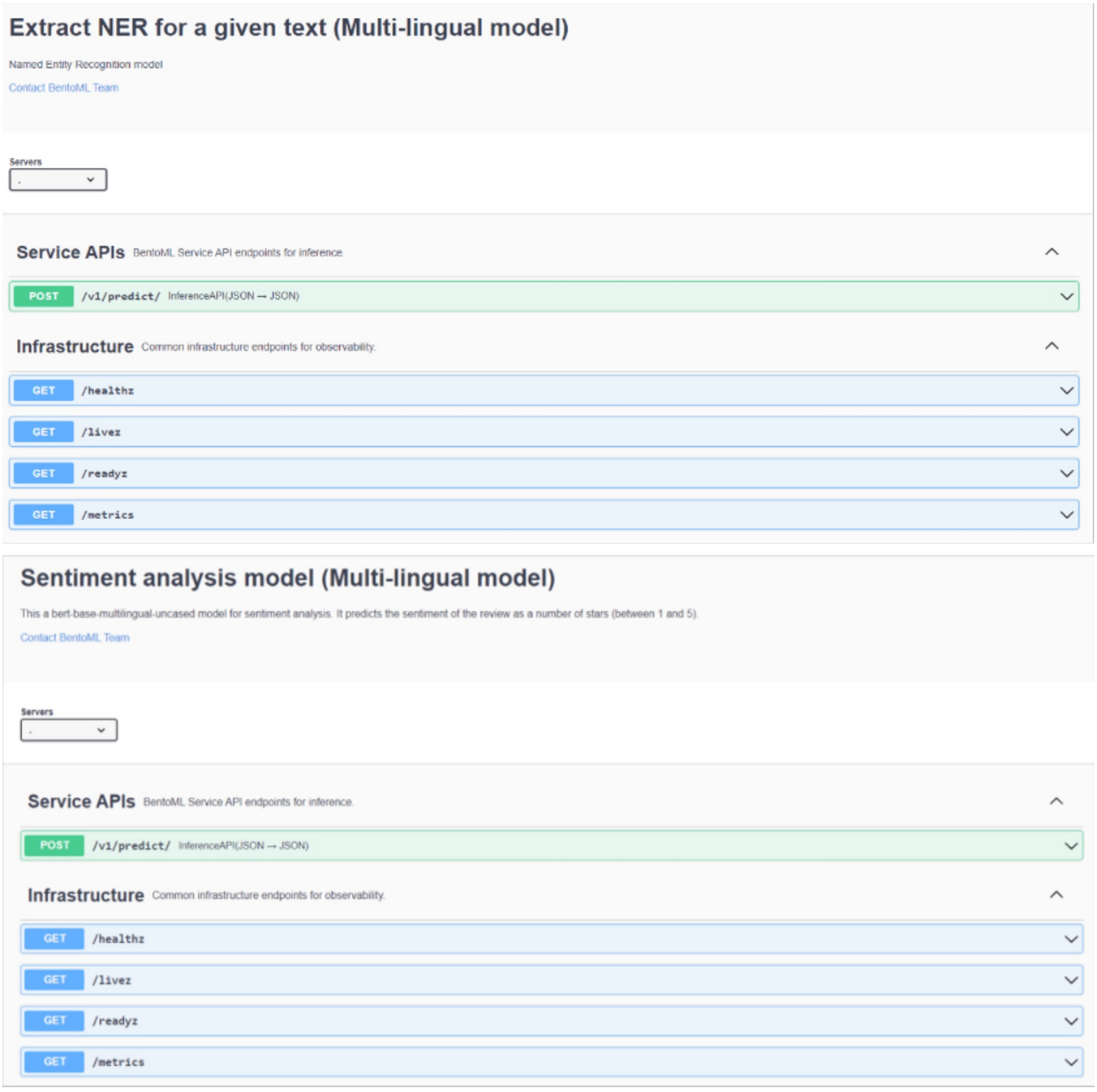


Figura 38 – Text Analytics Service

4.9.4.1 Service Description

The Text Analytics PaaS solution, developed by Leonardo, provides a ready-to-use NLP (Natural Language Processing) platform capable of extracting structured and interpretable information from unstructured texts, enabling quantitative and qualitative analyses that would be time-consuming and difficult to perform manually.
The system can identify entities (people, places, organizations, etc.), translations, key concepts, and sentiment from text to identify and extract opinions from text. Multilingual support.

The service is sized per unit of 1 partition H200 GPU.

4.9.4.2 Features and Advantages

The solution can perform various types of analysis, including:

- *Entity Extraction (NER)* → recognizes the names of people, companies, places, products, dates, etc.
- *Sentiment analysis* → understands whether the text expresses a positive, negative, or neutral opinion.
- *Theme and Topic detection* → identifies key concepts in the text.
- *Language Detection* → detects the language in which a text was written.

The main components of the service are:

- *Swagger UI* → Collection of HTML, CSS, and JavaScript assets automatically generated from the documentation, which must be compliant with the OpenAPI standard.
- *ML Models* → List of ready-to-use pre-trained models, including:
  - Key Phrase Extraction: extracts salient parts of text.
  - Language Detection: infers language from text.
  - Named Entity Recognition: extracts real-world entities from text, such as the names of people, places, data, companies, etc.
  - Sentiment Analysis: recognizes sentiment from text.
- *FastAPI Framework* → Modern, fast (high-performance) web framework for building APIs with Python.

Model creation workflow: 1. *Data acquisition* → obtains raw text data from various sources to create a robust dataset for NLP tasks.
2. *Text preprocessing* → includes several steps to refine the raw text data for meaningful analysis and model training (e.g., text cleaning) Text, tokenization, stopword removal, normalization).
3. *Feature Engineering* → transforms raw textual data into numerical features that machine learning models can understand and effectively use to capture semantic meaning, contextual information, and word relationships.
4. *Modeling & Evaluation* → the heart of the pipeline, where models are applied and evaluated using various approaches (heuristics, ML, Deep Learning, etc.) to comprehensively measure model performance from both a technical and practical perspective.
5. *Deployment* → marks the transition of the developed model from the development environment to a production environment, followed by continuous monitoring and adaptation to ensure lasting performance and relevance.

The service offers the following advantages:

- *Better understanding for users and service consumers* → analyzes feedback, reviews, chats, and surveys to extract sentiment.
- *Data-driven decisions* → transforms unstructured text into quantifiable insights that can be displayed in dashboards.
- *Reduced operational costs* → automates text comprehension, significantly reducing human overhead.
- *Reduced operational costs* → automates text comprehension, significantly reducing human overhead.
- *Automation and scalability* → analyzes large volumes of text from heterogeneous sources.
- *Faster time to market* → simple integration via API with third-party systems and applications.
- *Multilingualism and semantic support* → understands meanings, synonyms, and context (not just keywords).

4.9.5 Translation

4.9.5.1 Service Description

Developed by Leonardo using AI-based machine translation (NMT) technologies, the multilingual translation service to enable rapid and accurate translation of text from the source language to the target language in real time.
The service draws inspiration from the human brain not only for its neural structure, but also for its ability to adapt, learn from new experiences, and interact with users.
The result is a so-called human-in-the-loop approach, a cycle in which machine and human continuously support each other, providing exceptional translation quality and process efficiency that surpasses previous approaches.

It is sized per GPU unit. Each unit consists of 1 NVIDIA H200 GPU.

4.9.5.2 Features and Advantages

The service offers the following main features:

- *Neural Machine Translation (NMT)* → uses deep neural networks for more natural and contextual translations than statistical models.
- *Real-time translation* → streaming translation for chat, call centers, multilingual apps, or conferences.
- *Document translation* → translation of complete files (DOCX, PDF, TXT, HTML, etc.) while maintaining layout and formatting.
- *Custom translation* → training of custom AI models with glossaries and datasets specific to the industry or company.
- *Automatic language recognition* → automatically detects the source language before translation.

The main components of the service are:

- *Translator REST API* → main endpoint for sending text, receiving translations, or metadata (languages, glossaries).
- *AI NMT Engine* → proprietary neural engine based on Transformer networks (similar to GPT) for contextual translations.
- *Custom Translator* → portal + API for training models with custom datasets.
- *Document translation API* → service dedicated to batch file translation (integration with Blob Storage).

The service offers the following advantages:

- *International expansion* → allows you to easily communicate with customers, suppliers, and citizens of different languages, enabling access to new markets or linguistic communities.
- *Reduced translation time and costs* → automates the translation of texts, documents, and communications, reducing reliance on human translators and accelerating publication workflows.
- *Multilingual process automation* → integrates translation directly into digital processes, eliminating manual tasks and downtime.
- *Improved access to information and knowledge* → International content (reports, technical documents, studies) becomes immediately accessible in local languages.
- *Accuracy thanks to neural translation models (NMT)* → Neural translation engines understand context and produce more natural-sounding texts than older statistical models.
- *Multiformat support* → automatic translation of texts, documents (PDF, DOCX, HTML), and data streams in real time.
- *Linguistic customization* → ability to train custom models with glossaries or corporate terminologies for more consistent translations.

- *AI Model Updates* → Constantly updating the included neural models, improving accuracy and language support without manual intervention.

4.9.6 AI Search - RAG

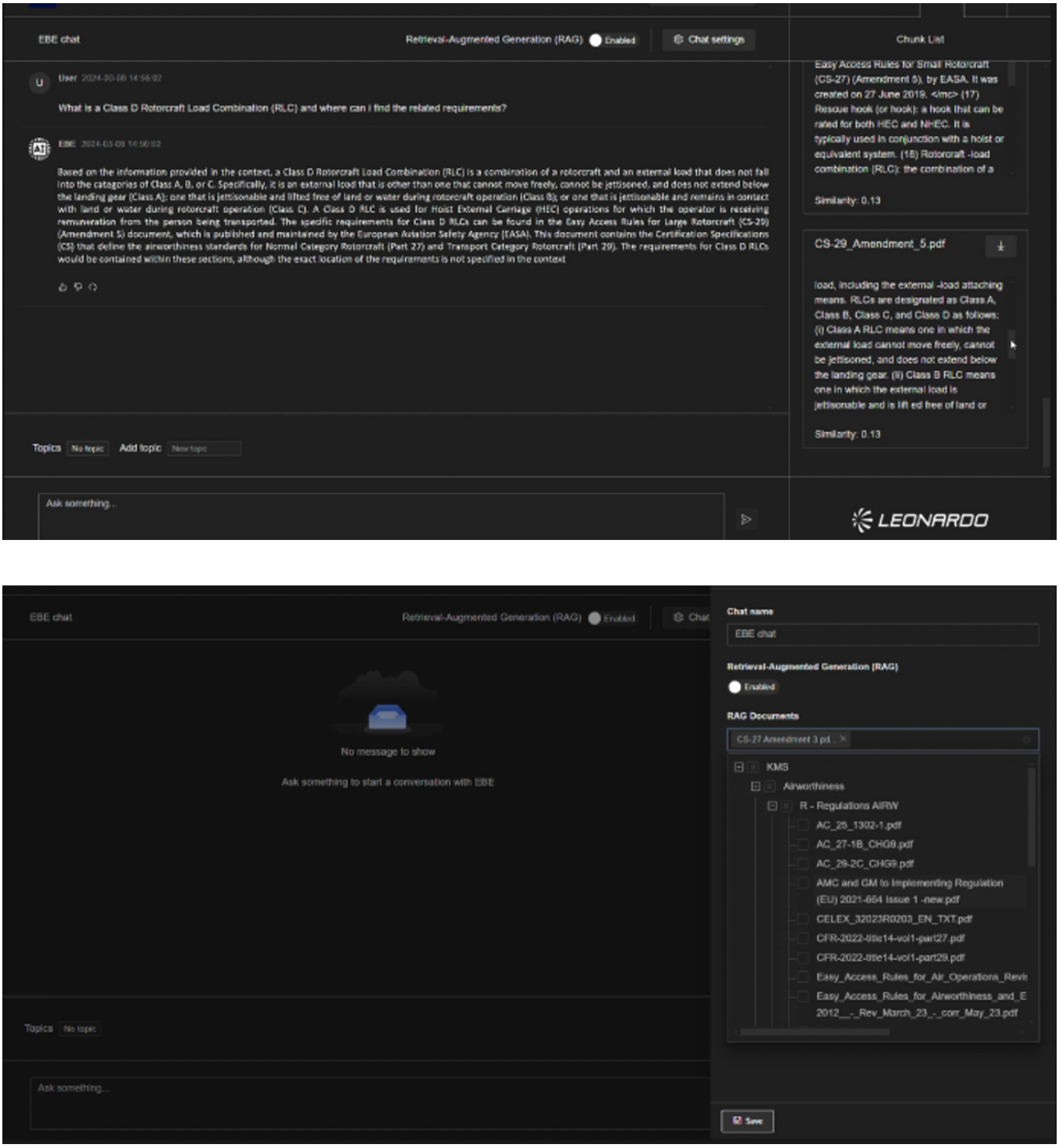


Figura 39 – AI Search - RAG Service

4.9.6.1 Service Description

AI Search-RAG is a system developed by Leonardo for automatically generating answers to user-generated questions using context and information from reliable data sources. It can be integrated into environments requiring a virtual assistant capable of responding using reliable, contextualized information. The system generates answers by first searching for relevant information or passages from a reliable external knowledge base using AGENTIC RAG (Retrieval-Augmented Generation) techniques. This service allows for better contextualization of the search, further improving the quality and accuracy of the generated answers compared to traditional text-based RAGs. AI Search allows individuals and organizations to quickly access relevant, contextualized information through a simple and intuitive graphical interface built on a chat model, improving efficiency and productivity through advanced intelligent search tools.

The service is sized per GPU unit. Each unit consists of one NVIDIA H200 GPU.

4.9.6.2 Features and Advantages

The service offers the following main features:

- *Activation of the Big Data PaaS Data Lake service* → to meet object storage needs.
- *Use of appropriately optimized Large Language Models and Embeddings* → to provide value to specific contexts and for specific users.
- *User authentication* → integrates with existing security protocols. Understands natural language → provides coherent and complete answers, retrieving multimodal information from knowledge expressed as text and audio. Supports multilingual models
- *Feedback collection* → after a query is resolved, AI Search collects user feedback
- *Document segmentation by user*

The main components of the service are:

- *Model Repository* → at a minimum, a virtual assistant and an embedding model are required.
- *Vector Database and Search Engine* → it uses a vector database that stores vector representations (embeddings) of the input data, allowing documents and information to be retrieved based on their meaning (semantic search). It also uses a traditional search engine (lexical search) that operates on text and metadata, performing searches based on keywords and structured criteria (e.g., BM25, FT-IDF).
- *Document Manager* → responsible for retrieving documentation from a specific repository and indexing it in the vector database for use in user queries.
  AI Search is composed of three layers:
- *Data layer* → represents the database and the primary source of information.
- *Analysis layer* → responsible for all processing, analysis, and generation of answers to user queries. It includes the Retriever and the Generator, responsible for retrieving the most relevant information and creating coherent

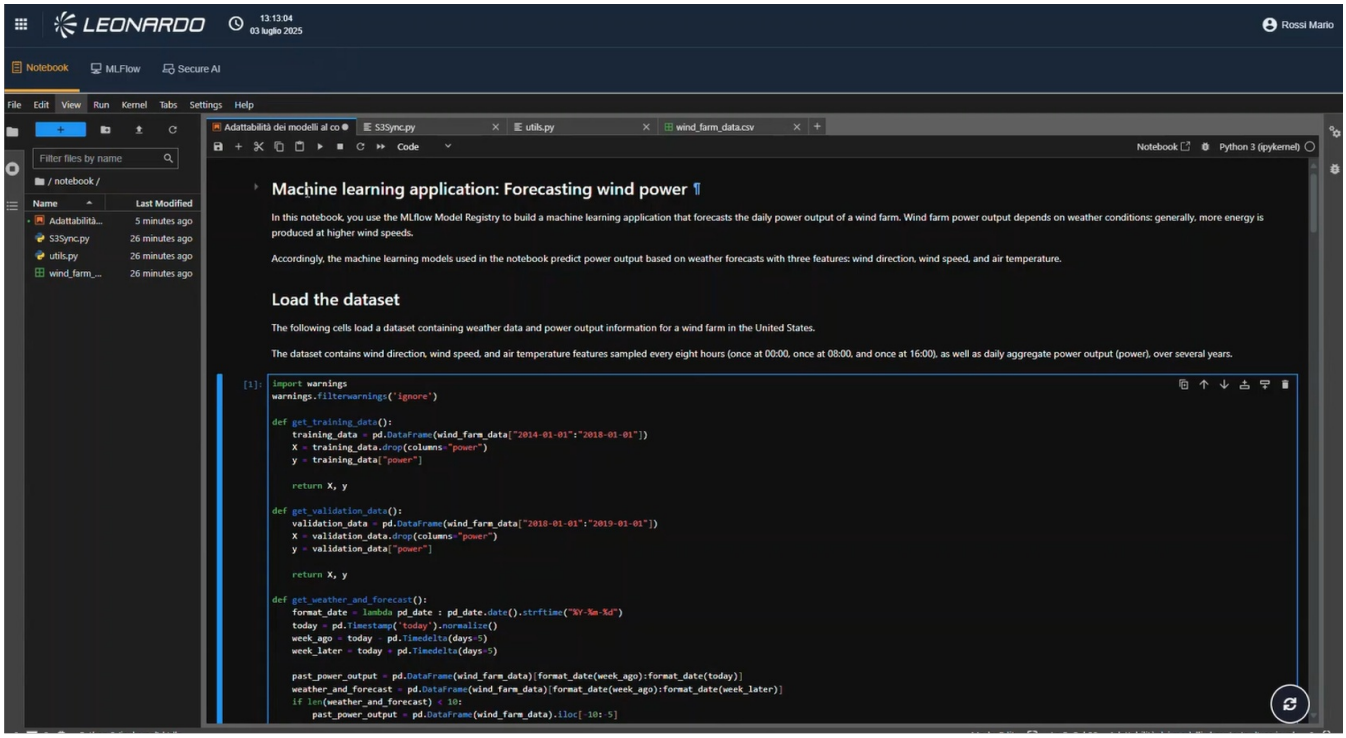
and personalized responses, respectively.

- *User layer* → interface through which the user interacts directly with the service, offering the ability to query the knowledge base, view answers with referenced sources, manage documents, and provide feedback.

The service offers the following advantages:

- *Access to up-to-date knowledge* → answers always based on the most recent internal and external documents.
- *Reduced operational costs* → less time spent on manual searches and repetitive support.
- *Improved customer/employee experience* → relevant, clear, personalized answers.
- *Increased competitiveness* → leverages proprietary knowledge, not just public knowledge.
- *Risk mitigation* → reduces errors and hallucinations, increasing the relevance of output to user questions.
- *Upgradability without retraining* → simply update the database/document repository, not the LLM.
- *Hybrid vector search* → combines semantic search with traditional text search.
- *Model efficiency* → LLM-based host model oversees activities and decisions and supervises other, simpler agents (LLM).
- *Traceability and transparency* → sources cited to support the answer can be displayed.
- *Bias reduction* → thanks to the indexing of the text on a vector DB, the LLM conductor will receive as input a context relevant to the questions asked by the users.

4.9.7 AI Platform



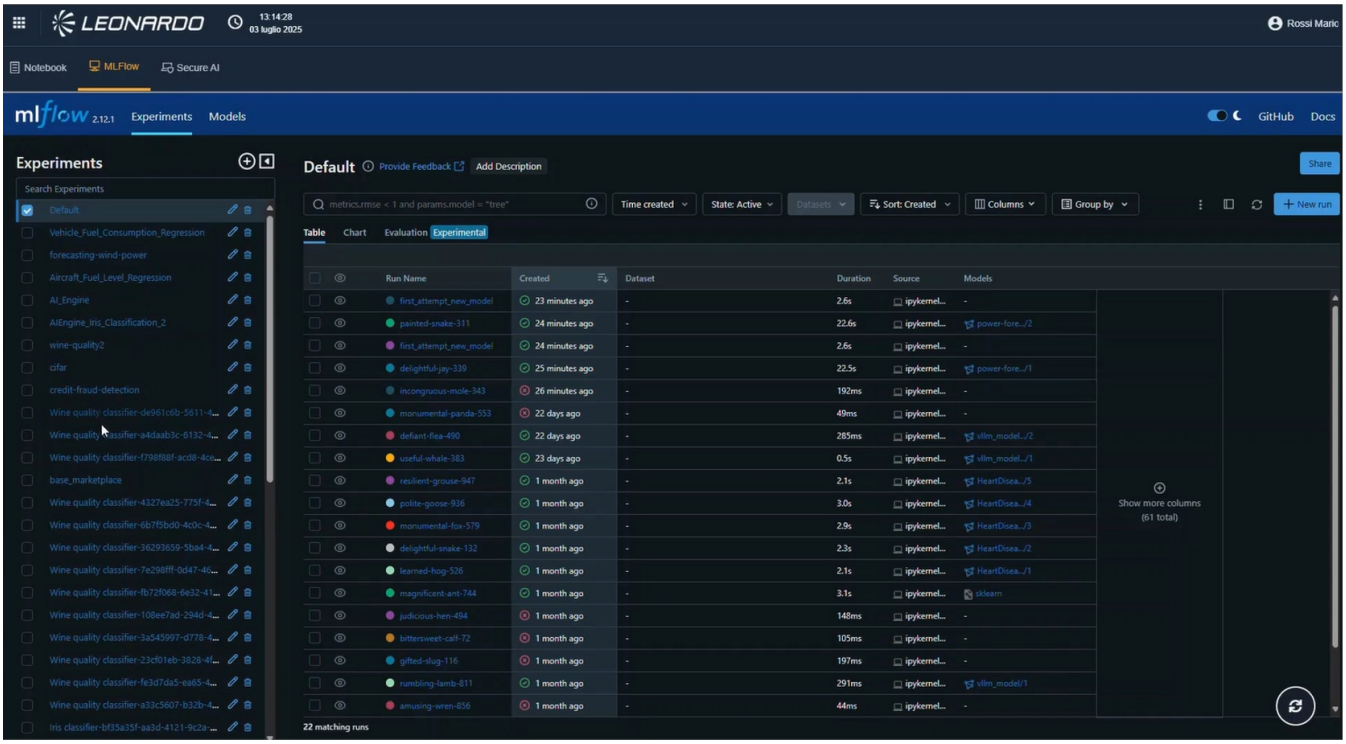


Figura 40 – AI Platform Service

4.9.7.1 Service Description

The AI Platform PaaS service, developed by Leonardo, uses AI technologies (machine learning and deep learning) to provide domain experts (data scientists, data analysts, and AI engineers) with a collaborative platform to create, track, use, and monitor ML models simply and intuitively, yet reliably and efficiently.
The service provides a ready-to-use platform capable of easily managing the entire lifecycle of ML models. The solution is certified, managed, and maintained by the provider.
The platform can be enhanced using, in addition to the Data Lake service, other technologies made available by the Big Data PaaS.
The services are designed to ensure digital sovereignty through deployment on secure national infrastructure, with a particular focus on latency and optimization of computational resources.

The service is sized per unit of 1 GPU H200.

4.9.7.2 Features and Advantages

The platform is capable of managing the lifecycle of ML models through the following phases:

- *Data processing* → which will be optimized if the Big Data PaaS Data Governance and Processing Engine services are activated for the extraction, transformation, and loading of datasets into the AI Platform.
- *Model training and evaluation process* → through a JupyterLab on the AI platform. - *Model tracking and saving process*.
- *Model management process* → through the model registry provided by the MLOps tool.
- *Model serving process* → for the creation of Docker images ready for deployment on any target system. These can be tested directly on the platform through the swagger describing the inference service.

The solution is primarily composed of the following custom tools:

- *JupyterLab* → allows the creation and sharing of web scripts in JSON format using a Notebook, which follow a schema and an ordered list of input/output cells. The created Jupyter documents can be exported as HTML, PDF, Markdown, or Python documents.
- *Mlflow* → allows for the lifecycle management of ML models. It simplifies the complex procedures for implementing machine learning. Consisting of:
  - MLflow Tracking: records and tracks metrics and artifacts (models plus their dependencies) of the training process.
  - MLflow Model Registry: stores models in a centralized registry to collaboratively manage the entire model lifecycle.
  - DBMS Metadata: stores all metadata in a relational database to track all development flows of a given ML model.

- Object Storage: stores all developed models and their dependencies to facilitate the subsequent model serving process in production.

- *Model Serving* → facilitates the deployment of ML models at scale in production environments through the creation of Docker images.

The service offers the following advantages:

- *Reduced initial and operational costs* → there is no need to invest in hardware infrastructure (GPU, cluster, server, storage, etc.), thus reducing maintenance, upgrade, and security costs.
- *Scalability* → the service can scale compute and storage resources based on model complexity or data volume.
- *Faster time to market* → models can be developed, tested, and deployed much faster thanks to pre-built tools and pipelines.
- *Focus on business value* → domain experts can focus on model research and development, increasing team productivity and efficiency.
- *Easy integration with other services* → trained models can be quickly integrated with other services (API management, Business Intelligence, Data Lake, etc.) to create complete AI-driven solutions.
- *Automated model lifecycle management* → native MLOps support for model versioning, performance monitoring, and automatic retraining.
- *Managed and optimized environment* → the execution environment is preconfigured with ML libraries, with security updates and patches managed by the provider.
- *Integrated monitoring and logging* → training metrics, logs, and results are tracked to easily diagnose convergence or overfitting issues.
- *Simplified deployment* → creating Docker images for model inference allows for simplified deployment to any target system.

4.9.8 AI SLM/LLM

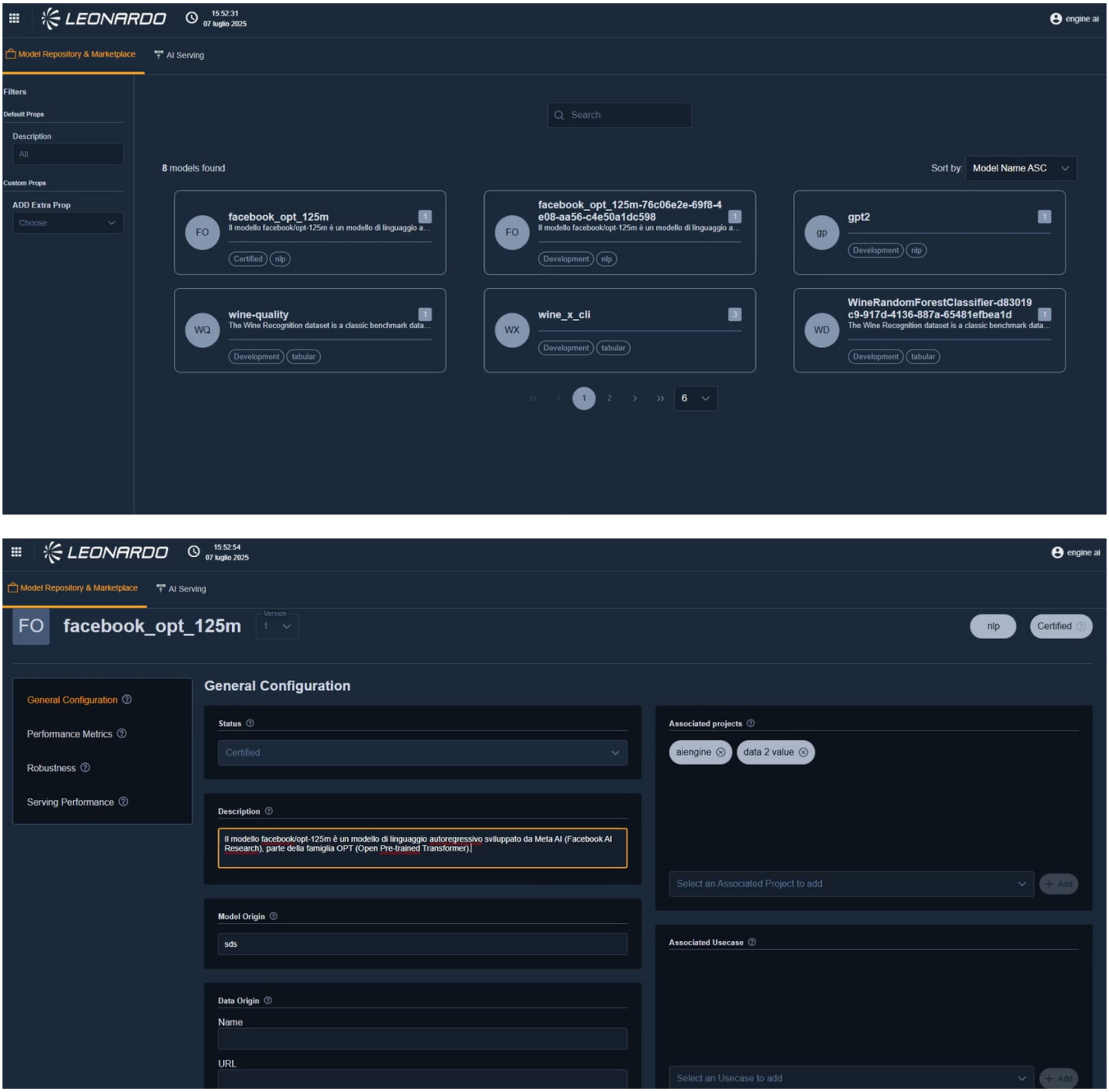


Figura 41 – AI SLM/LLM Services

4.9.8.1 Services Description

These are Generative AI PaaS developed by Leonardo that provide optimized linguistic inference capabilities. They use predefined linguistic models to understand and generate natural text.
They allow the use of two types of linguistic models:

- *Small Language Model (SLM)*: small-scale linguistic models that are lighter, more efficient, and specialized in specific domains, offering fast and precise solutions for everyday linguistic needs.
- *Large Language Model (LLM)*: linguistic models with numerous parameters for extremely high linguistic comprehension and generation capabilities, ideal for complex interactions, virtual assistants, semantic search, and automation. SLMs are suitable for performing specific, less complex applications and tasks (e.g., text autocompletion, short sentence translation, and text classification), where an LLM would be too computationally expensive.

The services are sized per GPU unit:

- for AI SLM service each unit consists of 1 partition NVIDIA H200 GPU.
- for AI LLM service each unit consists of 1 NVIDIA H200 GPUs.

4.9.8.2 Features and Advantages

The service offers the following main features:

- *Tenant isolation* → each customer will have a dedicated Tenant on the customer infrastructure with complete isolation of data, configurations, and uploaded models.
- *Resource allocation* → each customer will be assigned dedicated infrastructure resources (CPU, GPU, RAM, Storage) to their Tenant, sized appropriately.
- *Auto-scaling* → tenant resources can scale to respond to load variations.
- *Cloud-native deployment* → the service will be deployed in the customer's tenant in cloud-native mode on the OpenShift platform, ensuring portability, resilience, and standardization of operating procedures.
- *Centralized observability* → provides centralized platform monitoring services with log collection, metrics, and alerting for complete observability, audit trails, and advanced troubleshooting.
- *PaaS integration* → uses PSN PaaS components for storage, networking, security, and identity management, ensuring compliance with project requirements and leveraging the economies of scale of shared infrastructure.

Both services feature a modular architecture designed to ensure scalability, flow segregation, and ease of integration into public administration processes.

- *API Layer* → provides access to SLM/LLM services through two main methods: REST API calls for integration with existing systems, or through a Web UI for direct, user-friendly interaction.
- *Inference layer* → this is the heart of the service, where SLM/LLM models reside and execute. It consists of:
- *Inference engine* → runs language models optimized for latency and GPU/CPU resource consumption.
- *Model pool management* → maintains a set of validated and pre-configured models, selectable by the customer. Only one model is active per tenant at any time.

- *Platform layer* → provides cross-functional support services and includes: Resource Management & Scaling: Dynamic allocation of computational resources (CPU, GPU, RAM, storage), load-based auto-scaling, and service lifecycle management.

The service offers the following advantages:

- *Technological accessibility* → access to no-code Generative AI technology solutions.
- *Reduced operating costs* → no upfront investment in hardware infrastructure or proprietary models.
- *Faster time to market* → easier models to integrate into business solutions.
- *Operational efficiency* → automate repetitive tasks, reducing processing times and improving service quality.
- *Flexible adoption* → choose between SLM (small, specialized models) or LLM (generalist models with broader knowledge capabilities) depending on the use case.
- *Risk mitigation* → leverage pre-trained and validated models without the need for specialized ML skills.
- *Easy integration with existing systems* → orchestrate complex processes through microservices and integrated ML pipelines.
- *Performance optimization* → PaaS allows you to combine both advantages: use SLM for simple, targeted tasks, while LLM is used only for tasks that require broader, more generalized linguistic understanding.
- *Fast and simplified model testing* → ready-to-use models thanks to the playground functionality available directly in the interface. - *Rapid prototyping and DevOps AI* → ready-to-use environment for developing, testing, and deploying applications through standard interfaces.
- *Multi-model and hybrid AI* → ability to combine open source and proprietary models in the same ecosystem.

4.9.9 High Performance Computing description

The computational capacity is 14.3PFlops for the Davinci-2 is provided throught the GPUs NVIDIA H200 while 5PFlops for the Davinci-1 that is provided throught the GPU NVIDIA A100.
Cooling is mixed, air and liquid depending on the technology and density-

Technology assets:

- CPU Intel Cascade Lake
- CPU Intel Sapphire Rapids
- CPU AMD EPYC Rome
- CPU AMD EPYC Genoa
- NVIDIA A100 GPU
- NVIDIA Grace-Hopper

- NVIDIA H200 GPU
- NVIDIA RTX 8000 GPU
- NVIDIA L40s GPU
- AMD MI 300 GPU

The infrastructure is hosted in Italy and managed entirely by internal staff.
The architecture complies with NIST standards and is ISO27001 certified.
Information management and protection is guaranteed by international standards and company policies.
All data and infrastructure are hosted in Italy, with copying, backup, and redundancy systems.

The virtualization platform used is OpenStack.
Additional features developed by an internal team have been integrated into this platform.

The entire application layer is based on Linux operating systems and open source software such as: Openstack, OpenPBS, Slurm.

A testing system inside allows us to replicate features, so we can apply changes and patches without compromising production.

4.10 Collaboration Family

Below is the list of services belonging to the Collaboration family:

- Instant Messaging

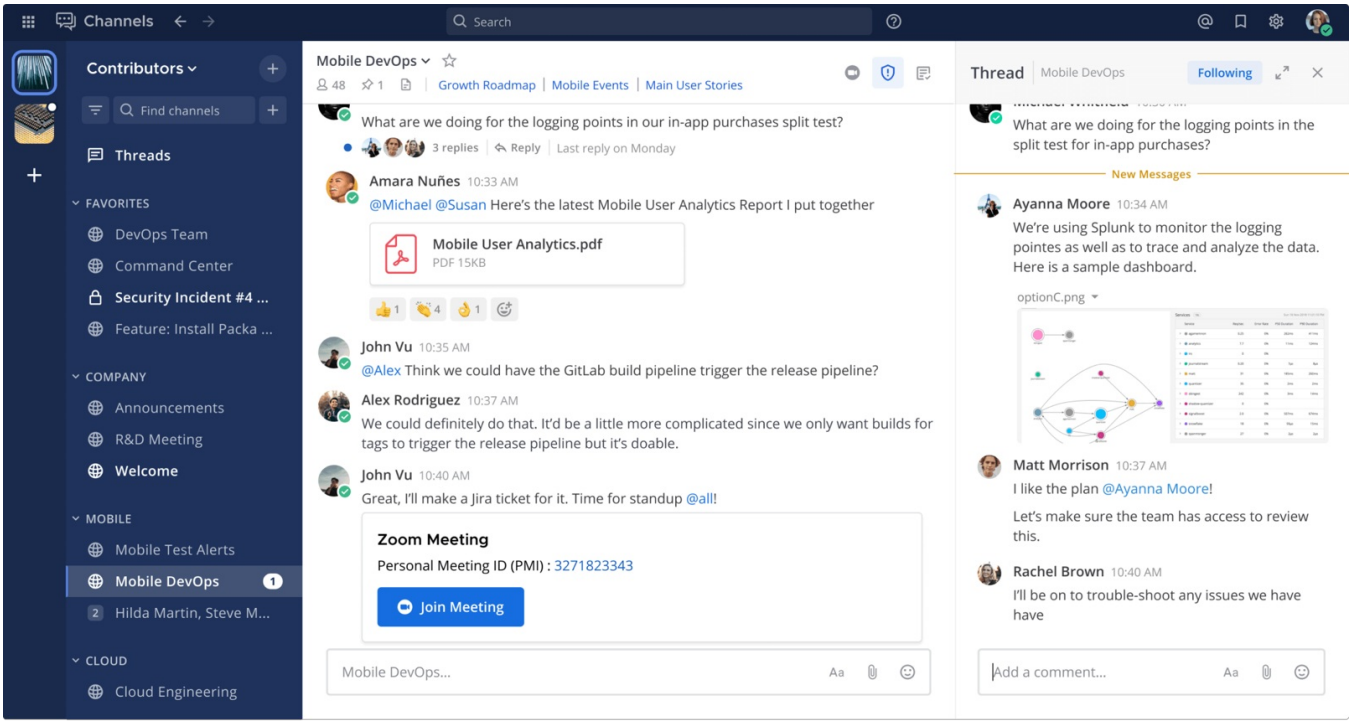
4.10.1 Instant Messaging

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform



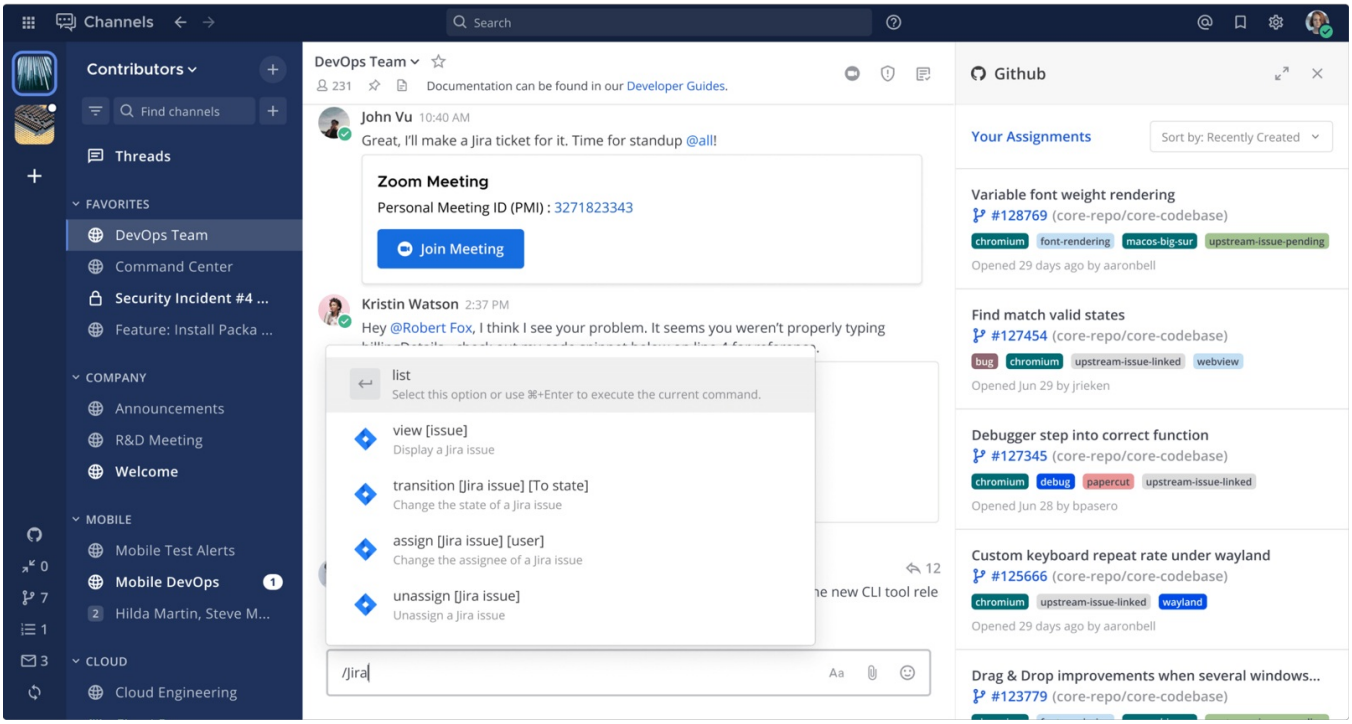


Figura 42 – Instant Messaging Service

4.10.1.1 Service Description

It is a messaging and collaboration platform based on the Mattermost solution that offers secure tools for team communication, file sharing, and integration with other applications, supporting productivity in distributed work environments.
It allows you to organize all team communications in one place via channels. In addition to standard messaging, channels support automation, slash commands, bot integrations, code snippets, and more.
Suitable for environments with high security, privacy, and control requirements. It supports multi-factor authentication, Active Directory, LDAP, SSO, and more.
The platform can be customized and extended by integrating it with the tools your team uses daily.

The service is offered with the following unit metric: *1000 users*.

4.10.1.2 Features and Advantages

The service offers the following main features:

- *Playbooks* → playbooks allow you to orchestrate work across tools and teams. They are prescribed workflows that support specific digital operations scenarios.
- *Audio calls* → it offers native audio calls on channels.
- *Integrations and customizations* → support for slash commands, bots, and inbound and outbound webhooks; extensive ecosystem of plugins and integrations; extensive APIs for extending functionality or building custom applications.
- *Accessibility* → cross-platform clients (web, desktop, mobile); Deployable behind firewalls/in private, air-gapped environments.
- *Security, Privacy, and Governance* → support for: encryption (in transit, at rest); Access control (Single Sign-On MFA, granular roles and permissions); Governance, privacy, and compliance; Zero Trust policy.

The main components of the service are:

- *Backend server* → can use MySQL or PostgreSQL as a database) that hosts messages, users, and files.
- *Storage for file attachments, images, etc.* → can be local or cloud-based (S3, MinIO, etc.).
- *WebSocket channels* → for real-time message transmission.
- *Configurable for scalability* → cluster support, high availability, deployment on Kubernetes, isolated networks.

The service offers the following advantages:

- *Complete data control* → useful for regulated sectors (finance, public administration, healthcare).
- *Reduced lock-in* → open source/source-available, no dependency on proprietary vendors.

- *Compliance and governance* → audit trail, retention policy, exports for legal and regulatory controls
- *Support for secure remote working* → mobile/desktop access with encryption and strong authentication.
- *Adaptable to different sectors* (legal, manufacturing, public administration, tech) thanks to customization options.
- *Extensive APIs and plugins* → extensive integration options with DevOps, CI/CD, ticketing, monitoring.
- *Advanced security* → SSO (SAML, LDAP, OIDC), MFA, encryption in transit and at rest Scalability → clustering, load balancing, support for enterprise and mission-critical environments.

4.11 Database Family

Below is the list of services belonging to the Database family:

- PaaS SQL - PostgreSQL
- PaaS SQL - MariaDB
- PaaS SQL - MS SQL Server EE
- PaaS SQL - MS SQL Server EE (BYOL)
- PaaS GraphDB
- PaaS NoSQL - MongoDB
- PaaS In Memory - Redis

4.11.1 PaaS SQL - PostgreSQL

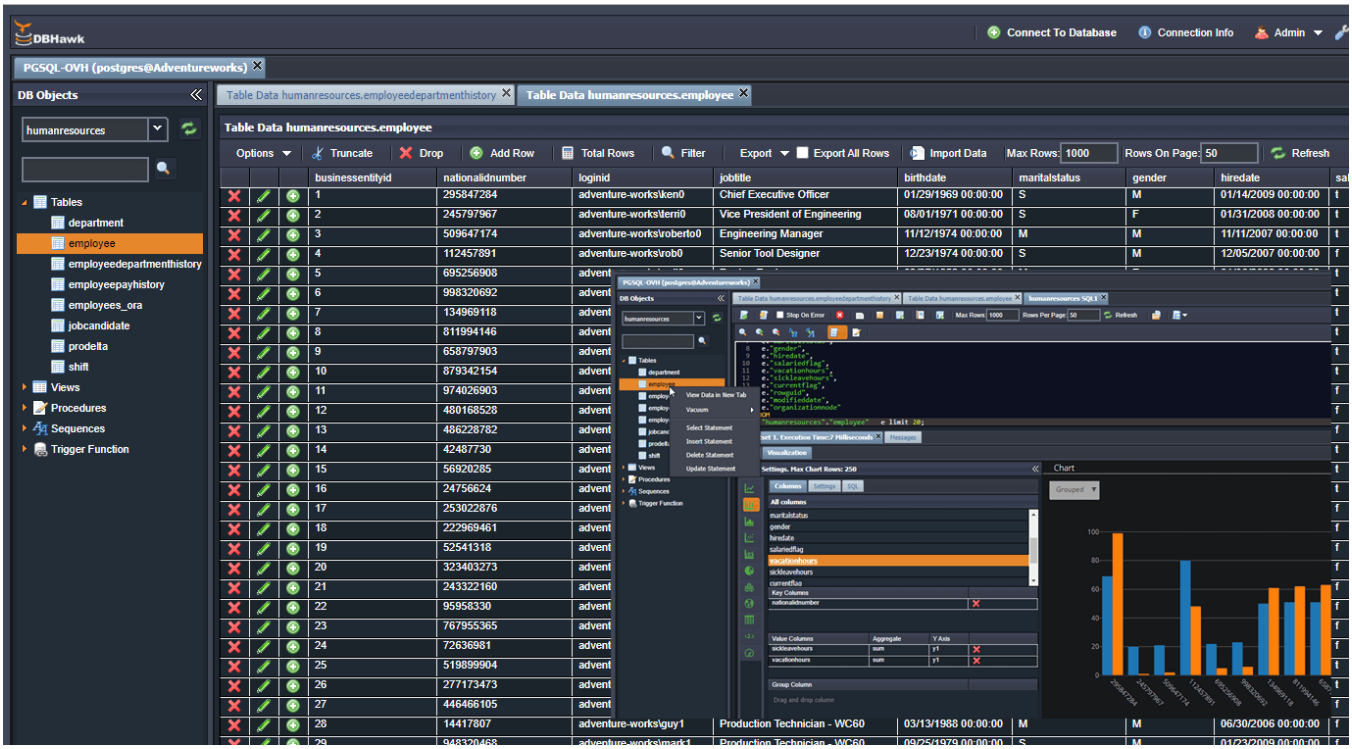


Figura 43 – PostgreSQL client interface

4.11.1.1 Service Description

The PaaS SQL – PostgreSQL is a cloud-based managed platform that provides ready-to-use PostgreSQL database instances without requiring the user to install, configure, or maintain the underlying infrastructure.
In essence, it delivers PostgreSQL “as a service”, allowing developers and organizations to focus on application development and data management instead of database administration.
PostgreSQL in a highly available configuration is a reliable solution for organizations seeking an open source database with performance, security, and scalability. This service is ideal for applications that require reliability without the costs of commercial database solutions.

The service could be used to:

- Host and manage relational databases in the cloud.
- Store and query structured data efficiently.
- Support applications that need high availability, scalability, and data integrity.
- Simplify DevOps workflows by automating database management tasks.
- Integrate easily with other cloud services (analytics, AI, APIs, etc.).

The service is offered per DB instance. Each instance with replication consists of:

- 4 vCPUs
- 16 GB of RAM

4.11.1.2 Features and Advantages

The service offers the following main features:

- *Fully managed service* → semplify provisioning, configuration, patching, and upgrades.
- *Scalability* → vertical and horizontal scaling of compute and storage resources as needed.
- *High availability and reliability* → built-in replication, automatic failover, and multi-zone deployment options.
- *Backup and recovery* → automated backups, point-in-time restore, and disaster recovery capabilities.
- *Security and compliance* → data encryption (in transit and at rest), identity and access management (IAM), network isolation (VPC/Private Link), and compliance certifications (e.g., GDPR, ISO, SOC).
- *Performance optimization* → query optimization, connection pooling, caching, and monitoring tools.
- *Monitoring and alerting* → integration with dashboards and metrics (CPU, memory, I/O, query performance). *Integration and extensibility* → compatible with PostgreSQL extensions (e.g., PostGIS, pg_partman, pg_stat_statements). API and CLI tools for management and automation.

The main components of the service are:

- *Control Plane* → it is the part of the service that manages the lifecycle and orchestration of database instance. Composed by: API, provisioning, configuration, monitoring
- *Data Plane* → it is the layer where PostgreSQL instances actually run. Each instance can be isolated in a VM, container, or pod, depending on the implementation
- *HA & Resilience* → it ensures that the service remains available even in the event of hardware or software failures. It implements replications, failovers and backups policies.
- *Security layer* → it ensures data protection and access control for respecting of the protection & compliance policies: authN/AuthZ, encryption, firewalls, auditing
- *Observability Layer* → It provides visibility and continuous management of the service, offrering monitoring & operations like metrics, logging, auto-patching.

The service offers the following advantages:

- *Cost Efficiency* → no hardware or infrastructure investment. Reduced operational costs: no need for DBA teams to handle maintenance, patching, or scaling manually.
- *Faster Time-to-Market* → database instances can be provisioned quickly through a web interface or API. Ideal for rapid development, prototyping, and product launches. Reduces dependency on infrastructure provisioning cycles.

- *Business agility and scalability* → elastic scaling of resources (CPU, RAM, storage) without downtime. Easily adapts to varying workloads and seasonal demand. Enables agile business models, including microservices and cloud-native architectures.
- *Increased reliability and availability* → High Availability (HA) and automated failover mechanisms ensure continuous uptime. Built-in replication and backup policies protect against data loss. Improves business continuity and reduces downtime risk.
- *Focus on Core Business* → the organization focuses on application development and innovation, not on database administration. Simplifies the technology stack and reduces management overhead.
- *Compliance and Risk Reduction* → the service provider ensures security, patching, and compliance with standards. Reduces risk of configuration errors or unpatched vulnerabilities.
- *Standardization and portability* → based on open-source PostgreSQL, ensuring compatibility and avoiding vendor lock-in. Databases can be exported or migrated easily to other PostgreSQL environments. Supports extensions and features like PostGIS, JSONB, and logical replication.

4.11.2 PaaS SQL - MariaDB

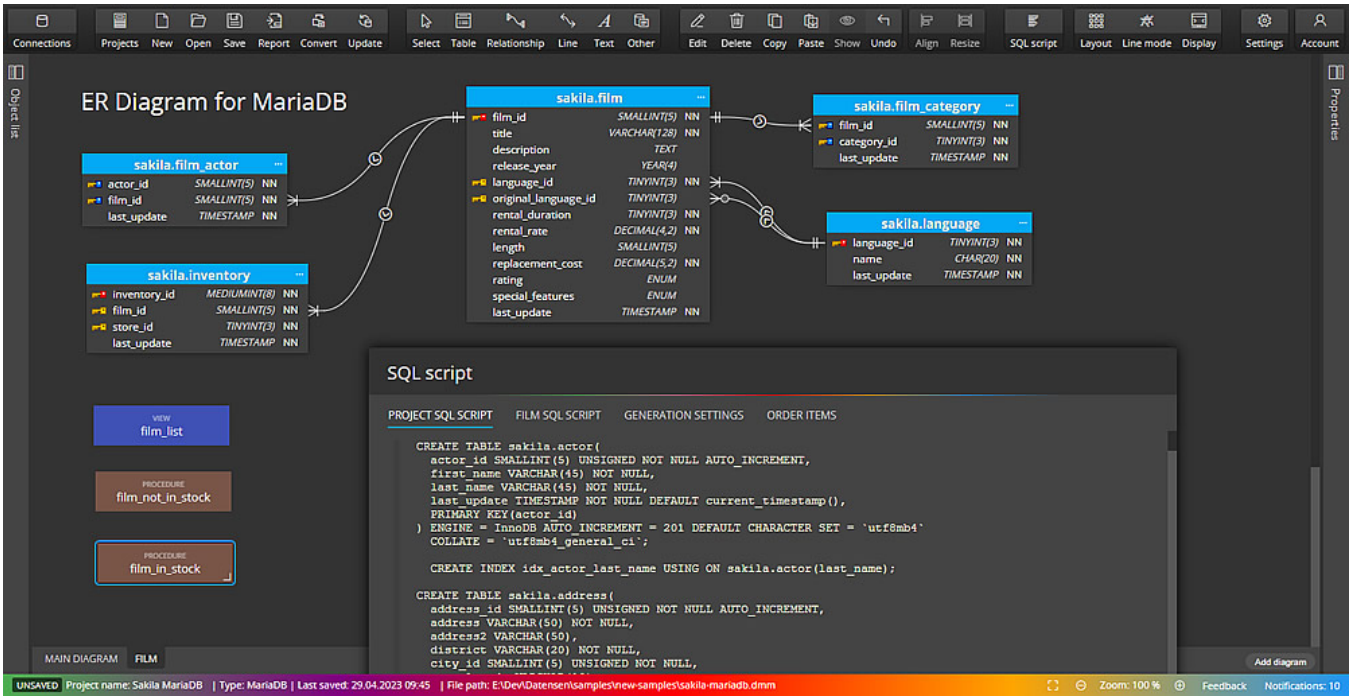


Figura 44 – MariaDB client interface

4.11.2.1 Service Description

The PaaS SQL – MariaDB is a managed Database-as-a-Service (DBaaS) offering that provides fully managed MariaDB database instances in the cloud.
It abstracts away the complexity of infrastructure, deployment, and database administration, allowing users to focus on application development rather than operational maintenance.
The service handles provisioning, configuration, patching, backups, scaling, monitoring, and high availability of MariaDB databases.
The PaaS SQL – MariaDB service is designed to support:

- Web applications and enterprise systems that require a relational SQL database.
- Developers who need quick and consistent access to production-ready databases without managing servers.
- Organizations aiming to reduce database maintenance overhead and improve performance, reliability, and security.

Typical use cases:

- Backend databases for web portals, CMS, ERP, CRM, or e-commerce systems.
- Data storage for microservices or APIs.
- Development and testing environments.
- Data analytics and reporting using SQL queries.

The service is offered per DB instance. Each instance with replication consists of:

- 4 vCPUs
- 16 GB of RAM

4.11.2.2 Features and Advantages

The service offers the following main features:

- *Fully managed lifecycle* → automated provisioning, configuration, updates, and patching. Backups and restores scheduled and managed by the platform. Monitoring and alerting for performance and availability.
- *High availability & reliability* → native MariaDB replication for redundancy. Automatic failover between primary and replica nodes in case of failure. Point-In-Time Recovery (PITR) for data protection. Backups stored on redundant storage systems.
- *Scalability* → vertical scaling: increase CPU, memory, or storage capacity dynamically. Horizontal scaling: optional read replicas for load distribution. Elastic scaling with minimal downtime.
- *Security* → data encryption at rest and in transit (SSL/TLS). Authentication and authorization with role-based access control. Network isolation via virtual private networks (VPC/VNet). Audit logging for security and compliance.

- *Performance optimization* → built-in query optimization and caching. Configurable parameters (buffers, thread pools) based on service tiers. SSD-backed storage for low-latency I/O. Connection pooling and resource limits to prevent overload.
- *Monitoring and integration* → real-time metrics and dashboards (CPU, I/O, connections, slow queries). Integration with external tools like Prometheus, Grafana, or APM systems. REST API and CLI for automation and DevOps pipelines.

The PaaS SQL MariaDB service is organized into multiple logical layers, each responsible for specific functions within the system.

- *Control plane (Management Layer)* → this layer manages the lifecycle and orchestration of MariaDB instances.
- *Data Plane (Execution Layer)* → this layer hosts and executes the actual MariaDB database workloads.
- *HA & resilience layer* → ensures fault tolerance and continuity of service.
- *Security & Access layer* → provides protection, compliance, and controlled access.
- *Observability & operations layer* → provides visibility, maintenance, and automation tools for both provider and customer.

The service offers the following advantages:

- *Cost efficiency* → no hardware or infrastructure investment. Reduced operational costs: no need for DBA teams to handle maintenance, patching, or scaling manually.
- *Faster Time-to-Market* → database instances can be provisioned quickly through a web interface or API. Ideal for rapid development, prototyping, and product launches. Reduces dependency on infrastructure provisioning cycles.
- *Business agility and scalability* → elastic scaling of resources (CPU, RAM, storage) without downtime. Easily adapts to varying workloads and seasonal demand. Enables agile business models, including microservices and cloud-native architectures.
- *Increased reliability and availability* → High Availability (HA) and automated failover mechanisms ensure continuous uptime. Built-in replication and backup policies protect against data loss. Improves business continuity and reduces downtime risk.
- *Focus on core business* → the organization focuses on application development and innovation, not on database administration. Simplifies the technology stack and reduces management overhead.
- *Compliance and risk reduction* → the service provider ensures security, patching, and compliance with standards. Reduces risk of configuration errors or unpatched vulnerabilities.
- *Standardization and portability* → based on open-source PostgreSQL, ensuring compatibility and avoiding vendor lock-in. Databases can be exported or migrated easily to other MariaDB environments.

4.11.3 PaaS SQL - MS SQL Server EE

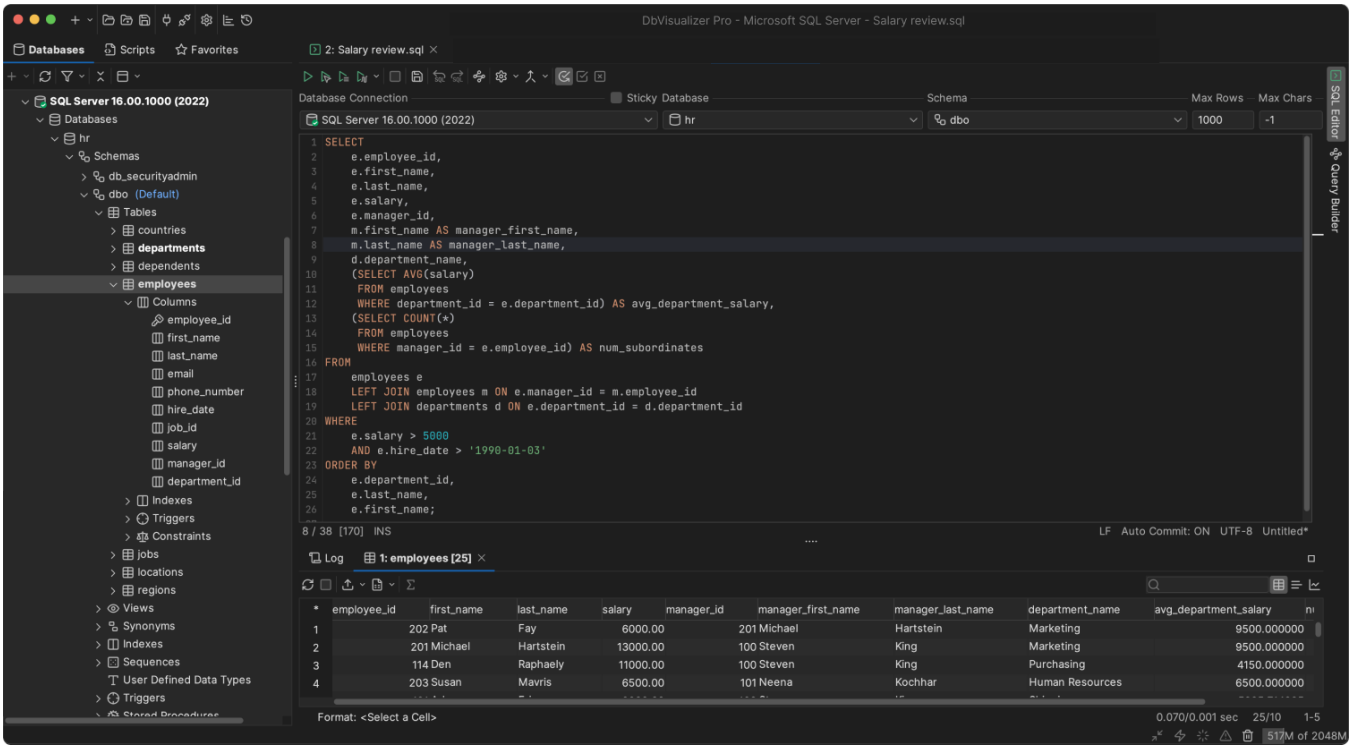


Figura 45 – SQL Server EE client interface

4.11.3.1 Service Description

The PaaS SQL – Microsoft SQL Server Enterprise Edition (EE) service is a fully managed relational database platform that delivers the capabilities of Microsoft SQL Server EE in a cloud-based, Platform-as-a-Service (PaaS) model.
It provides users with dedicated or shared SQL Server instances, managed and operated by the service provider, while abstracting away all infrastructure management tasks such as provisioning, patching, scaling, backup, and high availability.
The service offers enterprise-grade database performance, security, and resilience, optimized for mission-critical workloads and advanced analytics.
This service is designed to support enterprise and business-critical applications that require reliable, scalable, and high-performance SQL database functionality without the operational overhead of managing on-premises infrastructure. Typical use cases include:

- Core enterprise systems (ERP, CRM, SCM).
- Business intelligence (BI) and data warehousing workloads.

- Transactional applications (OLTP) and mixed OLAP/OLTP environments.
- Data integration and analytics pipelines using SQL Server Integration Services (SSIS) or Analysis Services (SSAS).
- Applications requiring high availability, disaster recovery, and compliance assurance.

The service is offered per DB instance. Each instance consists of:

- 8 vCPUs
- 16 GB of RAM

4.11.3.2 Features and Advantages

The service offers the following main features:

- *Fully managed service* → managing of provisioning, patching, configuration, version upgrades, monitoring, maintenance, and optimization. Integration with management portals and APIs for self-service database operations.
- *High availability and disaster recovery* → always on Availability Groups (AG) for real-time replication and automatic failover. Built-in geo-replication and multi-zone deployment for business continuity Point-In-Time Restore (PITR) from continuous transaction log backups.
- *Scalability and elasticity* → vertical scaling: adjust compute, memory, and storage resources dynamically. Read replicas: enable workload offloading for reporting or analytics. Elastic pools for cost-effective management of multiple databases with variable load patterns.
- *Enterprise performance and optimization* → advanced query optimization via Query Store, Adaptive Query Processing, and Columnstore Indexes. In-Memory OLTP and Buffer Pool Extension for high-performance transactions. SSD or NVMe-backed storage for low-latency I/O. Intelligent workload tuning and automatic statistics maintenance.
- *Security and compliance* → Transparent Data Encryption (TDE) and always encrypted. Integration with Active Directory (AD) and Azure AD for identity and role management. Row-Level Security, Dynamic Data Masking, and Auditing. Compliance with cyber security standards.
- *Analytics and integration* → support for SQL Server Analysis Services (SSAS) for OLAP cubes and data modeling. SQL Server Integration Services (SSIS) for ETL and data movement. SQL Server Reporting Services (SSRS) for enterprise reporting. Integration with Power BI, Azure Synapse, and other analytics ecosystems.
- *Monitoring and automation* → integrated dashboard and alerting system with real-time metrics on performance, connections, and query activity. Full API and CLI support for automation and DevOps integration. Logs and metrics exportable to external observability tools.

The main components of the service are:

- *Control plane (Management layer)* → it is responsible for orchestration, automation, and lifecycle management of SQL Server instances.
  Key Components: Management API / Portal, Provisioning engine, Configuration manager, Monitoring & metrics collector, Billing & subscription manager.
- *Data plane (Execution layer)* → it hosts the actual Microsoft SQL Server EE instances where user databases reside and operate.
  Key Components: SQL Server instances, Storage subsystem, Networking layer, Backup and recovery service.
- *High Availability & Resilience layer* → ensures the database service remains available and fault-tolerant.
  Key Components: Always On Availability Groups (AG), Failover controller, Geo-replication manager, Backup orchestrator.
- *Security & Access layer* → provides protection, compliance, and controlled access to data and administrative functions.
  Key Components: Authentication & authorization (integration with AD/Azure AD, support for MFA), Encryption Services (TDE, SSL/TLS, and Always Encrypted for data protection), Network Security.
- *Observability & Operations layer* → ensures visibility, performance optimization, and operational maintenance.
  Key Components: Performance monitoring, Alerting & incident management, Auto-patching System, Maintenance scheduler, Logging system.

The service offers the following advantages:

- *Reduced Total Cost of Ownership (TCO)* → eliminates capital expenses for hardware, networking, and software licensing.
- *Faster Time-to-Market* → databases can be provisioned quickly. Preconfigured and optimized SQL Server templates accelerate development and deployment cycles. Ideal for agile, DevOps, and CI/CD environments where rapid iteration is required.
- *Enterprise-grade reliability and availability* → built on SQL Server Enterprise Edition features such as Always On Availability Groups and In-Memory OLTP. Ensures continuous service availability with automatic failover and disaster recovery. Meets strict SLA targets for uptime and data durability.
- *Business agility and scalability* → scale compute, memory, and storage resources up or down without downtime. Supports variable workloads — from transactional processing to analytics — under a single service model. Allows businesses to expand globally through geo-replication and multi-region deployments.
- *Focus on core business Value* → offloads infrastructure management and DBA operations to the service provider. Frees internal teams to focus on data strategy, analytics, and business intelligence. Accelerates digital transformation by integrating seamlessly with enterprise and cloud ecosystems (e.g., Power BI, Azure, SAP).
- *Compliance and Governance* → enterprise-grade auditing, encryption, and access control meet global compliance standards. Provider-managed patching and updates reduce security and compliance risks. Supports fine-grained access policies and role-based authorization for regulated industries.

4.11.4 PaaS SQL - MS SQL Server EE (BYOL)

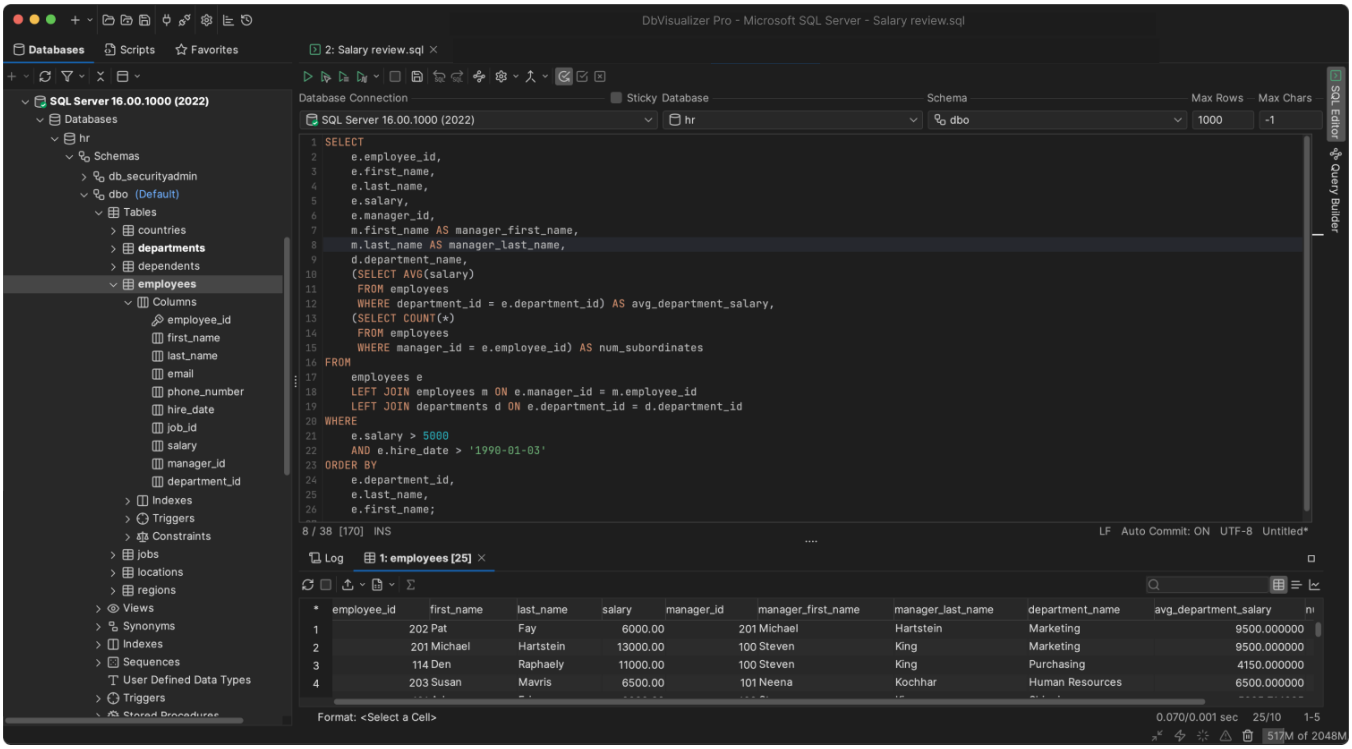


Figura 46 – SQL Server EE client interface

4.11.4.1 Service Description

This service allows organizations to utilize their own licenses for MS SQL Server Enterprise Edition, reducing licensing costs while benefiting from fully managed and optimized management in the cloud.

For all the details , please refer to the PaaS SQL - MS SQL Server EE.

The service is offered per DB instance. Each instance consists of:

- 8 vCPUs
- 16 GB of RAM

4.11.4.2 Features and Advantages

For all the details , please refer to the PaaS SQL - MS SQL Server EE.

4.11.5 PaaS GraphDB

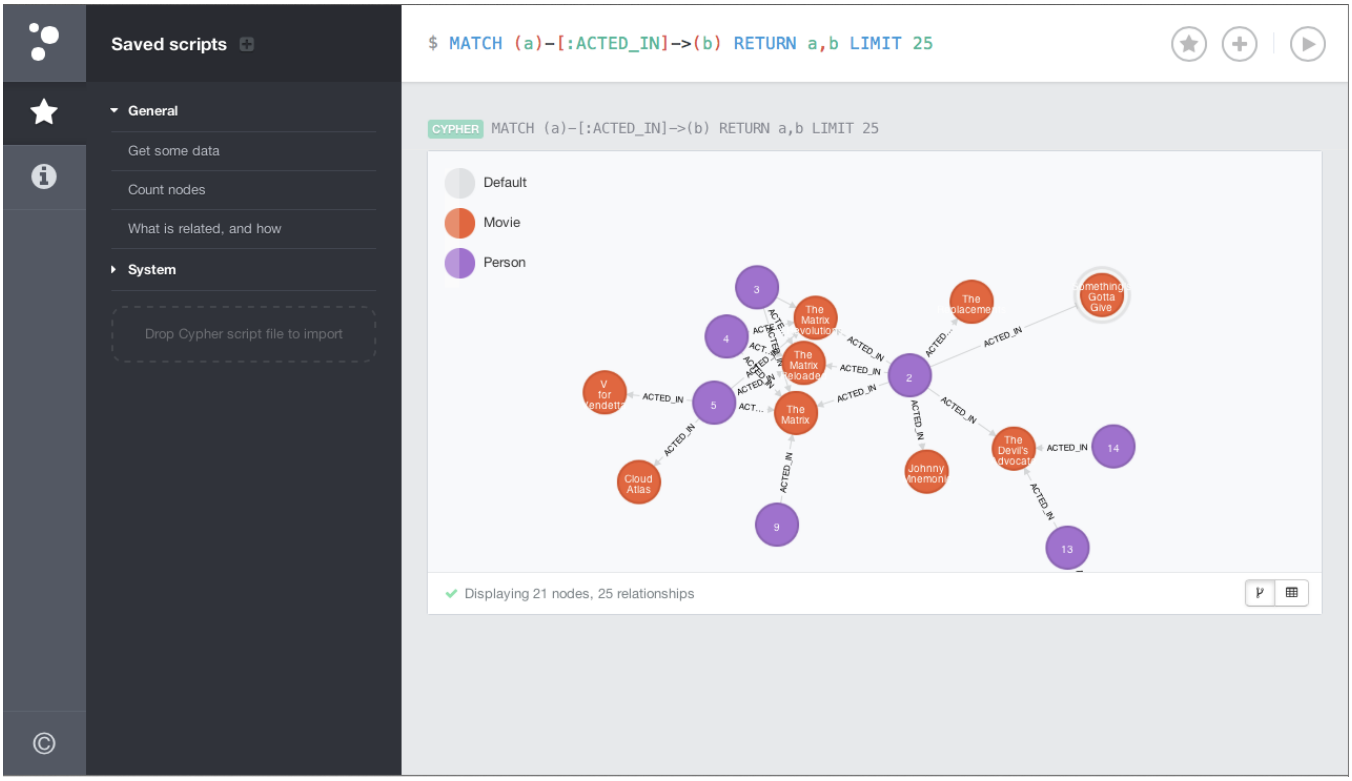


Figura 47 – GraphDB client interface

4.11.5.1 Service Description

The PaaS Graph Database (GraphDB) service, Neo4j-based, is a fully managed, cloud-based graph database platform designed to store, query, and analyze data based on complex relationships and interconnected structures. Unlike traditional relational databases that rely on tables and joins, a GraphDB represents data as nodes (entities) and edges (relationships), allowing for efficient traversal and querying of complex networks — such as social connections, knowledge graphs, fraud detection systems, and recommendation engines.
As a Platform-as-a-Service (PaaS) offering, the GraphDB service automates all operational tasks, including provisioning, configuration, scaling, patching, backups, and monitoring, enabling developers and data scientists to focus solely on building graph-powered applications without managing the underlying infrastructure.
The PaaS is intended for organizations and developers that need to manage and query highly connected data with low latency and high flexibility.
It provides native graph storage and querying capabilities optimized for real-time relationship exploration, graph analytics, and pattern matching across large datasets. Common use cases include:

- Social networks: modeling user interactions, followers, and communities.

- Recommendation systems: deriving product, content, or connection suggestions based on relationships.
- Fraud detection: identifying suspicious transaction patterns and entity links.
- Knowledge graphs: semantic search, ontology management, and enterprise metadata modeling.
- Network and IT operations: modeling dependencies and topology in complex infrastructures.
- Master Data Management (MDM): representing relationships between people, organizations, and assets.

The service is offered per DB instance. Each instance consists of:

- 4 vCPUs
- 16 GB of RAM

4.11.5.2 Features and Advantages

The service offers the following main features:

- *Fully managed service* → managing of provisioning, configuration, patching, and scaling of graph database clusters. Continuous monitoring and proactive maintenance. Built-in backup, restore, and snapshot management with defined retention policies.
- *Native graph model support* → supports both property graphs (e.g., Neo4j-compatible) and RDF graphs (semantic web standards). Enables flexible schema or schema-less design, allowing dynamic evolution of data models. Optimized for deep traversal queries, shortest-path calculations, and pattern matching.
- *High performance and scalability* → distributed architecture for horizontal scaling across multiple nodes.In-memory caching and optimized graph storage for high-speed traversals. Load balancing across query engines and replicas to ensure consistent performance. Low-latency graph query execution for complex relationship analysis.
- *High availability and fault tolerance* → clustered deployment with data replication across nodes or availability zones. Automatic failover and leader election for continuous service operation. Configurable consistency levels for balancing performance and data safety. Backup and Point-In-Time Recovery (PITR) options.
- *Advanced Querying and Analytics* → native support for graph query languages such as Cypher, Gremlin, SPARQL, or GraphQL extensions. Integration with graph analytics engines for algorithms like PageRank, community detection, and pathfinding. Full-text search and indexing capabilities for metadata and relationship attributes. Support for APIs and drivers in multiple languages (Python, Java, Node.js, Go).
- *Security and compliance* → encryption of data at rest and in transit (TLS/SSL). Authentication and authorization via IAM integration, role-based access control (RBAC), and fine-grained permissions. Network isolation with private endpoints, firewall rules, and VPC/VNet integration. Audit logging, compliance with GDPR, ISO 27001, and SOC 2 standards.
- *Integration and interoperability* → connectors and APIs for integration with data pipelines, ETL tools, and machine

learning platforms. REST, GraphQL, or Bolt endpoints for application access. Integration with BI tools and data visualization frameworks for relationship exploration. Support for data federation and linking external data sources (SQL, NoSQL, RDF stores).

The main components of the service are:

Control plane (Management and orchestration layer) → this layer provides centralized control over the provisioning, configuration, and lifecycle management of GraphDB clusters.
Key Components: Management API / Portal; Provisioning engine for automates deployment of graph database clusters across compute nodes; Configuration manager; Metrics & monitoring collector; Billing & quota manager for tracks usage (storage, query operations, nodes) and enforces subscription limits. - *Data Plane (Execution layer)* → this layer hosts the actual graph databases and query processing engines that execute user workloads.
Key Components: Graph Database engine nodes for executing queries and maintain graph data structures, Storage layer; Query engine that interprets and executes graph query languages (Cypher, SPARQL, Gremlin); Replication layer that synchronizes data across nodes for high availability and consistency; Networking Layer for secure communication via private endpoints and load balancers. - *High availability and resilience layer* → ensures service continuity, fault tolerance, and disaster recovery.
Key Components: Cluster Manager for coordinating replication, partitioning, and failover across graph nodes; Backup & Recovery Manager that schedules automated backups and handles restoration processes; Failover controller; Geo-replication service that replicates graph data across regions or availability zones for disaster recovery. - *Security & Access layer* → responsible for user authentication, authorization, encryption, and compliance management.
Key Components: Identity and Access Management (IAM); Encryption services; Access control policies; Audit logging system - *Observability & Operations layer* → provides visibility, automation, and operational maintenance for both administrators and users.
Key Components: Monitoring system; Alerting & incident management; Logging Service; Auto-patching & Upgrades; Maintenance scheduler that orchestrates backup, cleanup, and optimization tasks.

The service offers the following advantages:

- *Accelerated Time-to-Value* → rapid deployment of fully managed GraphDB clusters without infrastructure setup. Developers can focus on building relationship-driven applications rather than managing database servers. Preconfigured environments and APIs shorten time-to-market for data-intensive projects.
- *Reduced Total Cost of Ownership (TCO)* → eliminates hardware, networking, and software licensing costs. No need for in-house database administration or maintenance. Reduces hidden operational costs associated with upgrades, backups, and monitoring.
- *Business agility and innovation* → enables rapid experimentation with data relationships, graph analytics, and knowledge models. Scales on demand to handle growth in connected datasets. Supports new business capabilities such as recommendation systems, fraud detection, and semantic search without large upfront investment.

- *Improved decision-making and insight discovery* → provides a 360-degree view of data relationships across entities (customers, products, assets, etc.). Supports advanced analytics, predictive modeling, and data visualization. Helps uncover patterns, correlations, and dependencies that are invisible in traditional relational models.
- *High reliability and continuity* → built-in redundancy and replication ensure continuous service availability. Automated backups, failover, and point-in-time recovery minimize downtime and data loss. Meets enterprise-grade SLAs for uptime and durability.
- *Governance, security, and compliance* → managed security, encryption, and audit logging reduce compliance risks. Role-based access and data isolation protect sensitive relationships and metadata. Provider-managed patching and updates ensure continuous compliance with standards.

4.11.6 PaaS NoSQL - MongoDB

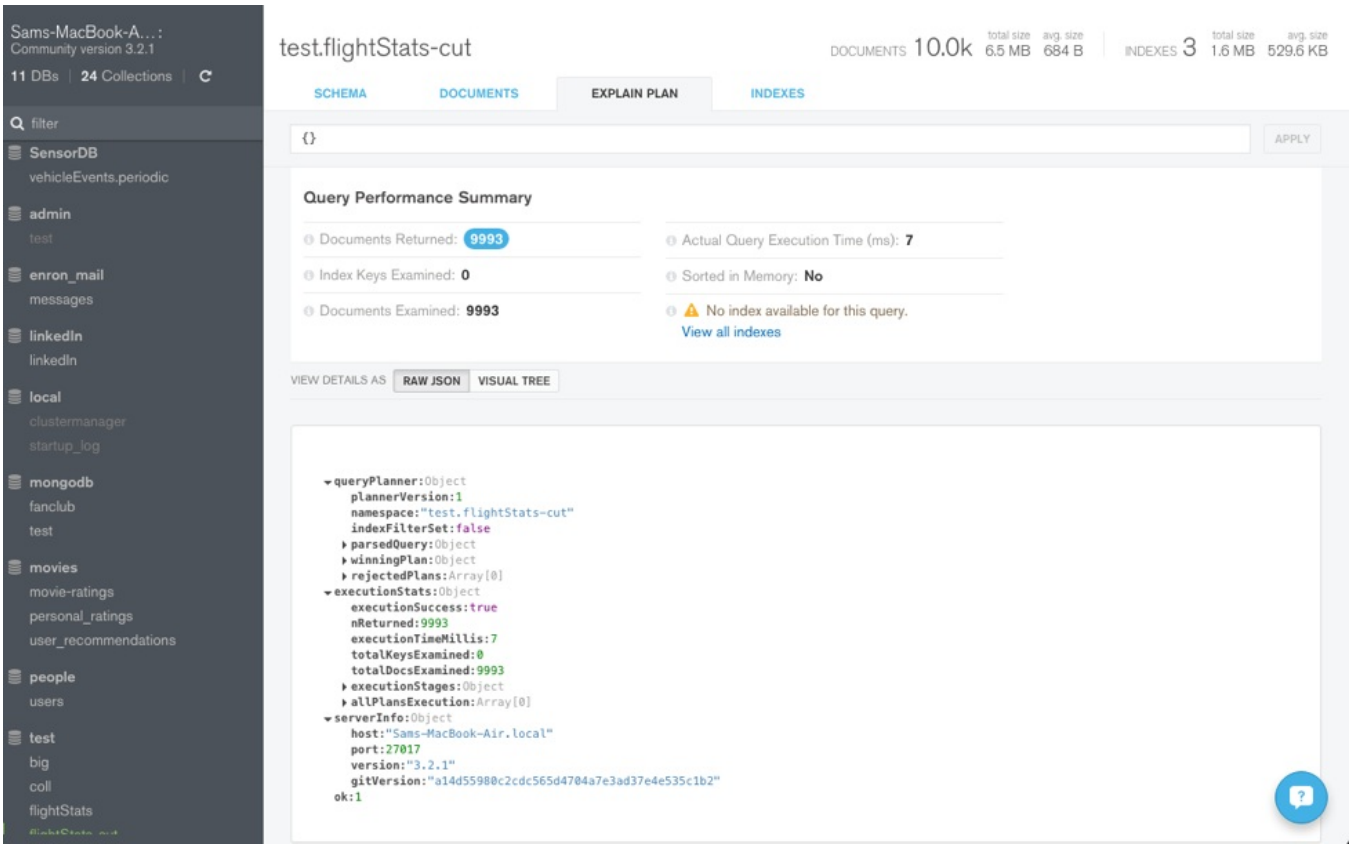


Figura 48 – MongoDB client interface

4.11.6.1 Service Description

The PaaS NoSQL MongoDB service provides a fully managed, cloud-native document database platform designed to handle large volumes of unstructured and semi-structured data.
It enables organizations to deploy and operate MongoDB clusters without managing infrastructure, scaling, or administrative overhead.
Built on the MongoDB engine, the service offers high flexibility in data modeling, seamless horizontal scalability, and advanced features such as replication, sharding, automated backups, and high availability.
The service is designed to support modern, data-driven applications requiring high performance, flexibility, and scalability. It is particularly suited for:

- Web and mobile applications that require dynamic schemas.
- IoT and telemetry systems generating high-volume JSON data.
- Real-time analytics and event processing.
- Content management systems (CMS) and e-commerce platforms.
- Big data pipelines and data lakes needing schema evolution and rapid ingestion.

The service is offered per DB instance. Each instance with replication consists of:

- 4 vCPUs
- 16 GB of RAM

4.11.6.2 Features and Advantages

The service offers the following main features:

- *Fully managed environment* → managing of provisioning, configuration, and maintenance of MongoDB clusters. Continuous patching, upgrades, and resource optimization.Service managed via web console, CLI, or API for full lifecycle operations.
- *Flexible data model* → document-oriented schema using JSON/BSON structures. Supports hierarchical and nested data with dynamic schema evolution. Allows storage of complex data without the rigidity of relational tables. Ideal for agile development and microservices architectures.
- *High performance and scalability* → horizontal scaling through automatic sharding across multiple nodes. Vertical scaling by dynamically increasing compute and memory resources. Built-in read/write replication for high throughput and low latency. Intelligent indexing (single field, compound, geospatial, text, wildcard).
- *High availability and resilience* → replication via Replica Sets for automatic failover and self-healing. Multi-zone deployment for fault tolerance and disaster recovery. Point-in-Time Recovery (PITR) and incremental backups ensure data integrity.
- *Security and compliance* → encryption at rest and in transit.Role-Based Access Control (RBAC) and fine-grained permissions.Integration with enterprise Identity and Access Management (IAM) systems. Auditing, logging, and

monitoring for compliance.

- *Monitoring and observability* → real-time dashboards for performance, resource utilization, and query profiling. Automated alerts and anomaly detection for proactive issue resolution. Integration with observability tools (e.g., Prometheus, Grafana, ELK Stack).
- *Developer tools and integration* → native support for MongoDB Query Language (MQL). APIs, SDKs, and drivers for major programming languages (Java, Python, Node.js, Go, etc.). Integration with CI/CD pipelines and Infrastructure-as-Code tools (Terraform, Ansible). Support for analytics and visualization via BI connectors and data APIs.
- *Backup, restore, and disaster recovery* → scheduled and on-demand backups with retention policies.Point-in-time recovery to mitigate data loss from logical errors. Geo-redundant replication across regions for disaster recovery.

The main components of the service are:

- *Control plane* → manages the provisioning, orchestration, scaling, and lifecycle of MongoDB clusters. Handles user authentication, access control, and billing integration. Provides APIs and UI for tenant management, monitoring, and configuration.
- *Data Plane* (MongoDB cluster layer) → comprises Replica Sets for high availability and Shards for distributed data storage. Each shard consists of multiple replica nodes (primary and secondaries). Mongos routers distribute queries intelligently across shards. Ensures horizontal scalability and automatic data balancing.
- *Storage Layer* → based on high-performance SSD or NVMe storage. Supports data encryption, snapshotting, and incremental backup mechanisms. Abstracted via cloud block storage for elasticity and redundancy.
- *Network and security layer* → implements network isolation via Virtual Private Cloud (VPC) or private endpoints. Firewall rules, IP whitelisting, and security groups restrict access. TLS-based encryption secures data in transit between components and clients. - *Management and monitoring layer* → provides observability, metrics collection, and alerting. Automated performance tuning and resource optimization. Integrates with logging and monitoring frameworks.
- *Backup and disaster recovery layer* → handles snapshot-based backups, replication, and PITR mechanisms. Automated restore operations from cloud object storage. Supports cross-region replication for business continuity.

The service offers the following advantages:

- *Reduced Total Cost of Ownership (TCO)* → eliminates capital investments in servers, storage, and licenses. Shifts database management from internal teams to the provider’s managed service. Reduces operational costs through automation of scaling, patching, and backups.
- *Faster Time-to-Market* → fully managed environment allows databases to be provisioned in minutes. Dynamic schema flexibility accelerates application development. Enables rapid prototyping and iteration, ideal for agile and DevOps workflows.
- *High agility and flexibility* → schema-less document model adapts easily to evolving application requirements.

Ideal for businesses managing heterogeneous or semi-structured data sources. Supports frequent data model changes without downtime or migration overhead.

- *Business continuity and reliability* → enterprise-grade high availability with built-in replication and automatic failover.Continuous backups and geo-redundant disaster recovery ensure data resilience. Meets stringent SLAs for uptime and data durability.
- *Scalability and growth enablement* → seamless horizontal scaling allows the service to handle growing data volumes and workloads. Supports global deployments with low latency through distributed clusters. Enables new data-intensive use cases (IoT, analytics, personalization) without redesigning architecture.
- *Compliance and data governance* → managed patching, auditing, and encryption ensure continuous compliance. Data isolation and access control simplify adherence to european laws. Facilitates transparent governance with built-in monitoring and reporting tools.
- *Focus on core business* → frees internal teams from database management and operational complexity. Allows developers to focus on innovation, application features, and user experience. Accelerates delivery of digital services and customer-facing applications.

4.11.7 PaaS In Memory- Redis

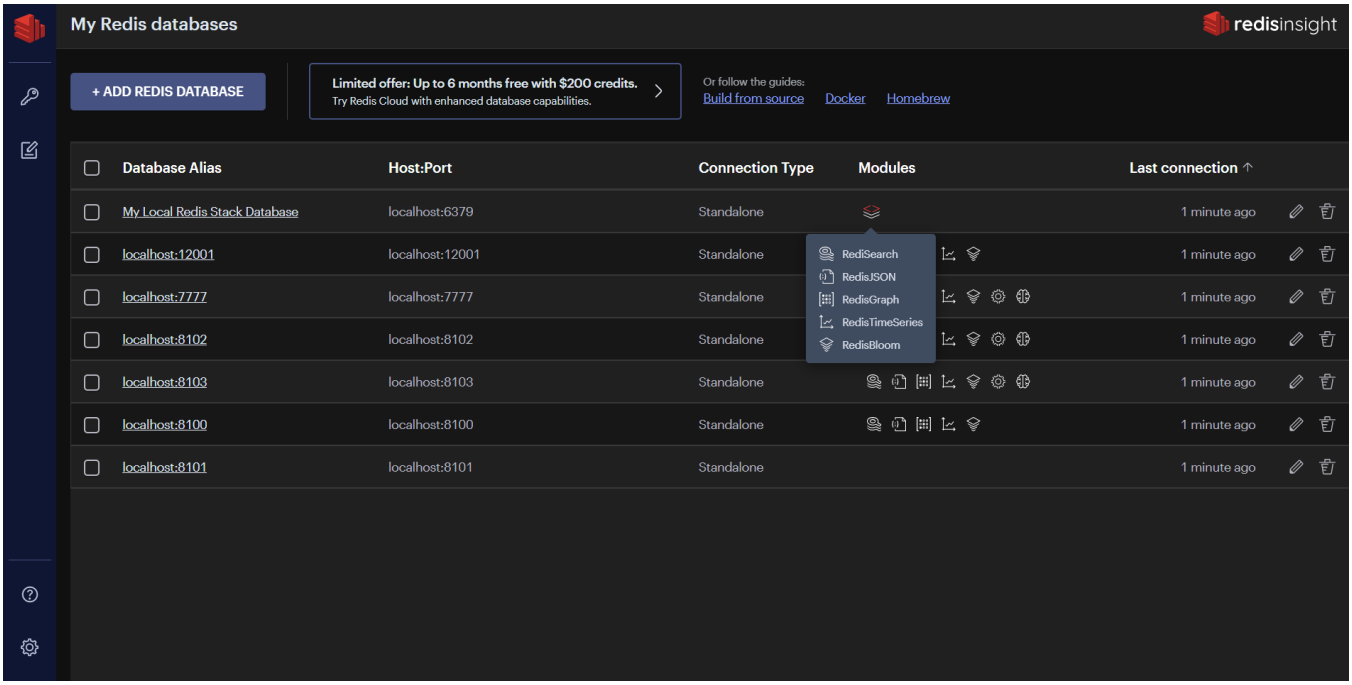


Figura 49 – Redis client interface

4.11.7.1 Service Description

It is a PaaS DB based on Redis technology (Remote Dictionary Server) that exposes a high-performance in-memory database, primarily used as a cache and database for web and real-time applications. Redis is a widely used database due to its flexibility and ability to handle a wide range of data types with low latency.
The service delivers sub-millisecond data access, advanced caching, session management, message streaming, and data persistence capabilities.
As a Platform-as-a-Service (PaaS) offering, it abstracts away the operational complexity of managing Redis clusters — including provisioning, scaling, patching, failover, and monitoring — while ensuring enterprise-grade reliability, security, and performance.

The PaaS Redis service is designed for applications that require extremely fast data access, real-time analytics, and low-latency transactions. Typical use cases include:

- Application caching to reduce latency and offload backend databases.
- Session storage for web and mobile applications.
- Real-time analytics and leaderboards (e.g., gaming, ad tech, telemetry).
- Message queues and event streaming for distributed systems.
- Geospatial data processing and time-series data handling.
- Rate limiting and token management in API gateways.

The service is offered per DB instance. Each instance consists of:

- 4 vCPUs
- 16 GB of RAM

4.11.7.2 Features and Advantages

The main features of the Paas In Memory Redis are:

- *In-memory* → data is stored in RAM, ensurig extremely fast access;
- *Persistence* → supports data persistence on disk, preventing data loss in the event of a system reboot;
- *Data type* → variety of data types, allowing for modeling different types of information;
- *Pub/Sub* → supports the publish/subscribe model for real-time communication between applications.
- *Fully managed platform* → managing of provisioning, patching, scaling, and maintenance. High availability clusters with zero-downtime updates. Self-healing orchestration to ensure continuous service delivery. Management via API, CLI, or Web Console.
- *High performance and low latency* → entire dataset stored in-memory for sub-millisecond access. Optimized for real-time operations requiring microsecond response times. Supports high throughput (millions of operations per second). Persistent storage optional for durability.

- *Flexible data structures* → rich data model beyond simple key-value pairs: strings, hashes, lists, sets, sorted sets. Bitmaps, HyperLogLogs, Streams, and Geospatial Indexes. Ideal for complex operations such as counters, queues, and pub/sub messaging.
- *High Availability and disaster recovery* → native Redis Sentinel or Cluster Mode for automatic failover and fault tolerance. Multi-AZ deployment to ensure continuous uptime. Backup and restore capabilities for data persistence and recovery. Optional geo-replication across regions for disaster recovery.
- *Persistence options* → RDB (Redis Database Backup): Snapshot-based persistence for periodic backups. AOF (Append-Only File): Logs every operation for durability and recovery. Hybrid mode combining both mechanisms for balance between speed and reliability.
- *Scalability and elasticity* → horizontal scaling through Redis Cluster sharding. Vertical scaling with dynamic memory and compute adjustments. Linear scalability for both read and write operations. Automatic rebalancing of data across nodes.
- *Security and compliance* → encryption in transit (TLS) and encryption at rest. Role-Based Access Control (RBAC) and user authentication. Integration with Identity and Access Management (IAM) systems. Continuous auditing, logging, and compliance monitoring.
- *Monitoring and observability* → real-time metrics on throughput, latency, and memory usage. Proactive alerts and anomaly detection. Integration with monitoring stacks (Prometheus, Grafana, ELK). Logging for audit trails and performance tuning.
- *Developer Integration and APIs* → compatible with standard Redis clients and libraries. REST and gRPC APIs for automation and DevOps workflows. Integration with CI/CD pipelines and Infrastructure-as-Code tools (Terraform, Ansible). Supports Redis modules (e.g., RedisJSON, RediSearch, RedisGraph, RedisTimeSeries).

The logical architecture of the PaaS Redis service consists of multiple layers designed for automation, scalability, and resilience.

- *Control plane* → responsible for service orchestration, cluster provisioning, scaling, and lifecycle management. Manages authentication, authorization, metering, and billing. Provides APIs, CLI, and web-based UI for service management.
- *Data Plane (Redis cluster layer)* → Core component that hosts user data in memory. Composed of multiple Redis instances organized as: Master nodes; Replica nodes; Implements sharding for horizontal scalability; Ensures high throughput and low latency for data operations.
- *Storage and persistence layer* → provides optional durable storage for backup and disaster recovery. Utilizes RDB snapshots and AOF logs stored on encrypted block or object storage. Supports automated retention policies and scheduled backups.
- *Networking and security layer* → virtual network isolation using VPC/VNet configurations. TLS-based encryption for client-to-server and inter-node communication. Security groups, IP whitelisting, and firewall rules for controlled access. Optional private endpoints for secure integration with internal systems.

- *Monitoring and Management layer* → aggregates telemetry and performance metrics. Implements logging, tracing, and alerting via monitoring systems. Provides dashboards for capacity planning and SLA tracking.
- *High availability and failover layer* → monitors node health and automatically triggers failover in case of node or zone failure. Uses Redis Sentinel or internal control mechanisms for cluster coordination. Supports synchronous or asynchronous replication for HA and DR.

The service offers the following advantages:

- *Reduced Total Cost of Ownership (TCO)* → no capital investment in hardware, software, or cluster management. Reduces operational overhead by automating deployment, scaling, and maintenance. Eliminates the need for specialized in-house Redis administration skills.
- *Faster Time-to-Market* → instant provisioning of Redis clusters enables rapid development and testing. Ready-to-use configurations optimize caching and real-time processing use cases. Enables teams to integrate low-latency data layers into applications in minutes. Accelerates delivery of digital services requiring immediate responsiveness.
- Improved application performance and user experience → sub-millisecond response times improve customer satisfaction and engagement. Reduces load on backend databases and APIs through caching and data offloading. Ensures consistent performance during traffic spikes or seasonal demand peaks.
- *Business agility and scalability* → easily scales up or down to accommodate fluctuating workloads. Enables dynamic adaptation to new business requirements without architectural redesign. Supports real-time analytics and streaming for modern, data-intensive applications.
- *Reliability and continuity* → built-in replication and failover mechanisms ensure continuous availability. Automated backups and geo-redundancy support robust disaster recovery. Meets enterprise-grade SLA commitments for uptime and data durability.
- *Compliance and security* → provider-managed encryption, patching, and access control ensure compliance with data security standards. Role-based access and network isolation protect sensitive data in-memory and at rest. Reduces compliance risks through centralized governance and auditing tools.
- *Focus on core business innovation* → frees developers and operations teams from managing infrastructure and cluster administration. Allows organizations to focus on value creation, product innovation, and user experience. Enables integration of Redis-based caching and real-time logic into cloud-native architectures effortlessly.

4.12 Networking Family

Below is the list of services belonging to the Networking family:

- Paas CDN (Content Delivery Network)

- PaaS DNS (Domain Name System)
- Single public IP
- L7 Load Balancer (regional)
- Cloud interconnect Gold SW (10 Gbps max throughput)
- Managed VPN Access Service
- PaaS Client/Forward Proxy
- PaaS Reverse Proxy

4.12.1 PaaS CDN (Content Delivery Network)

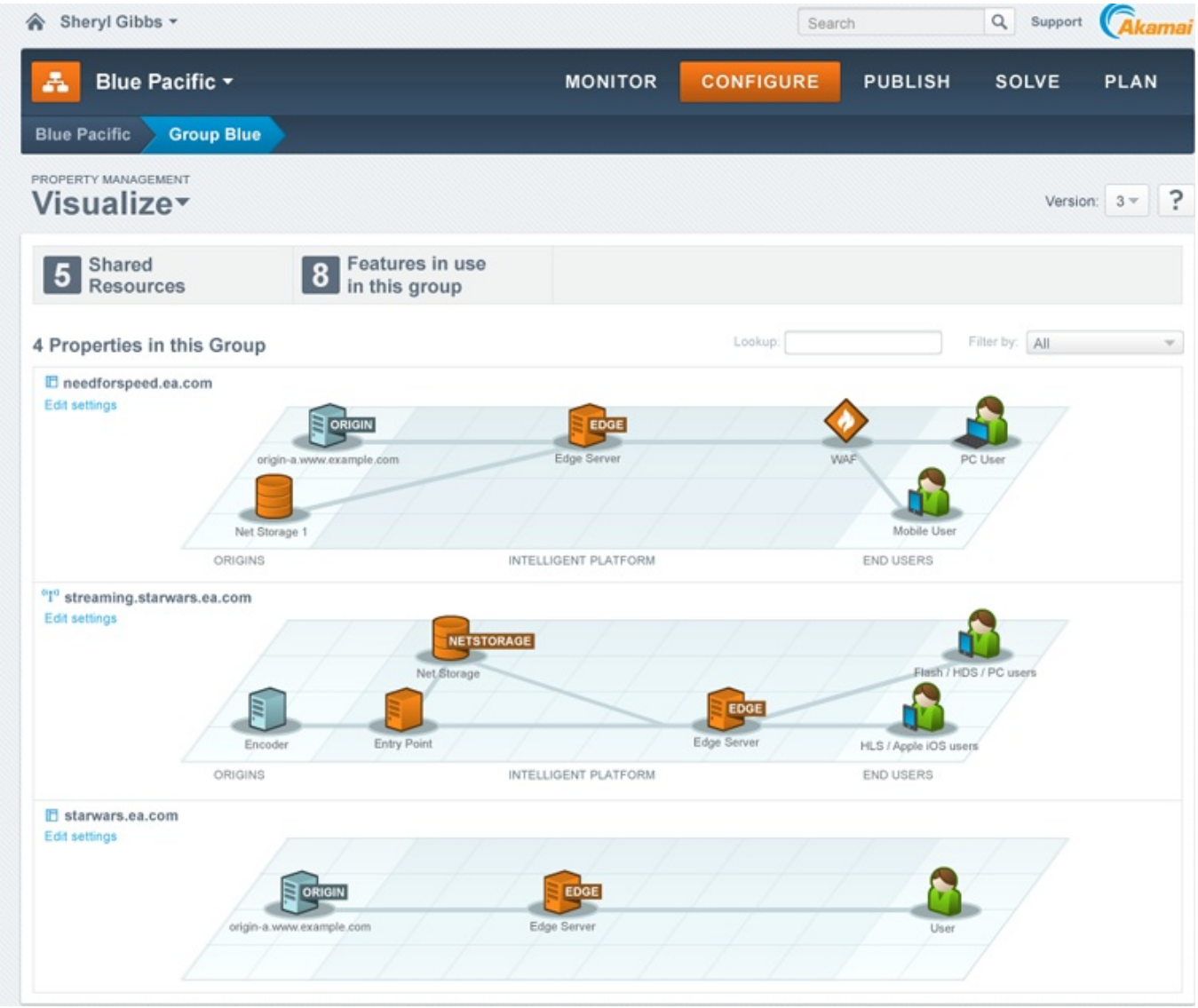


Figura 50 – PaaS CDN (Content Delivery Network) interface

4.12.1.1 Service Description

The PaaS CDN (Content Delivery Network) service based on Nginx memory cache is a cloud-managed platform designed to accelerate content delivery, reduce latency, and ensure high availability for web applications and digital services.
By leveraging Nginx's high-performance caching capabilities—optimized for in-memory operations—the platform delivers ultra-fast retrieval of static and dynamic content.
As a fully managed PaaS offering, it abstracts the complexity of operating CDN infrastructure, providing customers with a scalable, secure, and globally distributed content delivery layer.

The service is offered with the following unit metric: *10 Gbps of throughput (inbound & Outbound)* .

4.12.1.2 Features and Advantages

The main features of the service are:

- *High-Performance In-Memory Caching* → ultra-low latency content delivery powered by Nginx memory cache, ideal for frequently accessed assets.
- *Global Edge Distribution* → multiple distributed PoPs (Points of Presence) to ensure content is served as close to users as possible.
- *Dynamic Content Acceleration* → support for reverse proxy, micro-caching, and intelligent cache rules to optimize dynamic workloads.
- *Load Balancing and Failover* → built-in traffic distribution mechanisms to maintain availability and service continuity.
- *Real-Time Purge and Cache Control* → instant cache invalidation APIs for granular control over content lifecycle.
- *TLS Offloading and Security Filtering* → enhanced security features including HTTPS termination, rate limiting, and request filtering.
- *Centralized Management Interface* → unified portal for configuration, analytics, monitoring, and scaling.

The main components of the service are:

- *Nginx Edge Nodes* → distributed caching servers running Nginx with optimized memory caching for fast content retrieval.
- *Control and Orchestration Layer** → cloud-based management system for provisioning, updating, configuring, and scaling all CDN nodes.
- *Global Routing & Load Balancing* → smart routing algorithms directing users to the nearest or fastest-performing PoP.
- *API Gateway & Cache Management Tools* → APIs for programmatic cache purging, cache rules, routing policies, and provisioning.
- *Monitoring & Analytics Engine* → real-time dashboards providing metrics on latency, cache hit ratio, traffic

patterns, and health status.

- *Security Layer* → integrated HTTPS, WAF options, rate limiting, and request validation at the edge.

The service offers the following advantages:

- *Improved User Experience* → faster load times and reduced latency directly enhance customer satisfaction and engagement.
- *Predictable and Lower Operational Costs* → OPEX-based PaaS model avoids infrastructure investment and reduces maintenance burden.
- *Scalable for Growth* → easily supports increasing traffic volume without service interruptions or rearchitecture.
- *Global Reach with Minimal Effort* → organizations can instantly expand content delivery worldwide without deploying additional infrastructure.
- *Increased Service Reliability* → built-in redundancy and failover ensure business continuity even during traffic spikes.
- *High Performance Through Memory Caching* → in-memory content serving dramatically improves throughput and reduces backend load.
- *Flexible Caching Policies* → support for custom rules, micro-caching, selective purging, and dynamic acceleration.
- *Reduced Origin Server Load* → high cache hit ratios prevent unnecessary upstream requests, improving origin server performance.
- *Optimized for Modern Web Architectures* → compatible with APIs, microservices, SPA frameworks, and containerized environments.
- *Secure by Design* → integrated TLS termination, request filtering, rate limiting, and observability tools protect the delivery pipeline.

4.12.2 PaaS DNS (Domain Name System)

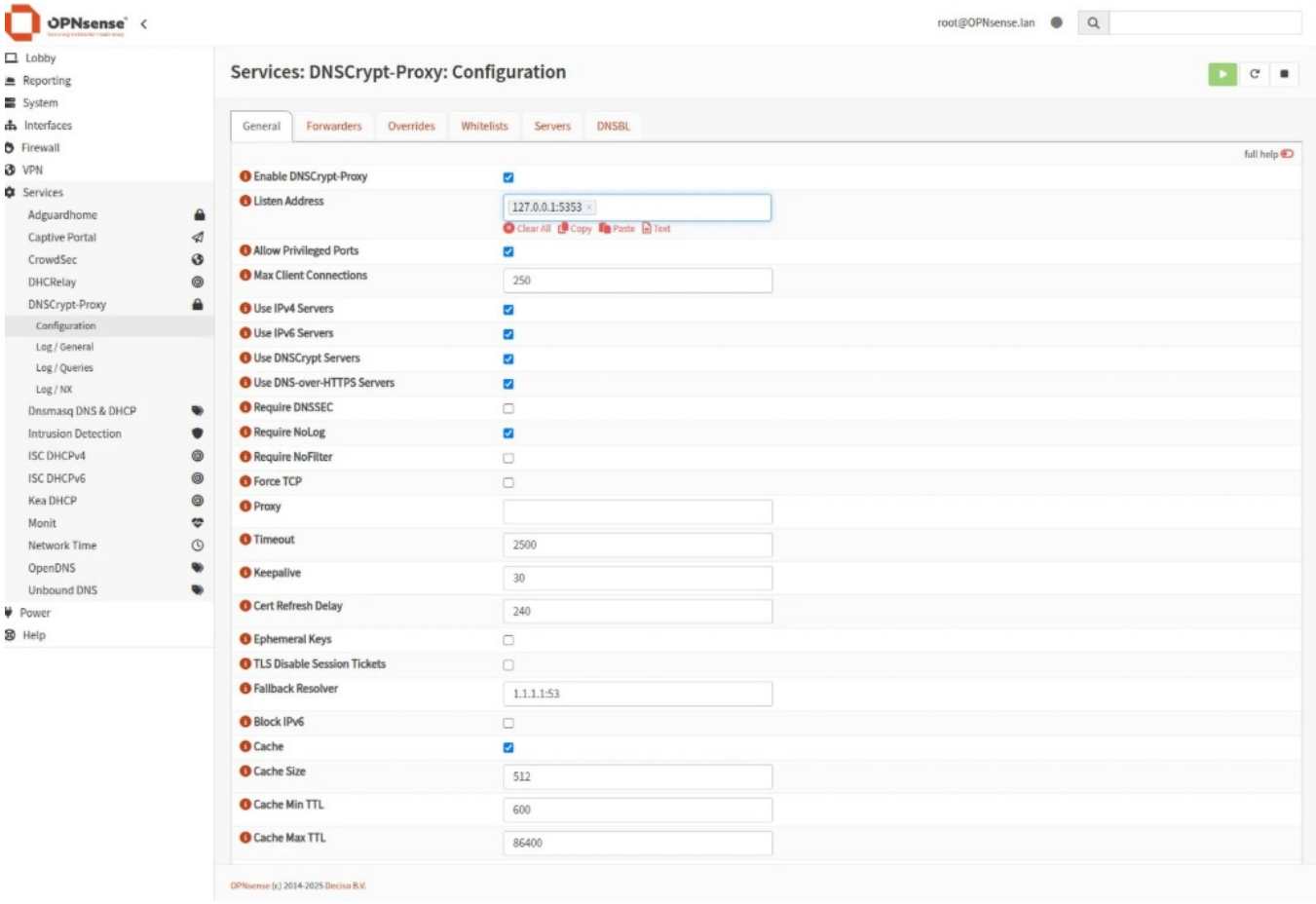


Figura 51 – PaaS DNS (Domain Name System) interface

4.12.2.1 Service Description

The PaaS DSN (Distributed Secure Network) service based on OPNsense provides a cloud-delivered, fully managed network security and routing platform designed for organizations that require scalable, secure, and highly available connectivity.
Built on OPNsense's open-source firewall and security capabilities, this service abstracts infrastructure complexity and offers customers a ready-to-use network environment delivered as a Platform-as-a-Service.
The solution centralizes policy management, simplifies deployment, and ensures consistent security enforcement across distributed sites, remote users, and cloud workloads.

The service is offered for each DNS Instance unit.

4.12.2.2 Features and Advantages

The main features of the service are:

- *Cloud-managed OPNsense firewall instances* → fully managed virtual appliances with automated updates, monitoring, and lifecycle management.
- *Zero-Trust network access* → policy-based access management for users and devices, enabling secure remote connectivity.
- *High Availability & scalability* → cluster configurations, automated failover and elastic capacity provisioning.
- *Centralized configuration & orchestration* → unified control panel for managing rules, VPNs, routing, and monitoring across multiple nodes.
- *Multi-tenant architecture* → logical separation of environments for partners, business units or customers.
- *Full API integration* → REST API support for automation, CI/CD pipelines and infrastructure-as-code workflows.

The main components of the service are:

- *OPNsense core platform* → the foundational DNS and security engine, providing routing, filtering, and advanced security modules.
- *Management & orchestration layer* → a cloud-native platform that automates provisioning, configuration, monitoring, and scaling of OPNsense nodes.

The service offers the following advantages:

- *Reduced operational ocmplexity* → eliminates the need to manage firewall hardware, updates, and maintenance in-house.
- *Lower total cost of ownership (TCO)* → subscription-based model removes CAPEX and ensures predictble cost planning.
- *Accelerated time-to-value* → rapid deployment and standardized configurations shorten rollout cycles.
- *Improved security posture* → centralized policy enforcement and continuous updates reduce exposure to threats.
- *Flexibility for business growth* → easily add new sites, users, or workloads without re-architecting the network.
- *Consistent and automated ocnfiguration* → reduces human error and ensures uniform security across the organization.
- *API-first approach* → smooth integration with DevOps pipelines and automated deployment systems.
- *Vendor neutral and open source–absed* → avoids vendor lock-in while benefiting from the transparency and flexibility of OPNsense.

4.12.2.3 Deployment in customer VNET

The DNS service is deployed as a virtual appliance within the customer's VNET.
It acts as the authoritative resolver for internal workloads while forwarding queries for external domains to upstream DNS servers. This ensures a single DNS endpoint for all workloads in the VNET, simplifying configuration and management.

4.12.2.4 Internal and external resolution

- Internal Resolution: the OPNsense DNS Resolver (Unbound) can be configured with local zones and host overrides. Workloads in the VNET can register their names dynamically, enabling seamless resolution of private IP addresses.
- External Resolution: queries for domains outside the VNET are forwarded to upstream DNS servers (e.g., ISP or public resolvers). Supports DNSSEC validation for secure external lookups.

4.12.2.5 Dynamic updates

The service supports dynamic DNS updates from workloads in the account, which can automatically register or update their DNS records in the OPNsense DNS Resolver.
This ensures that newly deployed or scaled workloads are immediately reachable by name without manual intervention.
Dynamic updates are authenticated using secure mechanisms (TSIG keys), preventing unauthorized changes.

Dynamic Updates Flow

1. Workload acquires IP address
   - a VM, container, or host in the customer VNET requests an IP lease from DHCP
2. DHCP assigns lease
3. DNS update request (RFC2136)
   - The DHCP service or workload sends a signed update message to the OPNsense DNS Resolver (Unbound).
   - Authentication is handled via TSIG keys to ensure only authorized clients can modify records.
4. Unbound DNS updates zone records
   - The resolver updates its local zone or forwards the update to an authoritative DNS server, and the A/AAAA records are updated with the new IP address.
5. Clients can resolve the updated names
   - Other workloads in the VNET query the OPNsense DNS service.
   - The resolver returns the updated IP address, ensuring connectivity.

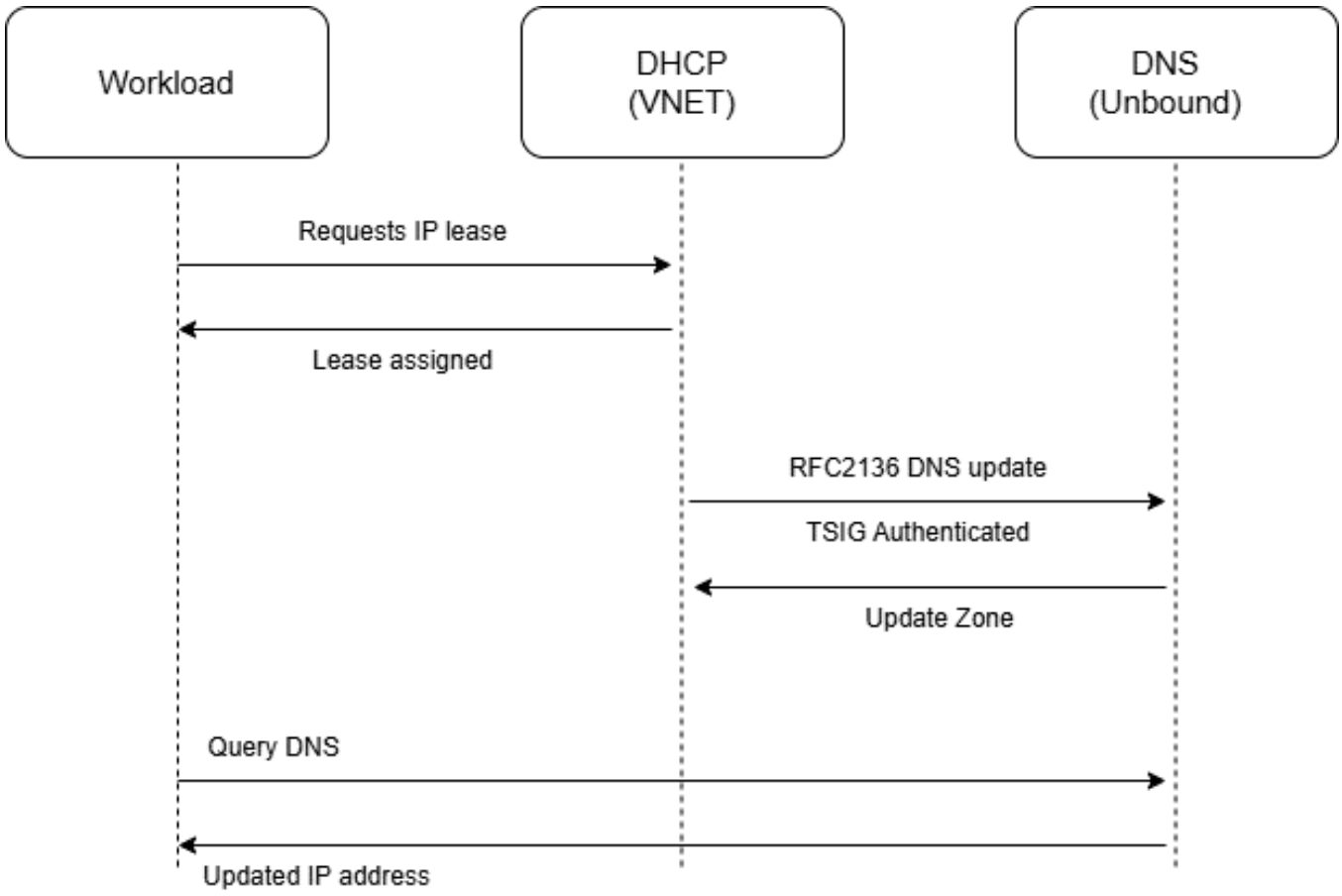


Figura 52 – Diagram of the Flow

4.12.3 Single public IP Service

4.12.3.1 Service Description

A PaaS Single Public IP service is a managed cloud networking offering that provides a dedicated, globally reachable public IP address for workloads hosted in the provider's cloud environment.
In this implementation the service enables customers to expose virtual machines, containers, load balancers, or platform services to the Internet using a stable, provider-managed public IP, without requiring them to manage networking infrastructure or routing complexity.

The service is offered *per number of public IP addresses* .

4.12.3.2 Features and Advantages

The main features of the service are:

- *Dedicated public IP assignment* → provides one unique and persistent public IPv4 or IPv6 address. The IP can be assigned to VMs, network interfaces, or load balancers within the cloud environment Ensures stable reachability even if the underlying infrastructure changes.
- *Managed routing and NAT* → the platform automatically manages inbound and outbound routing. Supports 1:1 NAT, DNAT, or SNAT depending on configuration. Simplifies network exposure of private resources, with no need to operate firewalls or routers.
- *High availability and redundancy* → public IPs are served through a highly redundant provider network. Automatic failover ensures continuity even if the underlying host or zone fails. Supports attaching the IP to different resources without service interruption.
- *Flexible binding to cloud resources* → the same public IP can be detached and reattached to: virtual machines, virtual network interfaces, load balancers, application gateways. Enables quick recovery, migrations, and architecture evolution.
- *Integrated security controls* → configurable security groups, ACLs, and firewall rules. Traffic filtering and connection control managed through the cloud portal. Protection against common network threats through provider-level safeguards.
- *Simplified internet exposure* → ideal for publishing: web applications, APIs, VPN gateways, remote management endpoints. No need to configure BGP, DNS routing, or physical network appliances.
- *Monitoring & logging* → platform dashboards show: traffic flows, connection statistics, security events. Useful for troubleshooting and capacity planning.

The main components of the service are:

- *Provider-managed edge network* → the public IP is routed through Aruba's redundant edge infrastructure. Anycast or geographically optimized routing ensures low latency and high availability. Backbone interconnects with major Internet exchange points.
- *Virtualized networking layer* → based on SDN-enabled virtual switches and routers. The public IP is associated to a virtual NIC via cloud networking APIs. Provides isolation between tenants and secure segmentation.
- *NAT & Firewall gateway cluster* → a cluster of virtual gateways manages: NAT operations, packet inspection, stateful firewalling, traffic shaping, Fully redundant and automatically scaled by the platform.
- *Control plane* → centralized management system allowing: creation and deletion of public IPs, binding/unbinding to resources, firewall rule management, configuration propagation across zones. Does not handle traffic directly but orchestrates network behavior.
- *Data plane* → distributed packet-processing nodes handle the real traffic. Designed for high throughput, low latency, and multi-zone resilience. Built to ensure performance even under heavy load.
- *Integration with DNS and load balancers* → the public IP can be connected to: DNS A/AAAA records, cloud load balancers, reverse proxies. Enables scalable and flexible application publishing.

The service offers the following advantages:

- *Simplified internet exposure* → easily expose VMs, applications, or services to the public Internet. No need to configure routers, gateways, or complex network infrastructure.
- *High availability and resilience* → public IPs are served through a redundant cloud network. Automatic failover ensures continuity if the underlying instance or zone fails. The IP remains reachable even when moving resources.
- *Flexibilty and portability* → the same IP can be detached and reattached to different cloud resources. Enables seamless migration, maintenance, and architecture changes. Supports disaster - - *Zero infrastructure management* → no need to deploy or maintain firewalls, NAT appliances, or BGP routers. Managing of routing, redundancy, and capacity at the network edge.
- *Integrated security* → built-in firewall rules, security groups, and access control lists Centralized management through the cloud portal or APIs. Provider-level protection against common network attacks.
- *Cost efficiency* → eliminates the need for purchasing and managing public IP blocks. Reduces operational overhead and network administration costs.
- *Consistent and stable reachability* → the public IP remains persistent, even if internal infrastructure changes. Guarantees stable endpoints for DNS records, APIs, and external integrations.
- *Improved operational agility* → fast provisioning of new public IPs on demand. Immediate configuration changes via self-service interface. Accelerates deployment pipelines and DevOps workflows.
- *Traffic monitoring and visibility* → built-in dashboards and logs for tracking inbound/outbound traffic. Useful for troubleshooting, auditing, and performance optimization.
- *Secure and scalable foundation for cloud services* → works seamlessly with load balancers, DNS records, VPN gateways, and edge services. Supports both small applications and large-scale enterprise architectures.

4.12.4 L7 Load Balancer (regional) Service

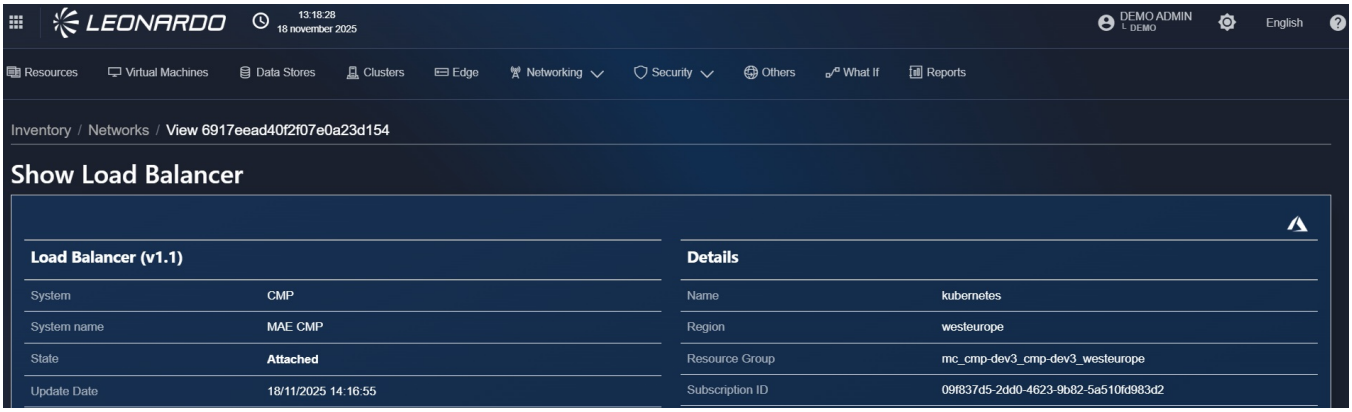


Figura 53 – L7 Load Balancer (regional)

Service Overview

4.12.4.1 Service Description

A PaaS L7 Load Balancer (Regional) is a fully managed platform service that distributes HTTP/HTTPS traffic across backend services (VMs, containers, or applications) within a specific cloud region.
It consists of a listener that receives requests on behalf of a set of backend pools and distributes them based on criteria based on application data, thus determining which pools serve a given request. The application infrastructure can therefore be specifically tuned and optimized to serve specific types of content.
Based on an OPNsense-like architecture, it provides advanced Layer 7 capabilities such as content-aware routing, SSL offloading, traffic inspection, and application firewalling—without requiring customers to deploy, monitor, or maintain any load-balancing infrastructure.

The service is offered *per each balancer instance*.

4.12.4.2 Features and Advantages

The main features of the service are:

- *Layer 7 application-aware routing* → inspects and routes traffic based on HTTP/HTTPS attributes: URL paths, hostnames, headers, cookies, query parameters, Enables fine-grained control and intelligent traffic distribution.
- *SSL/TLS termination and management* → offloads TLS/SSL handshake from backend servers. Centralized management of certificates (upload, renewal, rotation). Supports HTTPS redirection, HSTS, and modern cipher suites.
- *Backend load distribution* → supports several load-balancing algorithms: round-robin, least connections, IP hash, weighted distribution. Ensures efficient traffic handling and smooth scaling of applications.
- *Health checks and failover* → performs L7 health checks on backend services (HTTP codes, response payloads). Automatically excludes unhealthy instances and restores them when available. Prevents routing user requests to failed or degraded services.
- *Web Application Firewall (WAF)* → integrated OPNsense-compatible WAF engine. Protects against OWASP Top 10 and common web attacks. Provides rule sets, anomaly scoring, and traffic filtering.
- *URL rewriting and traffic transformation* → rewrite URLs, headers, or cookies. Inject or remove headers for security or routing logic. Useful for legacy system integration or microservices migration.
- *Regional scope* → traffic is handled within a specific cloud region for: predictable latency, compliance requirements, locality of data and workloads. Ideal for regional failover patterns.
- *Logging, monitoring, and metrics* → provides: request/response logs, traffic and error statistics, performance metrics, WAF alerts. Enables effective debugging and performance optimization.

- *Zero infrastructure management* → no need to deploy virtual appliances, firewalls, or proxies. The platform maintains: high availability, patching, upgrades, scaling, failover

The main components of the service are:

- *Regional load balancing cluster* → a distributed cluster of L7 processing nodes within the chosen region.Provides high availability (active-active or active-standby) → automatically scales horizontally based on traffic load.
- *OPNsense-based application proxy layer* → built on top of an OPNsense-like architecture: HAProxy or NGINX engine, integrated WAF, layer 7 parsing and filtering. Provides flexibility and robust application-level control.
- *Virtualized networking layer* → integrates with the cloud network fabric. Supports private and public endpoints. Ensures tenant isolation and secure routing to backends.
- *Control plane* → It's coordinates: configuration of listeners, rules, routes, and backends, certificate management, policy updates and propagation, versioning and rollback, API- and UI-based management. Does not handle traffic.
- *Data plane* → processes all HTTP/HTTPS requests. Terminates TLS, applies routing logic, executes WAF rules. Ensures high throughput and low latency.
- *Health check and failover engine* → continuously monitors backend endpoints. Maintains a dynamic view of backend availability. Ensures failover rules are applied in real time.
- *Logging & analytics layer* → collects request logs, WAF events, metrics, and anomalies. Provides dashboards and monitoring tools. Works independently from the data plane to ensure performance.

The service offers the following advantages:

- *Improved application availability* → automatic failover prevents downtime. Faulty backends are bypassed instantly.
- *Better performance and lower latency* → efficient L7 traffic distribution within the same region. TLS offloading improves backend performance.
- *Strong security posture* → built-in WAF protects against common web threats. TLS best practices and centralized certificate management.
- *Simplified operations* → fully managed service—no appliance deployment or patching. Easy configuration from UI or APIs. Reduces operational and networking overhead.
- High flexibility in routing → content-based routing for modern microservices architectures. Easy to map multiple applications under the same IP/hostname.
- *Cost efficiency* → eliminates need for dedicated load balancer appliances.
- Consistent user experience → evenly balances traffic to healthy backends. Ensures predictable application responsiveness.
- *Enhanced observability* → access to detailed logs, metrics, and WAF events. Faster troubleshooting and monitoring.

- *Compliance and regional data control* → all traffic processing remains within a specific geographic region. Helps meet regulatory and data residency requirements.
- *Rapid deployment and DevOps integration* → instant provisioning with minimal configuration. API-driven automation for CI/CD pipelines.

4.12.5 Cloud interconnect Gold SW (10 Gbps max throughput)

4.12.5.1 Service Description

The PaaS Cloud interconnect gold SW service provides a high-quality, software-defined, private connectivity between a customer's on-premises infrastructure (or external data centers) and the Aruba cloud environment.
It offers dedicated bandwidth tiers, enhanced SLA guarantees, secure routing, and enterprise-grade performance, enabling customers to build hybrid or multi-cloud architectures without deploying physical network appliances or managing complex routing setups.
The "Gold" tier represents the highest level of availability, performance, and support, while the "SW" component refers to software-based interconnect provisioning, ensuring flexibility, fast activation, and seamless scalability.
This service, delivered via hardware or software, is designed to simplify customer application migration with minimal impact on users and workloads.
It enables granularity down to the individual IP address during migration, increasing security and minimizing rollback times, if necessary.

The service is offered with the following unit metric: *10 Gbps of throughput*.

4.12.5.2 Features and Advantages

The main features of the service are:

- *Private and secure network connectivity* → ensures a private, non-public connection between customer networks and cloud resources. Traffic does not traverse the public Internet, reducing risk and improving performance. Ideal for workloads requiring compliance, isolation, or predictable latency. - *Software-defined provisioning (SW)* → fully software-based interconnect setup with no physical circuits required.On-demand provisioning via web console or API. Rapid activation (minutes instead of days or weeks). Flexible reconfiguration without service interruption.
- *High SLA & guaranteed bandwidth (Gold tier)* → provides defined bandwidth tiers with guaranteed throughput. Includes enhanced SLA for: availability, packet loss, latency, jitter. Suitable for mission-critical enterprise applications.
- *Multi-site and multi-zone connectivity* → supports connectivity to multiple Aruba regions or availability zones. Enables redundant hybrid cloud architectures. Facilitates interconnection of distributed workloads.
- *Routing integration* → supports dynamic routing (BGP) or static routing. Automatically adapts to network topology changes. Enables flexible hybrid cloud traffic engineering.

- *Segmentation and isolation* → allows creation of multiple isolated virtual circuits or VLANs. Ideal for separating environments: production, staging, development, partner networks
- *End-to-end encryption* → traffic can be encrypted at the network edge using IPsec or provider-managed encryption. Ensures compliance with data protection standards.
- *Monitoring, logs, and telemetry* → real-time monitoring of: bandwidth usage, packet loss and latency, connection health. Exportable logs for SIEM and analytics systems.
- *No Physical hardware required* → provider manages the entire connectivity layer. No need for physical circuits, routers, or carrier contracts. Reduces complexity and deployment time.

The main components of the service are:

- *Software-defined interconnect fabric* → centralized SDN layer orchestrating virtual connections. Provides flexible, scalable, multi-tenant connectivity. Allows rapid deployment and reconfiguration.
- *Regional interconnect gateways* → high-availability routing gateways located in Aruba cloud regions. Serve as entry/exit points for private customer traffic. Architected for redundancy and failover.
- *Cloud backbone network* → high-capacity fiber backbone interconnecting Aruba data centers. Ensures low-latency east-west traffic across regions. Supports both primary and backup routes.
- *Security & isolation layer* → strict tenant isolation enforced at: network virtualization layer, routing control plane, traffic segmentation policies. Ensures no cross-tenant visibility.
- *Control plane* → It manages: provisioning of interconnects, routing updates, bandwidth allocation, policy enforcement. Exposed through UI and APIs.
- *Data plane* → handles the actual traffic flow with: guaranteed QoS, deterministic routing, optimized latency paths. Decoupled from monitoring and control tasks.
- *Monitoring & observability layer* → aggregates telemetry from gateways and SDN controllers. Provides dashboards and alerting for performance and reliability.

The service offers the following advantages:

- *Enhanced security* → private connection avoids exposure to the public Internet. Supports encrypted tunnels and isolated routing domains.
- *Predictable and high performance* → guaranteed bandwidth and low latency. Stable connectivity ideal for enterprise workloads.
- *Rapid deployment* → software-defined provisioning reduces setup from weeks to minutes. No physical circuits or carrier coordination required.
- *High availability and reliability (Gold SLA)* → redundant gateways, paths, and failover mechanisms built in. Suitable for mission-critical connectivity.

- *Cost efficiency* → eliminates the need for physical interconnects or MPLS lines.
- Improved hybrid cloud architecture → seamlessly integrates on-prem infrastructure with cloud workloads. Supports migration, DR, and inter-site communication.
- *Scalability on demand* → quickly adjust bandwidth tiers or add new interconnects. Ideal for growing or fluctuating workloads.
- *Simplified network operations* → centralized management via API/portal. Automated routing and monitoring reduce operational overhead.
- *Better compliance and data governance* → private, regional connectivity supports regulatory requirements. Data paths remain under predictable network control.
- *Optimized application experience* → reduced jitter and packet loss improve performance for: databases, real-time apps, VoIP/UC, latency-sensitive services.

4.12.6 Managed VPN Access Service

4.12.6.1 Service Description

The Managed VPN Access Service provides secure connectivity between customer premises and cloud infrastructure using the OPNsense firewall appliance.
It is a fully-automated managed VPN service, meaning customers do not need to manually maintain or patch the underlying system. The service provider ensures continuous updates and security compliance.

Key capabilities: - Provisioning via portal and APIs for automation and integration. - Provider-managed patching of the OPNsense appliance and service components. - Multiple VPN connections per virtual network supported. - Flexible tunneling protocols: IPsec, SSL, and WireGuard. - BGP support for improved failover and routing across IPsec tunnels.

4.12.6.2 Features and Advantages

The service can be provisioned through the Leonardo's Secure Cloud Management Portal for quick setup. APIs are available for automated configuration and integration with Infrastructure-as-Code workflows. Declarative configuration files can be used to define VPN tunnels, routing policies, and security contexts.

The Managed VPN Access Service supports multiple tunneling protocols over the public Internet, ensuring flexibility, interoperability, and strong security for different use cases. Each protocol offers unique advantages depending on the connectivity scenario.

- IPsec VPN (Internet Protocol Security)
  - Purpose: Industry-standard protocol suite for securing IP communications.
  - Use Case: Commonly used for site-to-site tunnels between customer premises and cloud infrastructure.

- Features:
  - Strong encryption (AES, SHA-2, etc.) for confidentiality and integrity.
  - Widely supported across enterprise firewalls, routers, and appliances.
  - Compatible with BGP routing to enable dynamic failover and load balancing across multiple tunnels.
- Benefit: Ensures highly secure, standards-based connectivity for enterprise networks.

- SSL VPN (Secure Sockets Layer Virtual Private Network)
  - Purpose: Provides secure remote access for individual users or devices.
  - Use Case: Ideal for remote workforce connectivity, enabling employees to securely access internal applications from anywhere.
  - Features:
    - Operates over HTTPS, making it firewall-friendly and easy to deploy.
    - Supports client-based and clientless (browser-based) access.
    - Flexible authentication options (certificates, MFA, LDAP/AD integration).
    - Benefit: Simplifies remote access with minimal configuration, while maintaining strong encryption and user authentication.
- WireGuard VPN
  - Purpose: A modern, high-performance VPN protocol designed for simplicity and speed.
  - Use Case: Suitable for both site-to-site and remote access scenarios where performance and ease of configuration are priorities.
  - Features:
    - Lightweight codebase, reducing attack surface and improving maintainability.
    - Uses state-of-the-art cryptography (Curve25519, ChaCha20, Poly1305).
    - Faster connection setup and lower latency compared to traditional VPN protocols.
    - Easy configuration with minimal overhead.
  - Benefit: Delivers secure, efficient, and scalable VPN connectivity, particularly well-suited for modern cloud-native environments.

4.12.6.3 High Availability and Failover

The service supports High availability State Synchronization (pfsync), enabling VPN session states synchronization (including IPsec tunnels) between VPN service Instances, so active VPN connections continue without interruption during failover.
Configuration between instances is synchronized as well with a built in HA sync mechanism that replicates VPN configuration changes from the primary instance to the secondary.

The service supports Border Gateway Protocol (BGP) to improve failover across IPsec VPN tunnels, to dynamically reroutes traffic in case of tunnel failure, ensuring uninterrupted connectivity. Multiple VPN connections per virtual network can be configured for redundancy and load balancing.

4.12.6.4 Security and Compliance

Leonardo is fully responsible for patching the VPN protocols and services, offering a secure, compliant environment without customer patching responsibilities.

4.12.7 PaaS Client/Forward Proxy

4.12.7.1 Service Description

The Proxy service is a managed front-facing service designed to retrieve data from a wide range of sources across the internet.
It acts as an intermediary between internal users and external services, ensuring that requests are securely handled and filtered before reaching their destination.
The service is built on OPNsense, an open-source firewall and routing platform, and is delivered as a fully managed solution.
This means that all necessary updates, patches, and maintenance are handled by the provider, allowing IT staff to focus on their applications and users rather than the underlying infrastructure.

4.12.7.2 Features and Advantages

The Proxy service functions as a gateway. When a user inside the organization requests data from an external source, the request is first directed to Proxy.
The service evaluates the request against configured rules and policies, determines whether it should be allowed or blocked, and then forwards it to the destination if permitted. Responses from external services are similarly inspected before being passed back to the user.
This approach provides several benefits: it ensures that only authorized traffic leaves the network, it prevents malicious content from entering, and it gives administrators visibility into how users interact with external services.

Provisioning and Management

Proxy can be provisioned through the Secure Cloud Management Platform, the central portal for managing cloud services. Administrators can deploy the service by selecting the Proxy option within the platform. Provisioning can also be performed through APIs, enabling integration into automated workflows.
Once deployed, the service is automatically patched and maintained by the provider. This ensures that the system remains up to date with the latest security fixes without requiring manual intervention.

Authentication Integration

Proxy supports integration with Active Directory and OpenID Connect for user authentication. This means that organizations can leverage their existing identity management systems to control access.
- With Active Directory, Proxy can validate user credentials against the domain controller, ensuring that only authorized users are able to use the service.
- With OpenID Connect, Proxy can redirect users to an identity provider for authentication, then use the returned tokens to grant access.
This integration allows organizations to enforce consistent access policies across their environment without duplicating user management.

Request Filtering

Proxy supports both whitelisting and blacklisting of requests. Administrators can define rules that specify which destinations or types of requests are permitted and which are denied. For example, they may allow access to trusted business applications while blocking requests to known malicious domains.
This filtering capability ensures that users can only access approved resources, reducing the risk of data leakage or exposure to harmful content.

Anti-Virus and Anti-Malware Protection

Proxy includes integrated anti-virus and anti-malware scanning, typically powered by engines such as ClamAV. All traffic passing through the service can be inspected for malicious payloads, ensuring that harmful files or code are blocked before reaching users.
This functionality provides an additional layer of defense, complementing endpoint protection and reducing the likelihood of infections spreading through downloaded content.

Scalability

The Proxy service is designed as a fixed-capacity solution. It does not scale dynamically with demand. Administrators should plan usage accordingly, ensuring that the service is deployed in environments where its capacity is sufficient for the expected traffic load.

4.12.8 PaaS Reverse Proxy

4.12.8.1 Service Description

The Managed Reverse Proxy service provides a secure and automated way to control and route traffic between external clients and internal applications.
It is built on OPNsense and HAProxy, which is widely recognized for its performance and flexibility in handling web traffic.
Delivered as a fully managed solution, Leonardo assumes responsibility for all patching, updates, and maintenance, ensuring that administrators benefit from a hardened and continuously updated platform.

4.12.8.2 Features and Advantages

A reverse proxy sits in front of application servers and receives incoming requests from clients. Instead of exposing servers directly to the internet, the proxy terminates connections, applies configured rules, and forwards requests to the appropriate backend service.
This architecture improves security, simplifies certificate management, and enables sophisticated traffic routing.
The Managed Reverse Proxy service can be provisioned through the Secure Cloud Management Portal or via APIs.
Once deployed, the CSP ensures that the underlying OPNsense system and HAProxy plugin remain patched and secure.

SSL/TLS termination

The reverse proxy provides full support for SSL/TLS termination. This means that encrypted client connections are terminated at the proxy, where traffic is decrypted. Certificates can be uploaded and managed directly within the solution, and bound to frontends.

A typical frontend definition might look like this:

```
frontend https_frontend
    bind *:443 ssl crt /etc/haproxy/certs/
    mode http
    option httplog
```

Here the proxy listens on port 443, terminates SSL/TLS using the certificate stored in `/etc/haproxy/certs/` , and then processes traffic in HTTP mode.
Once decrypted, traffic can be inspected, filtered, or routed, and then forwarded to backend servers either as plain HTTP or re-encrypted if desired. This centralizes certificate management and reduces the complexity of maintaining certificates across multiple backend servers.
HTTP Termination.
In addition to SSL/TLS, the reverse proxy also supports HTTP termination. This allows the proxy to handle plain HTTP traffic directly, applying rules and routing logic before passing requests to backend servers. This is useful for internal services or applications that do not require encryption, and it ensures that both encrypted and unencrypted traffic can be managed consistently through the same proxy layer.

Server Name Indication (SNI) compatibility

The proxy is fully compatible with the Server Name Indication (SNI) extension of TLS. This capability allows the proxy to host multiple SSL/TLS certificates on a single IP address and port. When a client initiates a connection, the proxy uses the hostname provided in the SNI field to select the correct certificate. This makes it possible to serve multiple domains securely from the same proxy instance, a critical feature for organizations hosting multiple applications or services.

For example:

```
frontend https_frontend
    bind *:443 ssl crt /etc/haproxy/certs/domain1.pem crt /etc/haproxy/certs/domain2.pem
    mode http
```

When a client connects, HAProxy inspects the SNI field in the TLS handshake and selects the appropriate certificate based on the requested hostname. This allows multiple domains to be served securely from a single proxy instance.

Routing Rules and Traffic Management

One of HAProxy's most powerful features is its ability to define complex routing rules. Administrators can configure rules based on request attributes such as headers, paths, query strings, or even cookies. For example, traffic containing a specific header can be routed to one backend service, while requests with a different header are directed elsewhere.
The proxy also supports load balancing strategies, health checks, and content switching. This means that traffic can be distributed across multiple backend servers to improve performance and reliability, or directed to specific servers depending on the nature of the request. The OPNsense HAProxy plugin provides a user-friendly interface for defining these rules, making it possible to implement sophisticated traffic management policies without requiring deep knowledge of HAProxy's configuration syntax.

Below is an example of content switching, where traffic is routed depending on request attributes. For example, administrators may want to send requests with a specific header to one backend, and all other requests to another:

```
frontend https_frontend
    bind *:443 ssl crt /etc/haproxy/certs/
    mode http
    acl api_request hdr(X-Service) -i api
    use_backend api_backend if api_request
    default_backend web_backend
```

In this configuration:
- The `acl` (access control list) checks whether the request contains the header `X-Service: api`.
- If the header is present, traffic is routed to `api_backend`.
- All other requests are sent to `web_backend`.

4.13 Storage Family

Below is the list of services belonging to the Storage family:

- Block Storage (1000 GB) - High Density
- Archive Storage (1000 GB)

4.13.1 Block Storage (1000 GB) - High Density Service

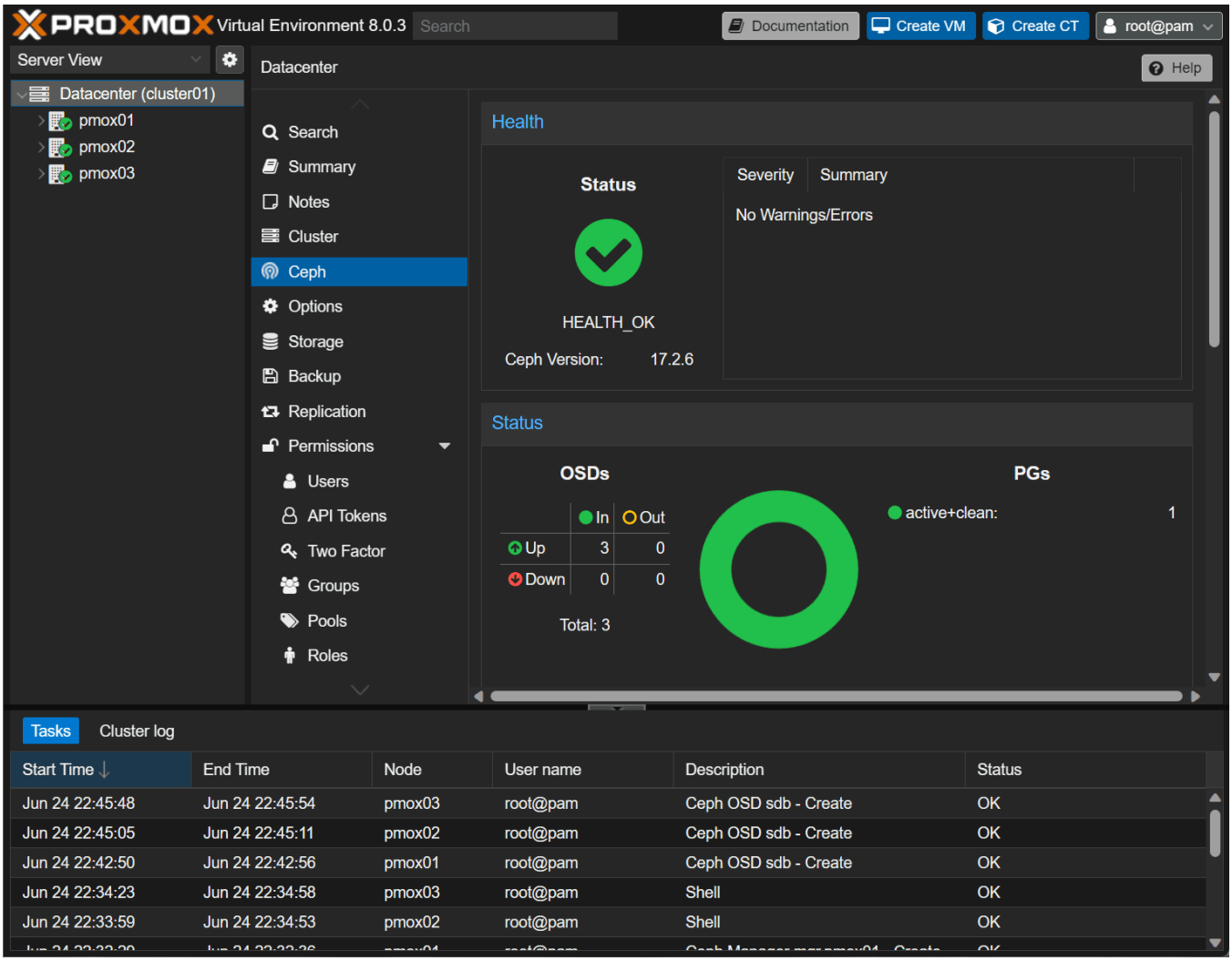


Figura 54 – Block Storage (1000 GB) - High Density Service interface

4.13.1.1 Service Description

The PaaS Block Storage (1000 GB) – High Density service provides enterprise-grade, fully managed block storage volumes designed for virtual machines and cloud workloads hosted on Proxmox platforms.
The storage layer is powered by Ceph, a distributed, fault-tolerant, and scalable SDS (Software-Defined Storage) technology that ensures durability, high availability, and efficient capacity utilization.
This service offers 1000 GB of high-density block storage, ideal for workloads that require large capacity at optimized cost while still benefiting from redundancy, resiliency, and seamless integration into virtualized cloud environments.

The service is offered with the following metrics: 1000 GB for each unit.

4.13.1.2 Features and Advantages

The main features of the service are:

- *Managed block storage volumes (1000 GB)* → provides fully provisioned 1000 GB block devices. Can be attached to Proxmox-based virtual machines. Supports OS disks, application data, databases, and file systems.
- *High-density storage tier* → optimized for workloads requiring large capacity. Uses cost-efficient high-density disks while maintaining reliability. Suitable for: archival data, moderately I/O-intensive applications, backup staging, large datasets that don't require ultra-high performance.
- *Ceph RBD (RADOS Block Device) integration* → volumes are exposed as Ceph RBD devices, enabling features like thin provisioning, snapshot support, cloning capabilities.
- *High availability and data replication* → data is replicated across multiple Ceph nodes. Ensures durability even in case of disk or node failure. Automatic recovery and self-healing functions enhance resilience.
- *Persistent and Reliable Storage* → volumes maintain data integrity across VM reboots, migrations, or failovers. Ideal for persistent disks in virtualized infrastructures.
- *Seamless VM integration* → managed directly through the Proxmox interface/API. It supports: VM disk attachments and detachments, live migration with attached volumes, dynamic resizing.
- *Performance optimization for large-capacity workloads* → balanced read/write response designed for high-density environments. Ceph intelligently distributes I/O across cluster nodes.
- *Managed service* → No need to manage Ceph clusters, disks, or replicating policies. Handling of: monitoring, maintenance, scaling, upgrades, fault resolution.

The main components of the service are:

- *Ceph storage cluster* → distributed architecture composed of Object storage nodes monitoring nodes for cluster coordination and manager nodes for cluster insight and APIs. Ensures high availability and horizontal scalability.
- *Proxmox integration layer* → Proxmox integrates directly with Ceph RBDs and provides unified API and management interface for VMs and storage. Allows dynamic allocation of block devices to VMs.
- *Replicated storage pools* → storage pools configured with replication. Ensures redundancy across multiple disks

and hosts. Prevents data loss from node or disk failures.

- *Data plane* → handles all I/O operations, including data striping, replication, rebalancing, recovery, snapshot management. Designed for reliability and optimized throughput.
- *Control plane* → Manages Ceph cluster coordination, health monitoring, volume lifecycle, config policies, Proxmox integration.
- *Monitoring and observability* → continuous monitoring of storage utilization, disk health, replication status, I/O performance. Automated alerts ensure proactive issue resolution.
- *Security and isolation* → tenant isolation at storage pool and access level. Encrypted communication between Ceph and Proxmox nodes. Optional disk encryption at rest depending on policy.

The service offers the following advantages:

- *High capacity at optimized cost* → designed for workloads needing large data volume without paying for premium performance tiers.
- *High udrability and fault tolerance* → multi-node replication ensures data remains safe even if disks or machines fail.
- *Fully managed storage infrastructure* → eliminates the need to configure, maintain, or troubleshoot Ceph clusters.
- *Scalable and flexible* → storage grows horizontally without downtime. Additional capacity or block volumes can be provisioned on demand.
- *Seamless integration with Proxmox VM environments* → easy attachment to VMs, live migration support, and simplified administration.
- *Improved operational efficiency* → snapshots, cloning, and thin provisioning speed up development and operations workflows.
- *Consistent performance for high-density workloads* → balanced I/O distribution with predictable storage behavior.
- *Enhanced data protection* → built-in replication, self-healing, and monitoring reduce risk of data loss.
- *Simplified backup and recovery* → volume snapshots enable fast backup operations. Easy rollback to previous storage states.
- *Enterprise-grade reliability* → Ceph’s distributed architecture provides continuous service availability and resilience.

4.13.2 Archive Storage (1000 GB) Service

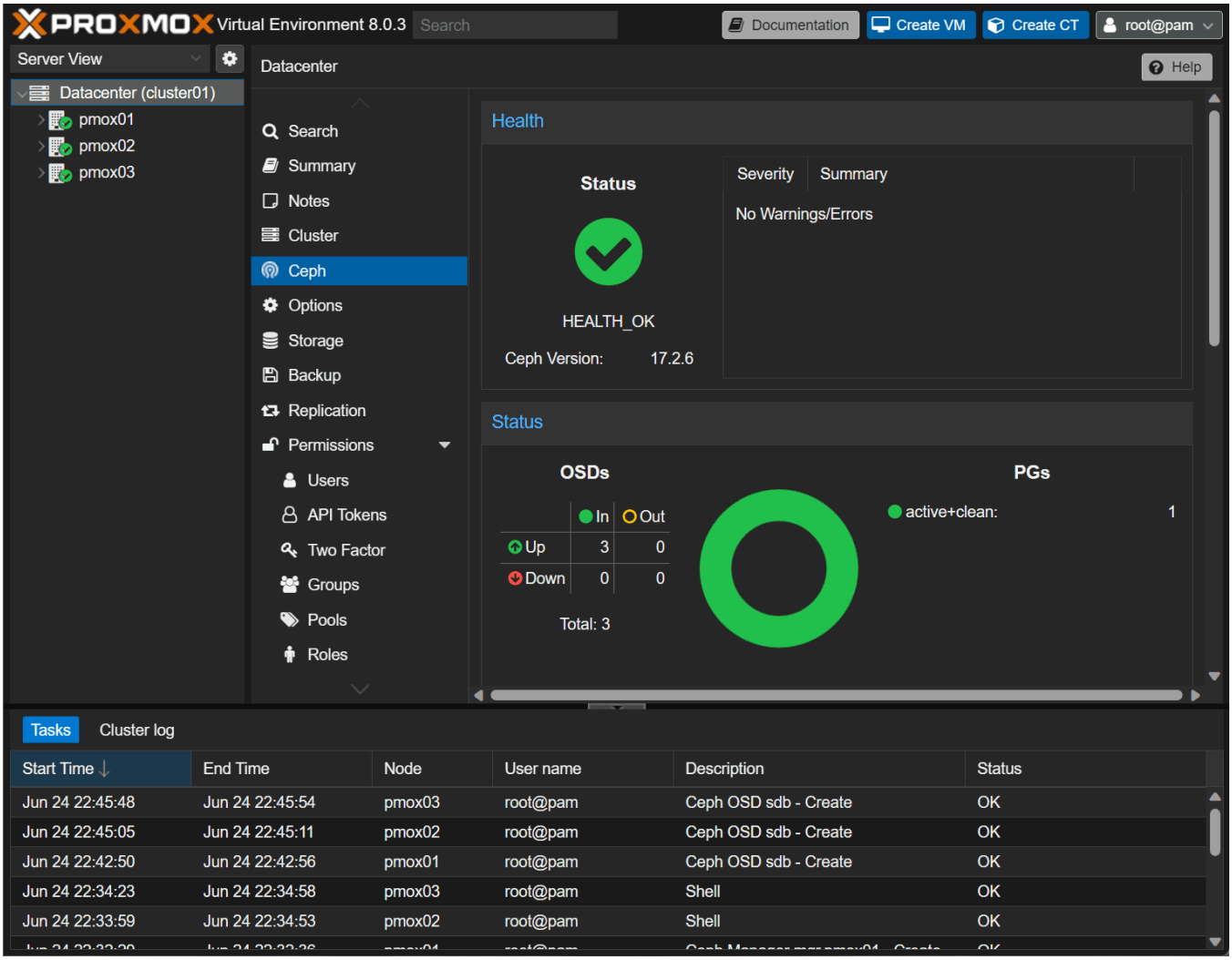


Figura 55 – Archive Storage (1000 GB)
Service interface

4.13.2.1 Service Description

The service provides a scalable, low-cost, long-retention storage environment designed for infrequently accessed data. It is built on Proxmox Virtual Environment (PVE) with Ceph as the underlying distributed storage layer. The service enables organizations to store large volumes of archival datasets—such as logs, backups, compliance records, media assets, or scientific data—while ensuring durability, fault tolerance, and controlled retrieval performance.

The service is offered with the following metrics: *1000 GB for each unit*.

4.13.2.2 Features and Advantages

The main features of the service are:

- Long-term data retention with policies tailored for infrequently accessed objects or files
- Distributed, reliable storage through Ceph's replication or erasure coding.
- Scalable capacity expansion by adding nodes or OSDs without service interruption.
- Multi-protocol access via CephFS, RBD, or S3-compatible gateways, depending on deployment.
- Automated data placement and self-healing mechanisms inherent to Ceph.
- Role-based access control and integration with existing identity systems (via Proxmox and optional gateways).
- Monitoring and lifecycle management through Proxmox's UI and Ceph dashboards.
- Optional tiering by combining faster Ceph pools with lower-cost archival pools.

The main components of the service are:

- *Proxmox VE Cluster* → Management layer for nodes, resources, authentication, and integration with Ceph; offers UI, automation tools, and API endpoints.
- *Ceph Cluster*:
  - OSD Nodes: Storage servers providing replicated or erasure-coded archival pools.
  - MON/MGR Nodes: Ceph Monitors and Managers responsible for cluster coordination, state tracking, and health management.
  - CephFS / RBD / RGW: Optional access interfaces to expose archival storage as a filesystem, block device, or S3-compatible object store.
- *Networking Layer* → High-bandwidth, redundant network for internal Ceph traffic (public and cluster networks) to ensure consistency and performance.
- *Monitoring and Logging Tools* → Proxmox and Ceph dashboards, Prometheus, and alerting integrations.

The service offers the following advantages:

- *Cost-efficient retention* → lower TCO for storing large datasets compared to high-performance primary storage.
- *High durability and fault tolerance* → data is protected through Ceph replication or erasure coding, reducing risk of data loss.
- *Horizontal scalability* → capacity and performance can grow incrementally without downtime, supporting evolving storage needs.
- *Vendor independence* → based on open technologies, minimizing lock-in and enabling custom tailoring.
- *Operational simplicity* → unified management from Proxmox with integrated monitoring, lifecycle management, and automation.

- *Flexible access models* → filesystem, block, or object interfaces allow integration with backup systems, archival workflows, and data management tools.
- *Resilience and self-healing* → ceph automatically redistributes and recovers data in case of disk or node failures, reducing administrative overhead.
- *Compliance support* → Suitable for long-term preservation and regulatory retention requirements.

4.13.3 Disaster Recovery Process for Block and Archive Storages

The PaaS Block Storage service is delivered on a high-density storage architecture powered by Proxmox VE and a Ceph distributed storage cluster.
Ceph provides native replication, self-healing and strong data durability.
Disaster Recovery (DR) ensures service continuity, data integrity and rapid restoration in case of partial or full site failure.

Disaster Recovery (DR) Objectives

- RPO (Recovery Point Objective): zero in an Availability Zone failure scenario, as Ceph writes are synchronously replicated across Zones.
- RTO (Recovery Time Objective): designed to be minimal. Recovery depends on the nature of the failure (node, rack, or site).

DR Protection Levels

- Full Availability Zone DR
  - Block volumes are continuously replicated to a coupled Availability zone through synchronous replication leveraging Ceph stretched cluster and CRUSH maps. In case of complete outage of an Availability Zone, the coupled AZ already contains the RBD images, and workloads can be restored automatically, or by registering the affected compute instances to the live AZ. This allows for 0 RPO and a variable RTO that can span from 0 (automated failover) to minutes if automatic failover is not used.
- Full Region DR
  - Inter-region mirroring can be enabled on a per-volume basis, allowing asynchronous replicas of data from any AZ of a given region to AZ of a paired region.
  - Replication can be continuous or snapshots-based, with a minimum internal between snapshots of one minute.
  - Recovery of impacted services to a new region is orchestrated by Leonard's Secure Cloud Management Platform where a DR plan.

Regional DR Process Workflow

- *Step 1 – Failure Detection*
  - The underlying storage continuously monitors the state of the storage nodes and cluster.
  - Automatic alerts for: Disk or node failures, Network disruption, Replication degradation, Cluster reaching “HEALTH_WARN” or “HEALTH_ERR”
- *Step 2 – Activation of workloads on the paired Region*

  If the failure affects an entire Region: - Administrators promote mirrored RBD images on the remote Ceph cluster. - Proxmox compute nodes at the DR site attach the promoted RBDs. - Services are restarted according to the failover plan.
- *Step 3 – Service Validation*
  - Verification that Block Storage volumes are consistent and available.
  - Checks of application logs and integrity validation.
- *Step 4 – Failback (Post-Recovery)*
  - Once the primary Region is restored:
    - Data is synchronized back (reverse RBD mirroring).
    - Primary cluster is reintroduced into production.
    - Normal operations resume.

5 Hybrid Services

The following table lists the services included in the *Hybrid* category.

FAMILY	LIST OF SERVICES
Hybrid	Edge Location - Pool Small (Confidential)
Hybrid	Bulk Data Transfer

List of families and related Hybrid services

5.1 Hybrid Family

Below is the list of services belonging to the Hybrid Edge family:

- Edge Location - Pool Small (Confidential

5.1.1 Edge Location - Pool Small (Confidential)

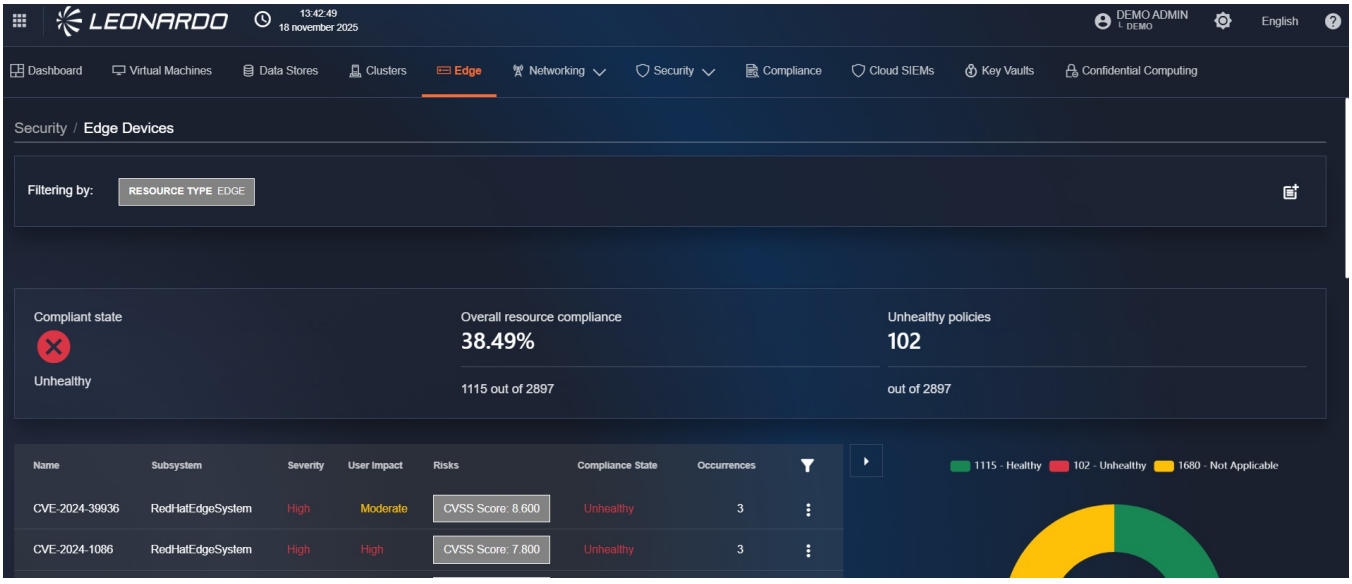


Figura 56 – Edge Location - Pool Small (Confidential) Overview

5.1.1.1 Services Description

The Edge Location Service provides a localized computing platform delivered across distributed edge locations, designed to offer low-latency processing, high availability, and centralized management.
Built on Proxmox Virtual Environment as the core virtualization layer and integrated with a Leonardo Secure Cloud Management Platform (SCMP) for orchestration, automation, and governance, the service enables customers to deploy, manage, and scale applications and workloads directly at the edge, close to the point of data generation or consumption.
The edge infrastructure operates as an extension of the corporate or hybrid cloud environment, maintaining consistent operational standards, security policies, and automation capabilities.

The service is sized in host unit. A single unit is composed by 3 Hosts, with the following settings: 2x 24 Core CPU - 512 GB RAM - 32 TB SSD.

5.1.1.2 Features and Advantages

The main functional capabilities of the service are:

- *Application Hosting* → execution of container-based or virtual machine–based applications. Support for real-time workloads, IoT scenarios, and local data processing. Automated provisioning of application environments via CMP orchestration.
- *Multi-tenant resource management* → logical segmentation of resources for tenants or business units. Quota-based allocation of CPU, memory, storage, and network resources. Role-based access and differentiated permissions.
- *Automation & orchestration* → automated provisioning of VMs, containers, and PaaS components. Standardized deployment workflows. Full lifecycle management of workloads (creation, update, decommissioning).
- *Governance & security* → integration with Identity & Access Management (IAM) systems. Enforcement of compliance and security policies. Centralized logging, audit trail capabilities, and continuous monitoring
- *High availability & resilience* → Proxmox high-availability clustering with automated failover. Fault isolation and hardware resilience. Integrated backup and restore capabilities.

The Architectural components are:

- *Edge Compute Layer (Proxmox VE)* → KVM hypervisor and LXC container virtualization. Proxmox clusters with distributed resource management. Local or distributed storage (Ceph, ZFS, or shared storage systems). Virtual networking using bridges, VLANs, and SDN capabilities
- *Secure Cloud Management Platform (SCMP)* → Central orchestration system managing all edge locations. Self-service portal for tenants and administrators. Policy engine for governance, permissions, and compliance enforcement. Monitoring, metering, and alerting functionalities. PIs for integration with external systems (CI/CD, ITSM, ERP) - *Networking & connectivity* → secure connectivity between edge locations and datacenters (VPN,

SD-WAN, MPLS). Network segmentation via virtualization technologies. Support for public and private addressing of workloads

- *Integration with enterprise systems* → integration with corporate authentication systems (LDAP, AD, SSO). Optional integration with Kubernetes for container-native workloads. Interoperability with public cloud platforms as part of a hybrid cloud model.

Below are the technical and infrastructural requirements of cloud physical appliances that have been taken into consideration for the design of the technological solution for the services:

- *Size and layout* → the data center must have sufficient space to accommodate the necessary racks, with standard sizes (42U, 45U, or 48U) and configurations that allow easy access for maintenance and component management.
- *Cabling* → an organized and optimized cabling system is essential, with cables labeled and routed to minimize interference and facilitate technical interventions.
- *Ventilation and cooling* → racks must be located in spaces with adequate ventilation and cooling systems to prevent overheating and keep electronic components at optimal operating temperatures.
- *Physical security* → rack spaces must be protected from unauthorized access with physical security systems such as locks, biometric access controls, and continuous video surveillance.
- *Power capacity* → the data center must have adequate power to support expected workloads. This includes assessing the power required for each rack and planning the total capacity required.
- *Redundant power supply* → to ensure business continuity, it is necessary to provide redundant power systems such as uninterruptible power supplies (UPS) and emergency generators that can intervene in the event of a primary power outage.
- *Power management* → implement tools and technologies to monitor and manage energy consumption, optimizing resource use and reducing operating costs.
- *Energy efficiency* → use energy-efficient equipment and infrastructure to minimize consumption and environmental impact, adhering to best practices for data center energy management.

42U Rack - P9K07A - HPE 42U 600mm x 1075mm	
Line Voltage	230 VAC
VA Rating	5081.1 VA
BTU HR	17240.99 BTU/h
System Current	22.08 A
Utilization Input Power	5056.01 W
Idle Input Power	1250.94 W
Max Load Input Power	5056.01 W
System weight (kg)	315.31 kg

Figura 57 – Rack energy power output

Apparato	VA Rating (VA)	BTU HR (BTU)	System Current (A)	Idle Input Power (W)	Max Load Input Power (W)
Infra - HPE ProLiant DL385 Gen11 8SFF	658.86	2226.35	2.86	164.71	652.89
Infra - HPE ProLiant DL385 Gen11 8SFF	658.86	2226.35	2.86	164.71	652.89
OCP - HPE ProLiant DL385 Gen11 8SFF	846.24	2869.48	3.68	159.6	841.49
OCP - HPE ProLiant DL385 Gen11 8SFF	846.24	2869.48	3.68	159.6	841.49
OCP - HPE ProLiant DL385 Gen11 GPU	1271.9	4324.74	5.53	216.32	1268.25
TOR Switch - HPE SN2410M 48SFP28 8QSFP28	362	1234.42	1.57	165	362
TOR Switch - HPE SN2410M 48SFP28 8QSFP28	362	1234.42	1.57	165	362
OOB Switch - Aruba 6300M	75	255.75	0.33	56	75

Figura 58 – Power and BTU of appliances

The service offers the following advantages:

- *Reduced latency* → processing occurs closer to the data source, improving performance for IoT, analytics, and real-time applications.
- *Operational continuity* → edge sites remain functional even in the event of connectivity loss to the central datacenter.
- *Local data compliance* → data remains within specific geographic boundaries, enabling regulatory adherence.
- *Accelerated innovation* → new services can be deployed rapidly across multiple sites using centralized orchestration.
- *Unified management* → a single platform controls all edge and cloud resources. Lower operational costs through automation of provisioning and routine maintenance.

- *Modular scalability* → the edge infrastructure can be expanded quickly with new nodes. Enhanced security through consistent policies and centralized logging.
- *Architectural flexibility* → support for VM-based, containerized, and mixed workloads.
- *Operational efficiency* → standardized processes for deployment, updates, and governance.

5.2 Bulk Data Transfer

5.2.1 Supply Chain for Storage Hardware in the Service Context

The supply chain for the specialized storage hardware used in the context of this service is a meticulously orchestrated ecosystem designed to ensure reliability, scalability, and compliance with stringent enterprise standards.

The hardware components—primarily high-capacity storage appliances equipped with solid-state drives (SSD) or hybrid storage configurations—are sourced through a vetted network of global manufacturers and distributors, emphasizing compatibility, resilience, and sustained performance under demanding operational conditions.

Raw materials and core electronic components typically originate from certified suppliers with strict quality controls and compliance certifications, encompassing ISO standards for manufacturing and environmental responsibility. These parts undergo assembly and rigorous quality assurance testing in strategically located manufacturing centers equipped with state-of-the-art fabrication and diagnostics tools to meet the exacting requirements of enterprise-grade data transfer solutions.

The finished appliances are then integrated with proprietary firmware and security modules before being provisioned at distribution hubs. These hubs serve as staging areas where customization—such as encryption key injection, network configuration, and audit logging setup—is applied in accordance with customer-specific parameters and security policies. From there, logistics chains involve carefully coordinated transportation utilizing trusted carriers capable of maintaining chain-of-custody protocols, tamper-proof packaging, and real-time tracking until delivery to the client site.

This layered, end-to-end supply chain ensures that hardware is not only performant but also secure and fully traceable throughout its lifecycle, from component sourcing to customer deployment and eventual return for data ingestion and secure sanitization.

5.2.2 Software Architecture and Development

The software underpinning the service is architected and developed by a dedicated specialized team comprising systems architects, software engineers, and security experts. This team typically operates within a corporate research and development environment with a focus on distributed storage systems, secure data transfer protocols, and device management frameworks.

System architecture is designed to be modular, supporting scalability and interoperability with diverse enterprise environments and cloud storage backends. Software modules encompass embedded device firmware, secure boot and attestation layers, transfer orchestration engines, encryption key management subsystems, and centralized portals for device tracking, logging, and audit reporting.
Development activities are governed by agile methodologies, emphasizing iterative testing, continuous integration/continuous deployment (CI/CD) pipelines, and strict adherence to internal coding standards as well as external compliance frameworks such as SOC 2, ISO/IEC 27001, and GDPR where applicable.

Cross-functional teams collaborate closely with supply chain, security, and operations units to ensure that software updates are rigorously validated for reliability and security before full deployment.

5.2.3 Software Licensing, Transparency, and Adaptability

The software components of the service embody a balanced approach to licensing and intellectual property protection, combining proprietary elements with open-source frameworks to facilitate transparency, security scrutiny, and adaptability.

Core platform components leverage mature open-source libraries and protocols vetted by the community for security and performance, enabling rights for the client or partners to audit, adapt, and extend functionalities within defined license parameters (such as Apache 2.0, MIT, or similar permissive licenses).

For proprietary modules—particularly those dealing with encryption, device attestation, and logistics orchestration—customers and regulatory auditors are granted access to source code under non-disclosure agreements or via escrow arrangements to meet compliance and due diligence requirements. This ensures trust in the software stack’s integrity, fosters collaborative innovation in extended use cases, and mitigates vendor lock-in risks.

5.2.4 Security Patch Management Capabilities Independent of Non-EU Vendors:

To address geopolitical and regulatory concerns, the service provider maintains a robust local capability for developing, testing, and applying security patches independently of non-European Union (EU) vendors.

This strategy encompasses a dedicated European-based security engineering team integrated within the broader development organization, empowered to rapidly respond to emerging vulnerabilities and compliance directives. The team employs advanced vulnerability scanning, static and dynamic code analysis, and threat modeling tools supported by incident response program.

Patch development follows a rigorous lifecycle: discovery, analysis, coding remediation, multi-environment testing—including integration and regression—and staged rollout guided by well-defined risk criteria and communication protocols with customers.

This autonomous ecosystem reduces dependency on foreign-sourced software updates for critical security components, minimizes patching latency, and aligns with EU data sovereignty frameworks, reinforcing trust and operational continuity for customers with stringent data protection and audit requirements.

6 Reference Architecture

6.1 Kubernetes Reference Architecture

6.1.1 Overview

This reference architecture describes the recommended baseline design for running containerized applications on **Leonardo Cloud Leonardo Kubernetes Service (LKS)**. It provides a secure, scalable, production-ready foundation aligned with cloud best practices for networking, identity, security, observability, DevOps, and resilience.

This baseline architecture is suitable for most production workloads and is the recommended starting point for any Kubernetes deployment on Leonardo Cloud.

6.1.2 Architecture Components

6.1.2.1 Leonardo Kubernetes Service (LKS)

LKS provides a fully managed Kubernetes control plane offering:

- High-availability master nodes
- Automatic patching and upgrades
- Secure API endpoints integrated with Leonardo Cloud IAM
- Managed certificates and control-plane hardening
- Unified lifecycle management (create, scale, upgrade, delete)

Customers interact only with the Kubernetes API; Leonardo Cloud operates and secures the control plane.

6.1.2.2 Node Pools

Node pools provide the compute layer and support:

- System node pool → hosts core Kubernetes components
- Multiple pool types (CPU-optimized, RAM-optimized, GPU-backed)
- Auto-healing nodes
- Manual or automatic scaling
- Managed node image lifecycle

6.1.3 Network Architecture

6.1.3.1 Virtual Networks

LKS clusters are deployed into a **customer-managed Virtual Network (VNet)**. The recommended configuration includes:

- SubnetDescription → Control-plane subnet
- Restricted subnet for accessing the Kubernetes API (managed by Leonardo Cloud) → Node subnet(s)
- Hosts system and user node pools
- Ingress subnet
- Load-balanced entrypoints (public or private) → Private services subnet
- Internal services such as databases, caches, message brokers

Pod CIDR and service CIDR must not overlap with customer VNets.

6.1.3.2 Pod and Service Networking

Leonardo Cloud LKS uses a cloud-integrated CNI supporting:

- Stable pod IP allocation
- Network policy enforcement
- Native routing within the VNet
- Egress governance & logging

Service CIDRs provide stable virtual IPs for Kubernetes services.

6.1.3.3 Ingress & Load Balancing

Customers can expose applications via:

- *Layer-7 ingress* with managed controllers
- *Private internal load balancers*
- Public load balancers*, optionally fronted by a WAF

Ingress provides TLS termination, routing rules, and isolation between environments.

6.1.4 Identity & Access Control

6.1.4.1 Leonardo Cloud IAM Integration

LKS authentication is fully integrated with **Leonardo Cloud Identity and Access Management (IAM)**:

- SSO integration with enterprise identity providers
- Multifactor authentication
- Workload identities and service principals
- Role-based API access to cluster endpoints

Authorization uses Kubernetes RBAC and supports fine-grained controls.

6.1.4.2 Recommended RBAC Model

Typical baseline roles: - *Cluster Admins* → full administrative access - *Namespace Operators* → developer teams isolated by namespace - *Service Accounts* → least-privilege identities for workloads

Quota policies and network policies help enforce multi-tenancy boundaries.

6.1.5 Security Best Practices

6.1.5.1 Control Plane Security

- Fully isolated, managed, and hardened control plane
- Encrypted API traffic
- Optional **private-only cluster endpoints**
- Automated certificate rotation

6.1.5.2 Node and Runtime Security

- Leonardo Cloud hardened node OS image
- Automatic security and kernel patching
- Enforcement of Kubernetes Pod Security Standards
- Optional OPA/Gatekeeper policies
- Encrypted secrets using KMS integration

6.1.5.3 Network Security

- Built-in Kubernetes Network Policies
- Per-namespace ingress/egress control
- Integration with Leonardo Cloud Firewall
- Optional WAF for HTTP(S) ingress

6.1.5.4 Image Security

- Scanning in Leonardo Cloud Container Registry
- Support for image signing & attestation
- Policy-based enforcement for trusted registries

6.1.6 Resilience & Business Continuity

6.1.6.1 High Availability

- Multi-zone support for node pools (when available)
- Multiple replicas for control-plane components
- Pod anti-affinity & topology spread constraints
- Recommended use of Pod Disruption Budgets (PDBs)

6.1.6.2 Backups

Customers should:

- Use **Velero** for application-level backups
- Use Leonardo Cloud Storage snapshots for persistent volumes
- Perform regular recovery validation

6.1.6.3 Disaster Recovery

For mission-critical applications:

- Deploy across multiple clusters or regions
- Store manifests in Git for reproducible redeployment
- Use replicated or multi-zone storage classes
- Enable cross-region backup replication

6.1.7 Observability

6.1.7.1 Native Observability Integration

Leonardo Cloud LKS integrates with the **Leonardo Cloud Monitor** service, supporting:

- Node and pod metrics
- Container and system logs

- Alerts & dashboards
- Optional distributed tracing

Observability agents are automatically deployed in the system pool.

6.1.7.2 Customer Observability Options

You may deploy:

- Prometheus + Grafana
- Loki / Elasticsearch for logs
- Jaeger or Tempo for distributed tracing

All can ship logs and metrics to Leonardo Cloud Monitor.

6.1.8 DevOps & GitOps

6.1.8.1 Continuous Deployment

LKS supports:

- GitOps (Argo CD, Flux CD)
- CI/CD pipelines (GitHub Actions, GitLab CI, Jenkins, Azure DevOps, etc.)
- Helm + OCI registry integration
- Kustomize manifests

6.1.8.2 Recommended Practices

- Store manifests in Git (declarative infrastructure)
- Use GitOps for automated reconciliation
- Enforce policy-as-code in CI/CD pipelines
- Separate environments (dev, test, prod) with isolated namespaces and networks

6.1.9 Storage Architecture

6.1.9.1 Storage Classes

Leonardo Cloud provides multiple storage classes:

- *General Purpose SSD*

- *High-Performance NVMe*
- *Replicated Storage* for high availability

All support:

- Dynamic provisioning
- Persistent Volume (PV) expansion
- Snapshots and cloning

7 Data Centers Description

7.1 General architecture

The Cloud Services described in the relevant categories are hosted within 9 Data Centers distributed throughout Italy and spread across 3 Regions (A, B, and C), each redundant with three highly reliable Availability Zones.

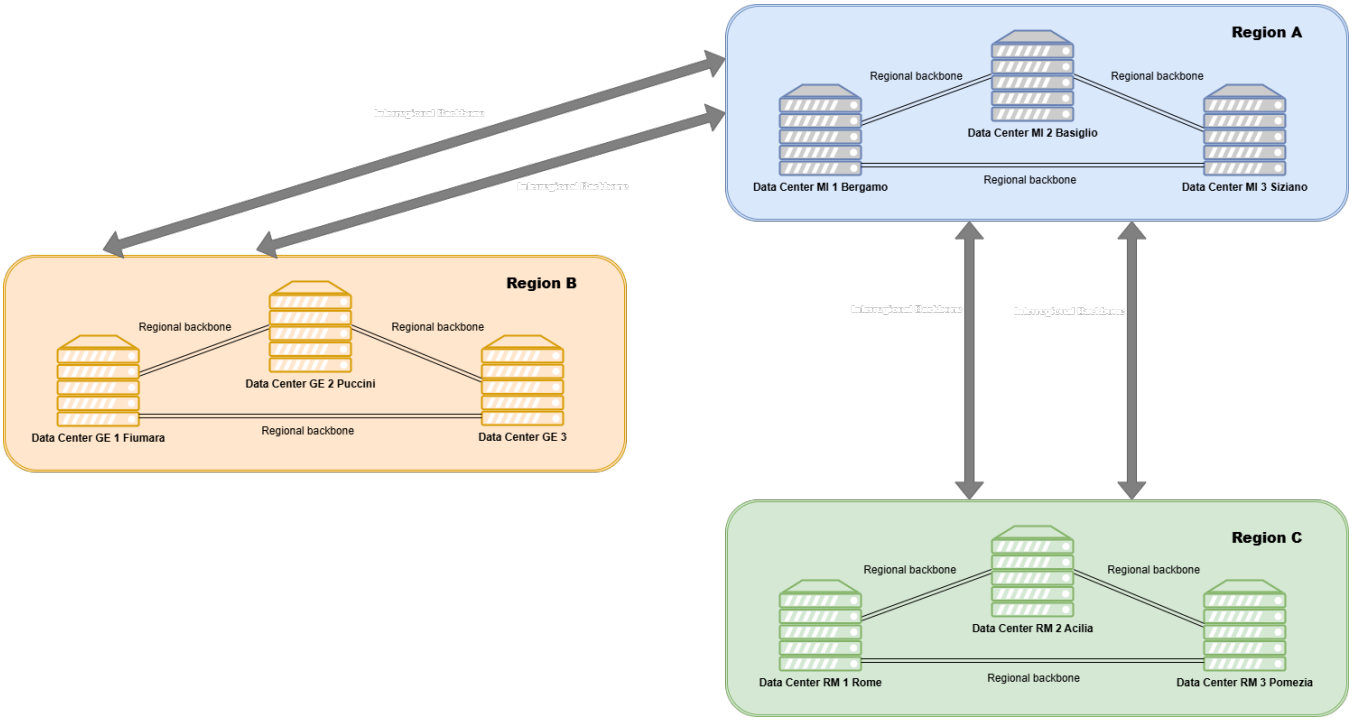


Figura 59 – Data Center Architecture and Interconnection

The infrastructure configuration is fully redundant thanks to the division of each of the three Regions, whose maximum distance exceeds 400 km. Each Region is composed of three Availability Zones (AZs), three Data Centers configured for business continuity, separated as the crow flies by tens of kilometers.

Specifically, the following table shows the DC association for each region:

Region	List of Data Centers
Region A	DC MI 1 Bergamo
Region A	DC MI 2 Basiglio

Region	List of Data Centers
Region A	DC MI 3 Siziano
Region B	DC GE 1 Fiumara
Region B	DC GE 2 Puccini
Region B	DC GE 3
Region C	DC RM 1 Rome
Region C	DC RM 2 Acilia
Region C	DC RM 3 Pomezia

Nomenclature of DCs for each Region

Below are the distances between each Region and between the DCs of each Region.

- Region A - Region B: distance more than 100 km
- Region A - Region C: distance more than 400 km
- Region B - Region C: distance more than 500 km
- DC MI 1 Bergamo - DC MI 2 Basiglio: approximate distance 53 km
- DC MI 1 Bergamo - DC MI 3 Siziano: approximate distance 54 km
- DC MI 2 Basiglio - DC MI 3 Siziano: approximate distance 10 km
- DC GE 1 Fiumara - DC GE 2 Puccini: approximate distance 10 Km
- DC GE 1 Fiumara - DC GE 3: approximate distance 15 Km
- DC GE 2 Puccini - DC GE 3: approximate distance 15 Km
- DC RM 1 Rome - DC RM 2 Acilia: approximate distance 30 km
- DC RM 1 Rome - DC RM 3 Pomezia: approximate distance 30 km
- DC RM 2 Acilia - DC RM 3 Pomezia: approximate distance 15 km

All data centers are equipped with all the technical and technological infrastructure necessary to ensure the highest quality standards in terms of reliability, availability, and physical security.

The three Availability Zones are interconnected via a dedicated regional backbone, which guarantees complete redundancy, negligible latency, and priority connectivity, logically characterizing the Regions as a single virtual Data Center (Software Defined Data Center).

The Regions are also interconnected via dedicated and reserved interregional backbones with IP/MPLS network transmission, enabling a flexible, software-defined logical network architecture, ensuring the mobility of application loads and the inherent high reliability of Cloud solutions. Within an Availability Zone, workloads are transparently distributed, and the HA (High Availability) configuration enables infrastructure service continuity (Business Continuity) between the three Data Centers in the same Region.

Thanks to this basic configuration, the Cloud platform will also provide data distribution between the three zones of each Region. This configuration is possible thanks to the distribution of storage space (identified with the best Storage Array technologies available on the IT market) within the three AZs and, therefore, thanks to the continuous replication of data for the service chosen by each individual organization. Therefore, if an individual organization decides to leverage the full redundancy of its infrastructure (physical or virtual), it can leverage the Cloud platform's HA configuration and create DR/BC solutions.

The unique nature of the Cloud platform, thanks to the backbone interconnecting the three AZs that make up each Region, will enable synchronous and asynchronous data replication between the Storage Array systems that make up the Storage Tier. In this operational context, the individual organization will benefit from the Cloud platform's inherent ability to reactivate workloads within one of the three AZs or in a different Region. Restarting workloads protected by the activated DR/BC solution will therefore allow the individual organization to independently manage the restart of each application, based on its own DR or BC plans.

7.2 Network description

The network is structured around three main components: Data Center Interconnection, Wide Area Network, and Local Area Network.

7.2.1 Data Center Interconnection (DCI)

Interconnection between the Data Centers relies on a high-capacity transport infrastructure built to ensure minimal latency, fault tolerance, and uninterrupted service.
Key elements include:

- IP/MPLS backbone, fully redundant and optimized for reliable, resilient routing.
- DWDM (Dense Wavelength Division Multiplexing) technology supporting high-capacity optical transmission with very low latency.
- VLAN-based segmentation, ensuring logical isolation of traffic domains and multi-tenant environments for different Organizations.
- Traffic management policies to regulate routing, priorities, and bandwidth allocation.

The DCI enables operation in a multi-region configuration with three Availability Zones, essential for high availability, synchronous/asynchronous replication, and business continuity.

7.2.2 Wide Area Network (WAN)

The WAN provides secure, high-performance connectivity to external networks, supporting access to the services.
It includes:

- Shared Internet connectivity, offering controlled access to the services.
- Traffic profiling tools for bandwidth management, flow optimization, and congestion prevention.
- IDS and APM systems, ensuring threat detection and performance monitoring.
- Additional services, such as:
  - Dedicated line aggregation.
  - VPN connectivity.
  - Special-purpose links for data migration.
  - Hosting of termination routers directly within the facilities.

The WAN ensures each Organization has isolated, secure channels for interacting with the infrastructure while maintaining high security and reliability.

7.2.3 Local Area Network (LAN)

Our cloud platform integrates a Software-Defined Networking (SDN) solution that allows customers to design and manage virtual networks directly from the management console.
Clients can define complex topologies, segment traffic, and configure IP addressing without interacting with physical infrastructure.

Technical Features:

- *Virtual network creation* → create virtual bridges and dedicated network segments to isolate environments (e.g., production, testing) and ensure traffic separation.
- *Dual-stack IPv4/IPv6 support* → each network can be configured with IPv4 and IPv6 addresses, with options to set dedicated gateways and custom subnets.
  - IPv4: static or DHCP configuration.
  - IPv6: support for static addresses and DHCPv6.
- *IP and routing management* → the console enables you to define IP ranges, gateways, and internal routing rules between subnets, without address translation functions.

- *Advanced segmentation* → support for VLAN tagging and isolated networks to ensure security and compliance.
  - Configurable VLAN IDs for each bridge.
  - Options for private and public networks.
- *Scalability and performance* → architecture optimized for low latency and high throughput, with the ability to add new networks and nodes without downtime.

Example Scenario

A customer can: 1. Create a private network with IPv4 (e.g., 10.0.0.0/24) and IPv6 (e.g., fd00::/64). 2. Connect multiple VMs and containers to the network via virtual bridges. 3. Define internal routing rules between subnets. 4. Add a VLAN to separate test traffic from production traffic.

Benefits:

- Self-Service: Everything managed from the console, no manual intervention.
- Flexibility: Custom configurations for each project.
- Compatibility: Full IPv4/IPv6 support.
- Integrated Security

7.3 Data Centers characteristics and technical specification

This section lists the general characteristics and technical specifications of the Data Center.

7.3.1 General requirements and site criteria

The architecture is designed to meet high standards for security, resilience, and sustainability, aligned with TIER III certifications and current regulatory requirements.
The Data Centers are selected and designed to reduce environmental and external risks:

- Located in seismic zones classified as zone ≥3.
- Sited away from coasts, major rivers, and heavily trafficked areas.
- Positioned near metropolitan zones while maintaining low risk.
- Equipped with independent power feeds, not derived from the same medium/high-voltage substation.

Compliance with key regulations is ensured.

7.3.2 Technical specifications

This section lists the technical specifications for each Data Center.

7.3.2.1 The Region A Data Centers

7.3.2.1.1 DC MI 1 BERGAMO

General specifications

- Total surface area: 17.600 m2
- Data hall surface area: 8.050 m2
- Number of independent data rooms: 10
- Secure location in terms of earthquakes
- Secure location in terms of hydro-geological risks

Building

- Height of the data hall: 3,5 m
- Height of upper plenum: 2,5 m
- Height of lower plenum: 2 m
- Load capacity of the floating floor : 2.000kg/m²(distributed load) 1.000 kg/m² (concentrated load in one place)
- External firewalls: REI 240
- Internal firewalls: REI 120
  - Double insulation with defrost system
  - Double loading bay

Certifications and compliance

- ANSI/TIA 942-B-2017 Rating 4 (formerly Tier 4)
- GO - Guarantee of Energy Origin
- Code of Conduct for Data Center Energy Efficiency
- ISO 9001 - Quality of services offered
- ISO 14001 - Environmental management system
- ISO 22237 - Data centre facilities and infrastructure
- ISO 27001 - IT security
- ISO 50001 - Energy management system
- ISO/IEC 27017 – Cloud security controls

- ISO/IEC 27018 – Managing personal data on the Cloud
- ISO/IEC 27035 – Managing security incidents and events

Connectivity

- Point of entrance: 4
- Entrance Room: 2
- Main Distribution Area (MDA): 2
  - Carrier neutral data center
  - Provision of managed connectivity
  - Dual transmission system to Milan Internet eXchange (MIX)

Energy

- Connection points to utilities: 2
- Total power: 12 MW IT 2N (redundant)
- UPS redundancy: 2N+1
- UPS type: double conversion static
- Individual UPS power: 500kVA
- UPS run time: 15 minutes at full power on single module in emergency conditions - 40 minutes in standard conditions
- Generator redundancy: 2N
- Generator type: diesel generator units
- Full load run time: 26h in emergency conditions, 52h in standard conditions

Cooling

- Cooling type: Chilled water - - water to water - water to air system
- Normal mode: Ground water cooling system
- Redundancy of heat exchangers: 2N
- Groundwater extraction wells: 5
- Emergency mode: air/water chiller
- CRAH redundancy: 2N

Security

- CCTV
- 24/7/365 security
- Separate parking for employees/visitors
- Vehicle bollards
- Separate entrance gates for visitors/goods
- Mantrap for visitors and goods with anti-tailgating and antipiggybacking systems
- Network Operations Center (NOC)
- Security Operations Center (SOC)
- Facility Operations Center (FOC)
- Building Management System (BMS)

Fire prevention system

- Air replacement: 2vol/h
- Extinguishing system: inert gas
- Extinguishing gas: IG-541
- Redundancy of extinguishing cylinders: 2N
- Highly sensitive smoke detection system
- Liquid loss detection system
- Fire detection and extinguishing system in each single module
- Standalone system on every generator unit

7.3.2.1.2 DC MI 2 BASIGLIO

General specifications

- Colocation Space: 2.380 m².
- Global uptime average of >99,999%
- Energy: covered by 100% renewable energy

Building

- Building type: 4-floor concrete structure
- Floor type: Raised floor
- Floor load capacity: 1.500 kg/m²

- Parking: Adjacent to building (free)
- Seismic design: low seismic category.
- Flood zone: not applicable

Certifications and compliance

ISO Standards: - ISO 9001 - ISO 22301 - ISO 27001 - ISO 45001 - ISO 14001 - ISO 50001

Other Certifications: - Cyber Essentials - PCI DSS - SOC 1 Type II - SOC 2 Type II - EU Code of Conduct

Connectivity

- Access to 30+ carriers across the Milan metro ecosystem
- Direct peering through Equinix Internet Exchange™.
- Direct connectivity via Equinix Fabric® to distributed digital infrastructure
- Access to MIX, TOP-IX and other interconnections at Via Caldera, Milan

Energy

- Utility feeders: 1 × 3 MVA electrical feed
- PS configuration: N+N
- UPS redundancy: N+1
- Standby power configuration:
  - 2 × 1,900 kVA diesel generators (mechanical load)
  - 4 × 1,400 kVA diesel generators (IT load)
- Standby power redundancy: N+N.
- Power density: 1.0–7.0 kVA per cabinet

Cooling

- Cooling configuration: Chilled water system
- Cooling redundancy: N+1

Security

Physical Security:

- Mantrap entry
- Proximity access card + PIN

Human Security:

- 24/7 on-site security officers

Electronic Security:

- PIN and card readers
- Optional biometric readers for customer cages
- CCTV with 7-day video retention
- Motion detection

Fire prevention system

Detection:

- VESDA
- HSSD (High Sensitivity Smoke Detection)
- Visual and audio alarms
- Double-knock activation

Suppression agents:

- Novec
- FM200
- Argon

7.3.2.1.3 DC MI 3 SIZIANO

General specifications

- The campus in Siziano (PV) hosts all hosting and cloud infrastructure used by CoreTech
- Designed according to Tier IV multi-tenant data center standards offering unmatched connectivity
- Located within a 100.000 m² campus, hosting Italy's largest and most advanced data center
- Building footprint is 42.000 m²
- Designed for 100% Power & Cooling guaranteed uptime
- Highly focused on energy efficiency, using advanced cooling and climatization technologies.

Building

- Constructed according to NTC anti-seismic regulations (D.M. 14/01/2008)

- Double roof resistant to winds up to 280 km/h
- Intumescent-coated metal structure for fire resistance
- Perimeter walls of the technical area built to REI120 standards
- Flood-mitigation measures:
  - 3 m-high perimeter wall, waterproofed up to 1,5 m
  - Building elevation +1 m above primary urban level
  - Rain-water balance basin for extreme weather events
  - No water pipes inside the DC (air-based cooling)
- Infrastructure benefits from 218 patented technologies (granted or pending)

Certifications and compliance

- ISO 9001:2015 – Quality Management
- ISO 14001:2015 – Environmental Management
- OHSAS 18001 – Health & Safety Management
- ISO 27001:2013 – Information Security Management
- ISO 50001:2011 – Energy Management
- ANSI/TIA-942-B:2017 – Rating 4 (Tier IV)

Connectivity

- 100 fiber pairs with diversified routes in multi-carrier configuration provide connectivity to each data hall
- All structured cabling (fiber, copper, electrical) runs through dedicated overhead trays

Energy

- Campus powered by a redundant 132 kV high-voltage line, supporting up to 40 MW at full capacity
- Tri-redundant UPS system ensuring 100% availability
- Electrical system engineered for Tier IV “system + system” (2N+1) requirements
  - Two completely independent electrical systems
  - Each capable of supporting the full facility load
  - Includes independent UPS, Bypass Modules, PDUs, RPPs
- Racks receive dual power feeds (Feed A + Feed B), each from separate electrical systems.

Cooling

- Cooling system based on modular AHUs (Air Handling Units)
- Utilizes indirect evaporative cooling, with air-to-air heat exchangers cooled by external water systems
- Designed to achieve PUE < 1.4 (estimated)
- Steel infrastructure under the T-SCIF serves as a thermal flywheel to increase resilience

Security

Physical Security:

- Multilevel badge + numeric code access control
- 24/7/365 security personnel and anti-intrusion systems.
- CCTV video surveillance with digital archiving (privacy-compliant)

Data Hall Security:

- 4 data halls (expandable to 6), up to 1,056 racks per hall
- Racks organized into T-SCIF islands (Thermal Separate Compartment in Facility)
  - Complete separation of hot and cold airflows
  - Cage-protected
  - Maximizes density and thermal efficien

Fire prevention system

- Intumescent paint on metal structures
- REI120 fire-resistant perimeter walls around technical areas
- Part of the electrical and environmental risk-mitigation strategy includes fire-resistant compartmentalization

7.3.2.2 The Region B Data Centers

7.3.2.2.1 DC GE 1 FIUMARA

Building

Tier II classification.

Certifications and compliance

ISO 27001.

Connectivity

Two redundant Dark fiber link 100 + 100 GB between GE1 and GE2.

Energy

The Data Center has two power supply branches, A and B, that reach the same substation, capable of delivering up to 1 MW (500 kW + 500 kW).
The substation is served by:

- 3 x 1600 kVA transformers
- 1 medium voltage main switchboard.
- 2 low voltage switchboards.
- An 824 kW generator.
- A 320 kW UPS.

The work to bring the DC system into TIER III standards will be completed in 2026.

Cooling

It features an air cooling type cooling system composed of 7 CDZ with Water technology (with the use of Chilled) + Liquid cooling.

Security

Security levels implemented:

- Perimeter walls
- Reception
- Internal VDS system at the data center
- Fingerprint or badge access
- Internal armed surveillance system, 24/7.

Fire prevention system

Gas and NOVEC 1230 primer.

7.3.2.2.2 DC GE 2 PUCCINI

Building

It was built on TIER III logic.

Certifications and compliance

ISO 27001.

Connectivity

Two redundant Dark fiber link 100 + 100 GB between GE1 and GE2.

Energy

It has two certification branches, A and B.
Currently, depending on the air conditioning units installed, the DC can accommodate a maximum of 340 kW of IT computing power.
The characteristics of the two branches are as follows:

- Branch A characteristics:
  - DATA CENTER BRANCH "A" Distribution Cabinet
  - 1 1000 kW transformer
  - 1 LV main panel
  - Equivalent earthing system connected to the main earthing system.
  - 1 576 kW Milantractor generator.
  - 1 UPS sized as follows:
  - 1 Piller 500 kW rotary unit each.
- Branch B characteristics:
  - DATA CENTER BRANCH "B" Distribution Cabinet
  - 1 1000 kW transformer
  - 1 LV main panel
  - Equivalent earthing system connected to the main earthing system.
  - One 500 kW Perkins generator.
  - One 576 kW Spark generator for air conditioning only.
  - One UPS sized as follows:
  - One 500 kW Piller rotary generator.

Cooling

It has an Air cooling system composed of 6 CDZs with mixed Water (with the use of Chilled) and Gas technology.

Security

Security levels implemented:

- Perimeter walls
- Reception
- Internal VDS system at the data center
- Fingerprint or badge access
- Internal armed surveillance system, 24/7.

Fire prevention system

Water mist.

7.3.2.2.3 DC GE 3

General specifications

Landing of Blue & Raman submarine cables.
BlueMed system with branches between Italy, Africa, Europe, and the Middle East.
Infrastructure designed to support up to six new submarine cables in the future via the Genoa Landing Platform.

Certifications and compliance

- Multiple ISO certifications, including: ISO 9001, ISO 14001, ISO 45001, and ISO 27001

Connectivity

The data center has an active IP node for IP transit services. The IP node is integrated with Sparkle's global Tier-1 Seabone backbone.
Submarine cables: the facility supports or plans to support multiple undersea cable systems, including BlueMed, Blue & Raman, and Unitirreno.
Interconnection / IX: The landing hub provides access to local IX ecosystems and supports peering; it is aligned with the local Ge-DIX Internet Exchange.

Energy

The data center is designed with environmental sustainability in mind.
Total installed power of 4.7 MW.

Cooling

Use of advanced cooling systems (including "green" techniques) and lithium-ion batteries.

Security

- Digital security: Sparkle's corporate commitment includes security management aligned with ISO 27001.
- Services offered (security layer): the site supports DDoS protection and virtual NAP capabilities.

7.3.2.3 The Region C Data Centers

7.3.2.3.1 DC RM 1 ROME

General specifications

- Total surface area: 10.730 m²
- Data hall surface area: 3.120 m²
- Number of independent data rooms: 6
- Floors on which the server rooms are distributed: 3
- Secure location in terms of earthquakes
- Secure location in terms of hydro-geological risks

Building

- Height of the data hall: 3,5 m
- Height of upper plenum: 1,4 m
- Height of lower plenum: 1,95 m
- Load capacity of the floating floor: 2.000 kg/m² (distributed load) - 1.000 kg/m² (concentrated load in one place)
- External firewalls: REI 240
- Internal firewalls: REI 120
- Double insulation with defrost system
- Double loading bay

Certifications and compliance

- ANSI/TIA 942-C-2024 Rating 4 (formerly Tier 4)
- ISO 9001 - Quality of services offered
- ISO 14001 - Environmental management system
- ISO 22237 - Data Center Lifecycle Management
- ISO 27001 - IT security
- ISO 45001- Workplace health and safety management system
- ISO 22301 - Business Continuity management system

- ISO 20000-1 - IT services management

Connectivity

- Point of entrance: 6
- Entrance Room: 2
- Main Distribution Area (MDA): 2
  - Carrier neutral data center
  - Provision of managed connectivity

Energy

- Total power: 6 MW IT 2N (redundant)
- UPS redundancy: 2N+1
- UPS type: double conversion static
- Individual UPS power: 500 kVA
- UPS run time: 15 minutes at full power on single module in emergency conditions - 30 minutes in standard conditions
- Generator redundancy: 2N
- Generator type: diesel generator units
- Full load run time: 24h in emergency conditions, 48h in standard conditions, refill within 12h

Cooling

- Cooling type: Chilled water - water to air system
- Normal mode: air/water chiller to indirect free cooling
- Chiller redundancy: 2N
- CRAH redundancy: 2N

Security

- CCTV
- 24/7/365 security
- Separate parking for employees/visitors
- Vehicle bollards
- Separate entrance gates for visitors/goods

- Mantrap for visitors and goods with anti-tailgating
- Network Operations Center (NOC) 24/7/365
- Security Operations Center (SOC) 24/7/365
- Facility Operations Center (FOC) 24/7/365
- Building Management System (BMS)

Fire prevention system

- Air exchange: 2vol/h
- Extinguishing system: inert gas Extinguishing gas: IG-541
- Redundancy of extinguishing cylinders: 2N
  - Highly sensitive smoke detection system
  - Underfloor liquid loss detection system
  - Fire detection and extinguishing system in each single module
  - Standalone system on every generator unit

7.3.2.3.2 DC RM 2 ACILIA

General specifications

- Total surface area: 8.000 m²
- Powered by two separate medium-voltage lines, each coming from distinct ACEA substations, ensuring electrical redundance

Certifications and compliance

- Certified at Tier IV level, the highest standard for redundancy and uptime
- It holds ANSI/TIA-942 Rating 4 for facility design
- Management and operations standards include:
  - ISO 50001 (energy management)
  - ISO 14001 (environmental management)
  - ISO 27001 (information security)
  - ISO 20000-1 (IT service management) and ISO 22301 (business continuity)
  - ISO 9001 (quality management)
- The facility adheres to the European Data Center Code of Conduct for energy efficiency.

Connectivity

- It uses dual-ring fiber connectivity via two distinct Points of Entry (POEs), connecting to an optical backbone through POPs both located in Rome.
- The internal campus distribution ensures physically separate fiber paths between POEs and the meet-me rooms / data halls.
- The three AZs in Region A are interconnected via DWDM (Dense Wavelength Division Multiplexing) links, at high capacity, with a proprietary backbone for redundancy and low-latency.

Energy

- It is powered with 100% renewable energy, aligning with TIM's sustainability targets.
- An onsite photovoltaic installation providing up to 75,000 W (75 kW) capacity.
- Energy management systems are real-time: the infrastructure monitors electrical and thermal parameters to drive predictive maintenance and efficiency optimizations.

Cooling

- The cooling architecture uses air delivered via raised floor systems, with return air collected in alternating ceiling plenums.
- It includes free-cooling, using external air when conditions allow, to reduce the energy used by mechanical refrigeration.
- Geothermal heat exchangers (ground-based dispersers) are used for heat rejection from chillers when needed.
- A Building Management System (BMS) monitors temperature, humidity, and airflow to optimize when and how cooling is deployed

Security

- External and internal fencing, with anti-climb perimeter protection.
- Armed security guard presence.
- Video surveillance (CCTV) throughout the site.
- Pedestrian access is controlled by security mantraps / turnstiles.
- Intrusion detection systems (perimeter alarms) and corner / glass protection: the windows are blast-resistant / reinforced.
- Internal security patrols / rounds.
- Access to critical system rooms (data halls) is through security airlocks (bussole) and requires badge-based dual authentication.

- Cybersecurity: the infrastructure is monitored by a Security Operation Center (SOC), providing continuous threat detection.
- The facility complies with the PSN’s Technical Security Measures (MTMS), which define guidelines for logical segmentation, risk management, and protection

Fire prevention system

- The Data Center is equipped with Very Early Smoke Detection Apparatus (VESDA) or similarly sensitive smoke detection systems to detect fire in its early stages
- The fire suppression uses 3M Novec 1230 as the extinguishing agent: it's electrically non-conductive, volume-expanding, and designed to absorb heat to inhibit the combustion reaction.
- The fire suppression system has redundancy to provide 2N (fully redundant) coverage and ensure reliability in case of activation

7.3.2.3.3 DC RM 3 POMEZIA

General specifications

- The campus comprises a total area of ~51.000 m², with 13 system-rooms and 6 telecom rooms

Building

- The PISP building within Pomezia is elevated and built with a 0.9 m raised floor, offering enhanced protection in case of flooding
- Power is provided via two separate 20 kV medium-voltage lines from an ACEA substation, giving high reliability and redundancy
- The primary electrical distribution is designed with redundancy: primary distribution uses an N+1 logic, while secondary distribution is a+b (or N+1) with dual radial path

Certifications and compliance

- The data center meets Uptime Institute Tier III standard
- It has ANSI/TIA-942 Rating 3 certification for facility design
- The system is compliant with multiple ISO standards: ISO 50001 (energy management), ISO 14001 (environmental management), ISO 9001 (quality), ISO 27001 (information security), ISO 22301 (business continuity)

Connectivity

- Connected via a dual-fiber ring: two independent paths link it to main ISP'score network via the POPs both located in Rome

- The internal campus network ensures physically separate fiber routes between Points of Entry (POEs), meet-me rooms, and system rooms for redundancy

Energy

- The electrical supply uses redundant medium-voltage (20 kV) lines, ensuring high availability
- It uses two diesel generators plus two DRUPS (UPS + generator combo) for backup power
- Fuel storage: there are two 15,000-litre double-walled diesel tanks with leak detection, strictly for emergency use
- It aims for sustainability: adhere to green energy standards.

Cooling

- The cooling system is built with dual-loop refrigerant circulation (two independent loops) to remove heat efficiently across the campus
- On the rooftop, there are redundant chillers (N+1), ensuring that if one fails, thermal rejection can continue without service interruption
- Inside the system rooms, there are approximately 120 air-conditioning units to manage local heat load

Security

- Physical security is multilayered: perimeter protection, intrusion detection, surveillance, and access control
- Access to sensitive rooms is controlled through security airlocks (“mantraps”) and requires badge-based authentication
- Cybersecurity is managed through a Security Operation Center (SOC), with continuous monitoring, threat detection, and incident response

Fire prevention system

- The security manual (MTMS) mandates very early smoke detection systems to detect fire risk promptly
- Fire suppression likely uses inert, clean agents suitable for data centers, to avoid damaging sensitive IT gear
- The fire protection architecture is designed with redundancy, according to high-availability and resilience standards

8 Service Price List

This section contains the price lists of the services for each family.

For each service, you can choose from three alternative purchase options:

- *Monthly Subscription* with bimonthly payment in arrears;
- *Annual Reserved Subscription* with upfront payment upon activation and testing of the service;
- *Three-year Reserved Subscription* with upfront payment upon activation and testing of the service.

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Compute	Pool Small (Confidential)	Hosts number	3 Host Number (2x 24 Core CPU - 512 GB RAM - 32 TB SSD)	21.586,03 €	233.129,08 €	621.677,54 €
Compute	Pool Medium (Confidential)	Hosts number	6 Host Number (2x 24 Core CPU - 512 GB RAM - 32 TB SSD)	34.560,46 €	373.252,97 €	995.341,26 €
Compute	Pool Large (Confidential)	Hosts number	9 Host Number (2x 24 Core CPU - 512 GB RAM - 32 TB SSD)	47.344,20 €	511.317,32 €	1.363.512,84 €
Compute	Pool X-Large (Confidential)	Hosts number	12 Host Number (2x 24 Core CPU - 512 GB RAM - 32 TB SSD)	62.304,31 €	672.886,55 €	1.794.364,13 €
Compute	VM Small (Confidential)	Resource instance	2 VCPUs, 4 GB RAM per instance	37,25 €	402,30 €	1.072,80 €
Compute	VM Medium (Confidential)	Resource instance	4 VCPUs, 8 GB RAM per instance	72,00 €	777,60 €	2.073,60 €

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Compute	VM Large (Confidential)	Resource instance	8 VCPUs, 16 GB RAM per instance	133,00 €	1.436,40 €	3.830,40 €
Compute	VM X-Large (Confidential)	Resource instance	16 VCPUs, 32 GB RAM per instance	413,50 €	4.465,80 €	11.908,80 €
Compute	Kubernetes Confidential Computing	Node worker	15 node workers with 8 GB RAM	10.499,77 €	113.397,52 €	302.393,38 €

Price list of the Compute Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Security	Identity & Access Management (IAM) Service	concurrent Users	100 concurrent users	454,59 €	4.909,58 €	13.092,20 €
Security	Key Vault as a Service - Standard	Client	500 clients	18.508,98 €	199.896,94 €	533.058,50 €
Security	Endpoint Protection	Endpoint	100 endpoints	7.774,28 €	83.962,25 €	223.899,33 €
Security	NGFW Platform	Throughput (Gbps)	1	1.148,53 €	12.404,11 €	33.077,64 €
Security	PAM (Privileged Access Management)	Number of admin users	10	2.801,62 €	30.257,50 €	80.686,66 €
Security	Intrusion Prevention System (IPS)	Throughput(Gbps)	1	7.541,19 €	81.444,88 €	217.186,36 €

Price list of the Security Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Middleware	PaaS API Management	Request	500M API request	24.900,56 €	268.926,08 €	717.136,23 €
Middleware	Functions As A Service (FAAS)	VCPU	100 VCPUs	6.315,12 €	68.203,33 €	181.875,55 €
Middleware	Jboss as a Service	Container	4 VCPUs-8GB RAM per container	537,78 €	5.808,04 €	15.488,10 €
Middleware	Spring boot as a Service	Container	16 GB RAM for container	651,62 €	7.037,54 €	18.766,76 €
Middleware	PaaS Business Process as a Service	Istance	8 VCPUs-16 GB RAM per istance	12.755,33 €	137.757,60 €	367.353,61 €
Middleware	PaaS CMS as a Service	User	1000 users	5.722,14 €	61.799,09 €	164.797,57 €
Middleware	Semantic Knowledge Search	Container	8 VCPUs-16 GB RAM per container	244,06 €	2.635,81 €	7.028,84 €

Price list of the Middleware Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Data Protection	Backup Platform	TB	1	30,52 €	329,62 €	879,00 €

Price list of the Data Protection Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Infra & Ops Platform	Multicloud Management Platform	Volume	Managed <1MEuro or 5 TB RAM	8.621,22 €	93.109,16 €	248.291,09 €

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Infra & Ops Platform	IT infrastructure Service Operations (Logging & Monitoring)	GB	1GB for data storage	244,06 €	2.635,81 €	7.028,84 €
Infra & Ops Platform	PaaS Ticket Management Service	Number of Service Desk Operators	50 operators	7.136,65 €	77.075,77 €	205.535,38 €
Infra & Ops Platform	PaaS Operations Management	Concurrent users	25 concurrent users	13.899,53 €	150.114,91 €	400.306,42 €

Price list of the Infra & Ops Platform Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
DevSecOps	Configuration Manager	Managed worker	25 managed workers	494,25 €	5.337,86 €	14.234,29 €
DevSecOps	Test Automation	User	10 automation testers-concurrent, 5 Robots	13.057,79 €	141.024,08 €	376.064,22 €
DevSecOps	Quality Code Analysis	lines codes	1M lines codes	8.486,66 €	91.655,89 €	244.415,71 €
DevSecOps	DevSecOps As A Service	User	100 Users Ultimate/500 Users premium/2000 Free	25.006,90 €	270.074,54 €	720.198,78 €
DevSecOps	Qualizer DevSecOps	Project	10 Projects	10.010,65 €	108.115,00 €	288.306,67 €

Price list of the DevSecOps Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Big Data	Data Lake	TB	1 TB	25,23 €	279,00 €	744,00 €
Big Data	Data Lake-Cold	TB	1 TB	23,25 €	251,10 €	669,60 €
Big Data	Business Intelligence Platform	User	100 users	8.365,83 €	90.351,00 €	240.936,01 €
Big Data	PaaS ETL Batch/Real time Processing	Worker node	16 vCPU-128 GB RAM per worker	608,48 €	6.571,54 €	17.524,11 €
Big Data	Event Message	Worker node	16 vCPU-128 GB RAM per worker	291,29 €	3.145,95 €	8.389,20 €
Big Data	Data Governance	User	10 users	461,45 €	4.983,68 €	13.289,82 €

Price list of the Big Data Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
AI	Speech to Text	GPU	1 partition H200	2.819,93 €	30.455,25 €	81.214,00 €
AI	PaaS-AI Audio Analytics	GPU	1 GPU partition H200	219,65 €	2.372,23 €	6.325,95 €
AI	PaaS-AI Video Analytics	GPU	1 GPU H200	648,28 €	7.001,38 €	18.670,35 €
AI	OCR	Container	16 GB RAM per container	1.109,42 €	11.981,77 €	31.951,40 €
AI	Text Analytics/NLP	GPU	1 partition H200	393,54 €	4.250,25 €	11.334,00 €
AI	Translation	GPU	1 GPU H200	18.247,86 €	197.076,90 €	525.538,40 €
AI	AI Search-RAG	GPU	1 GPU H200	23.305,31 €	251.697,33 €	671.192,88 €

Leonardo Cyber & Security Solutions

3 Dec 2025
01.00
Secure Cloud Management Platform

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
AI	AI Platform	GPU	1 GPU H200	1.281,30 €	13.838,03 €	36.901,40 €
AI	AI SLM	GPU	1 partition GPU H200	6.896,91 €	74.486,63 €	198.631,00 €
AI	AI LLM	GPU	1 GPU H200	30.824,01 €	332.899,28 €	887.731,41 €

Price list of the Artificial Intelligence (AI) Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Collaboration	Instant Messaging	Users	1000 users	67.785,44 €	732.082,73 €	1.952.220,60 €

Price list of the Collaboration Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Database	PaaS SQL-PostgreSQL	DB Instance	4 vCPUs-16 GB RAM per instance(with replication)	550,42 €	5.944,50 €	15.851,99 €
Database	PaaS SQL-MariaDB	DB Instance	4 vCPUs-16 GB RAM per istance(with replication)	601,71 €	6.498,45 €	17.329,20 €
Database	PaaS SQL-MS SQL Server EE	DB Instance	8 vCPUs-16 GB RAM per instance	4.909,78 €	53.025,66 €	141.401,76 €
Database	PaaS SQL-MS SQL Server EE (BYOL)	DB Instance	8 vCPUs-16 GB RAM per instance	212,27 €	2.292,49 €	6.113,31 €
Database	PaaS GraphDB	DB Instance	4 vCPUs-16 GB RAM per instance	1.873,84 €	20.237,47 €	53.966,58 €

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Database	PaaS NoSQL-MongoDB	DB Instance	4 vCPUs-16 GB RAM per istance(with replication)	1.172,65 €	12.664,62 €	33.772,33 €
Database	PaaS In Memory-Redis	DB Instance	4 vCPUs-16 GB RAM per istance	1.873,84 €	20.237,47 €	53.966,58 €

Price list of the Database Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Networking	PaaS CDN (Content Delivery Network)	Throughput 10 Gbps(inbound & Outbound)	10	566,00 €	6.112,80 €	16.300,80 €
Networking	PaaS Domain Name System (DNS)	DNS Instance	1	3.899,57 €	42.115,37 €	112.307,66 €
Networking	Single public IP	#Public IP	1	4,67 €	50,40 €	134,40 €
Networking	L7 Load Balancer (regional)	Instance	1	994,08 €	10.736,04 €	28.629,43 €
Networking	Cloud interconnect Gold SW (10 Gbps max throughput)	Throughput(Gbps)	10	9.112,76 €	98.417,78 €	262.447,40 €

Price list of the Networking Family Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Storage	Block Storage (1000 GB) - High Density	GB	1000 GB	107,24 €	1.158,24 €	3.088,65 €

Leonardo Cyber & Security Solutions

3 Dec 2025

01.00

Secure Cloud Management Platform

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Storage	Archive Storage (1000 GB)	GB	1000 GB	96,52 €	1.042,42 €	2.779,78 €

Price list of the Storage Services

Family	Service	Unit	Value	PAYG (Monthly)	1Y Reserved	3Y Reserved
Hybrid	Edge Location-Pool Small (Confidential)	Host number	3 Hosts of: 2x24 Core CPU-512 GB RAM-32 TB SSD	21.586,03 €	233.129,08 €	621.677,54 €

Price list of the Hybrid Services

9 Service Provisioning

In this section you can find information about the provisioning of the services offered, depending on their type.

9.1 Creation of Provisionings

9.1.1 Provisioning of "Physical Resources"

Generally, service provisioning is done through the Leonardo Security Cloud Management Platform console. Using the tabs in the console's provisioning functionality, you can view lists of provisionable resources, such as Virtual Machines, Storage, and Kubernetes.
The features available for these items are identical; only the parameters entered during creation differ.

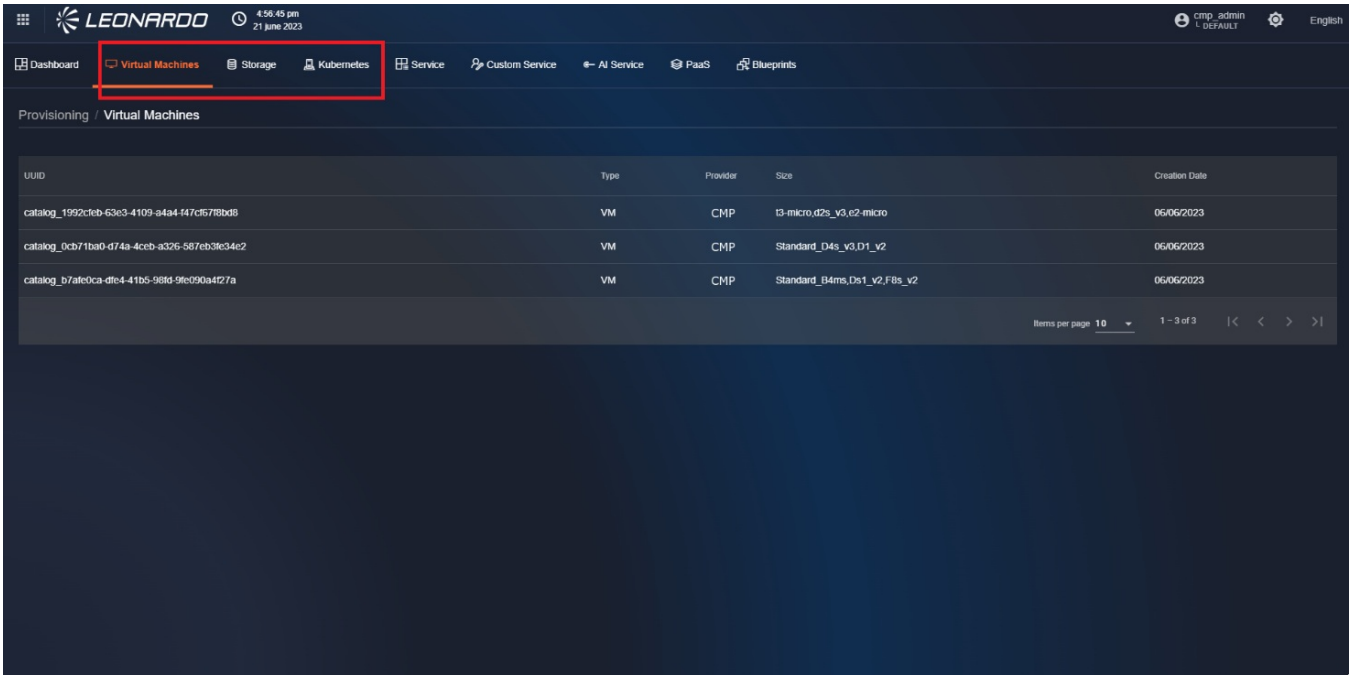


Figura 60 – Tabs for resource creation

9.1.2 Provisioning of Virtual Machines

To start provisioning a resource, click on the corresponding row to view the page containing step 1 of provisioning creation. In this step, it is necessary to select, using the dropdown on the left, the "target" subsystem where the resources are to be provisioned. Once selected, an information mirror will be displayed on the right indicating the characteristics of the resource that will be provisioned. To continue, click the "Next" button at the bottom right to go to step 2 "Config" page.

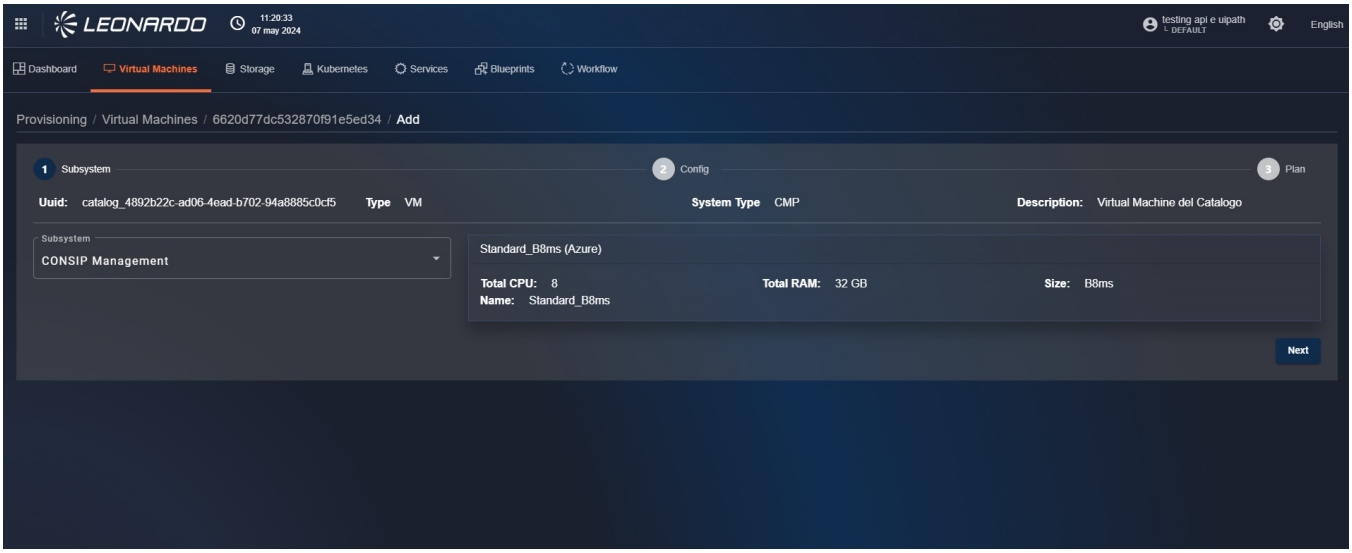


Figura 61 – Selection of the “target” subsystem, provisioning step 1

On the "Config" page of step 2, fill in all mandatory fields in all sections of the form. At the bottom left, click the "Reset" button to reset all fields on the page.

Instead, on the right, click the "Submit" button to go to step 3 "Plan".

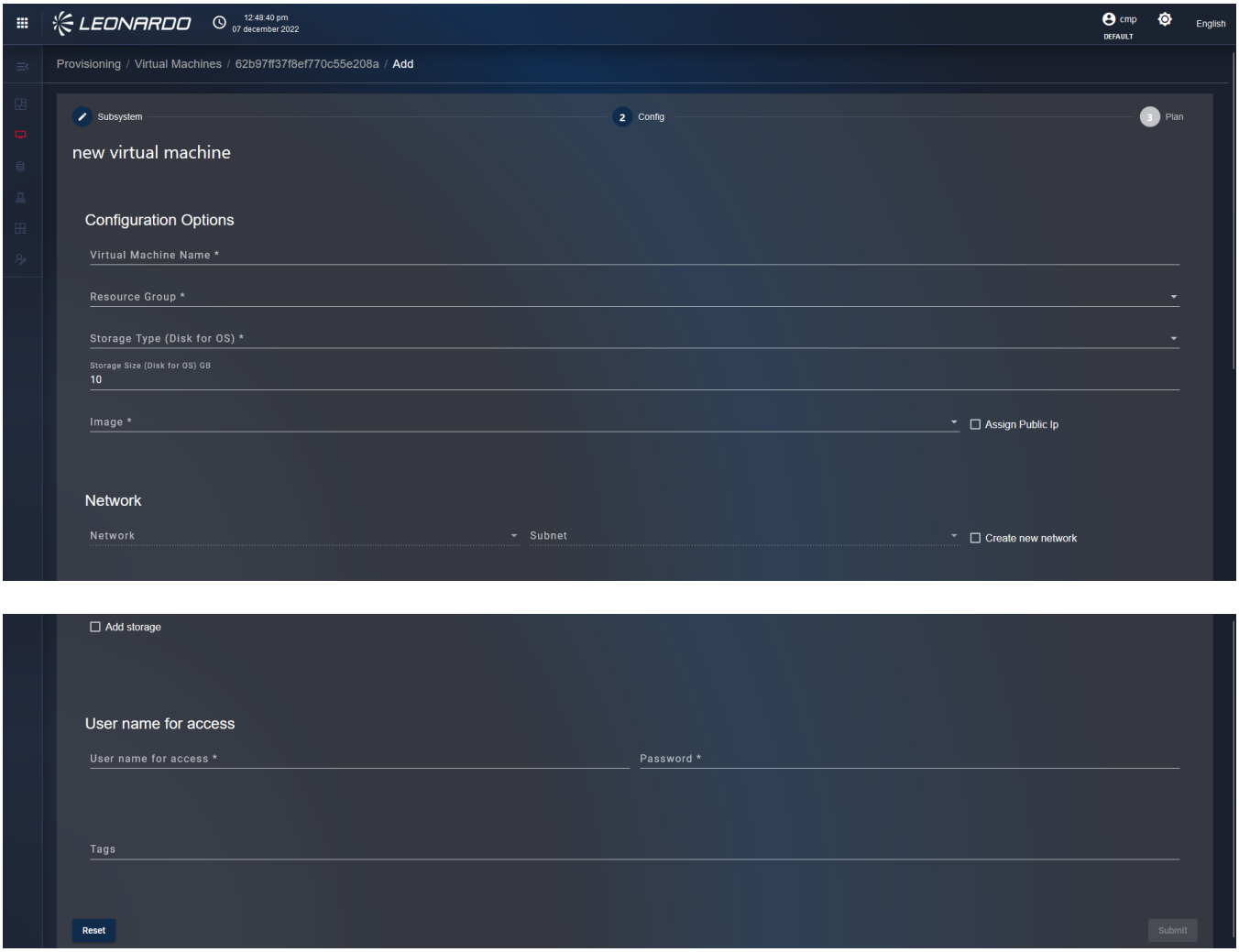


Figura 62 – Filling in the resource prediction form fields

After clicking the "Submit" button, the user is redirected to the "Plan" page of step 3 where we can view the provisioning plan sent by Terraform, which indicates all the parameters of the resources that will be configured, and at the bottom, there is a list with a cost perspective.

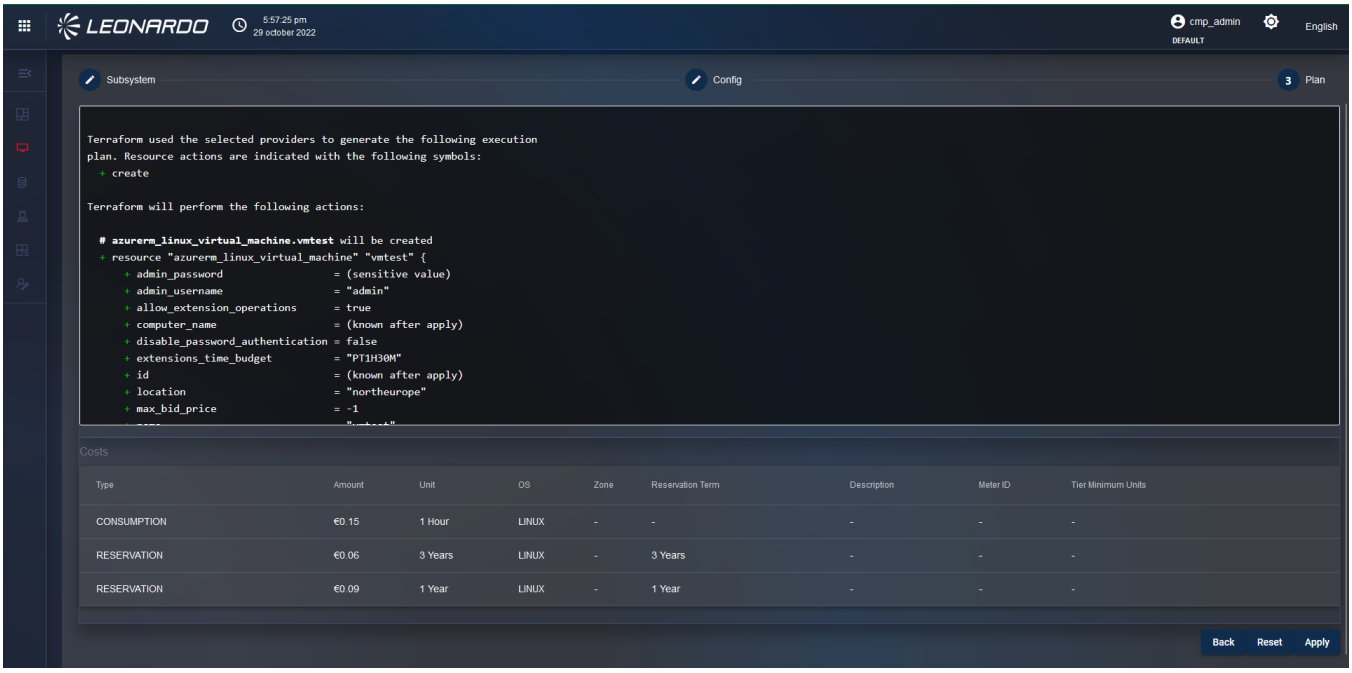


Figura 63 – Forecast screen

Still from the "Plan" page of step 3, at the bottom right, there are three buttons: "Back", "Reset", and "Apply". If you click the "Back" button, the user returns to the "Config" page of step 2 where parameters can be modified.

If you click the "Reset" button, the user is redirected to the "Subscription" page of step 1 where it is necessary to select a subsystem, and then enter the parameters on the "Config" page of step 2.

Finally, if you click the "Apply" button, the forecast is saved, and the user is redirected to the "Dashboard" tab page where the user verifies the presence of the newly created forecast.

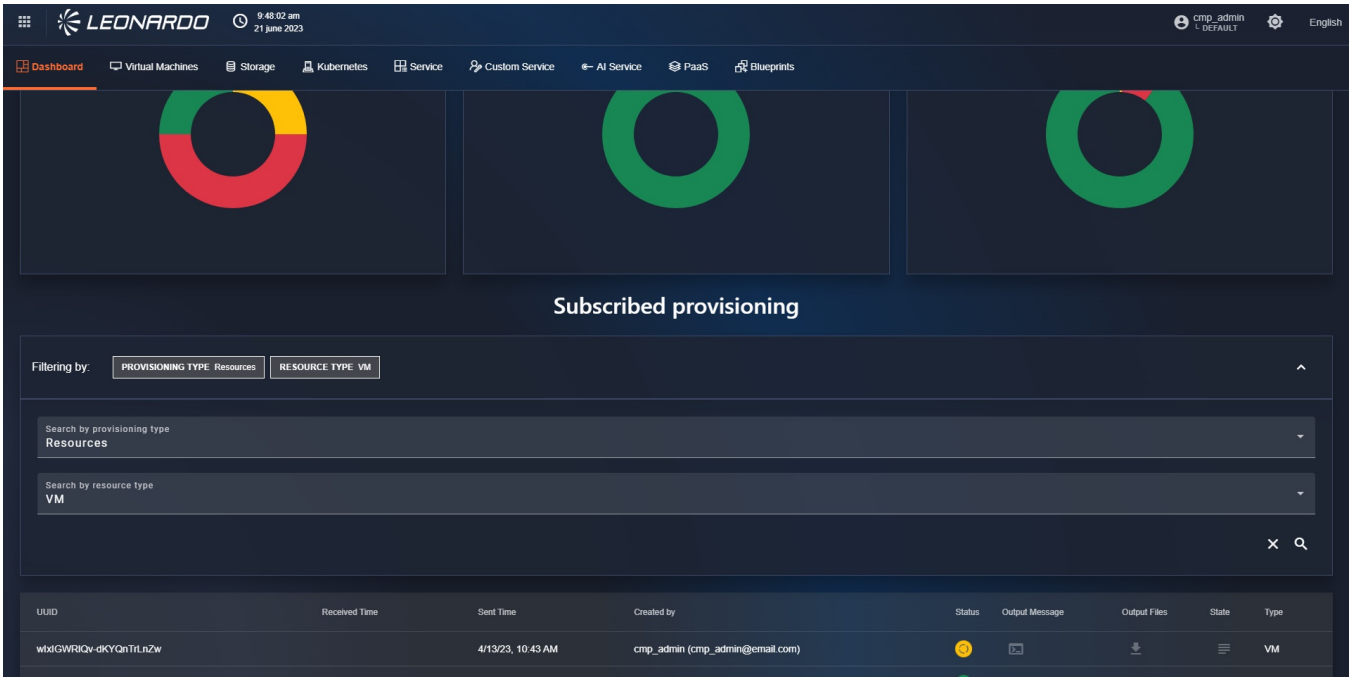


Figura 64 – List of provisionings performed

9.1.3 Provisioning of "Services"

To access the services page, click on the tab that depicts a shelf located in the top menu. After doing this, you will find yourself on the "Service" page.

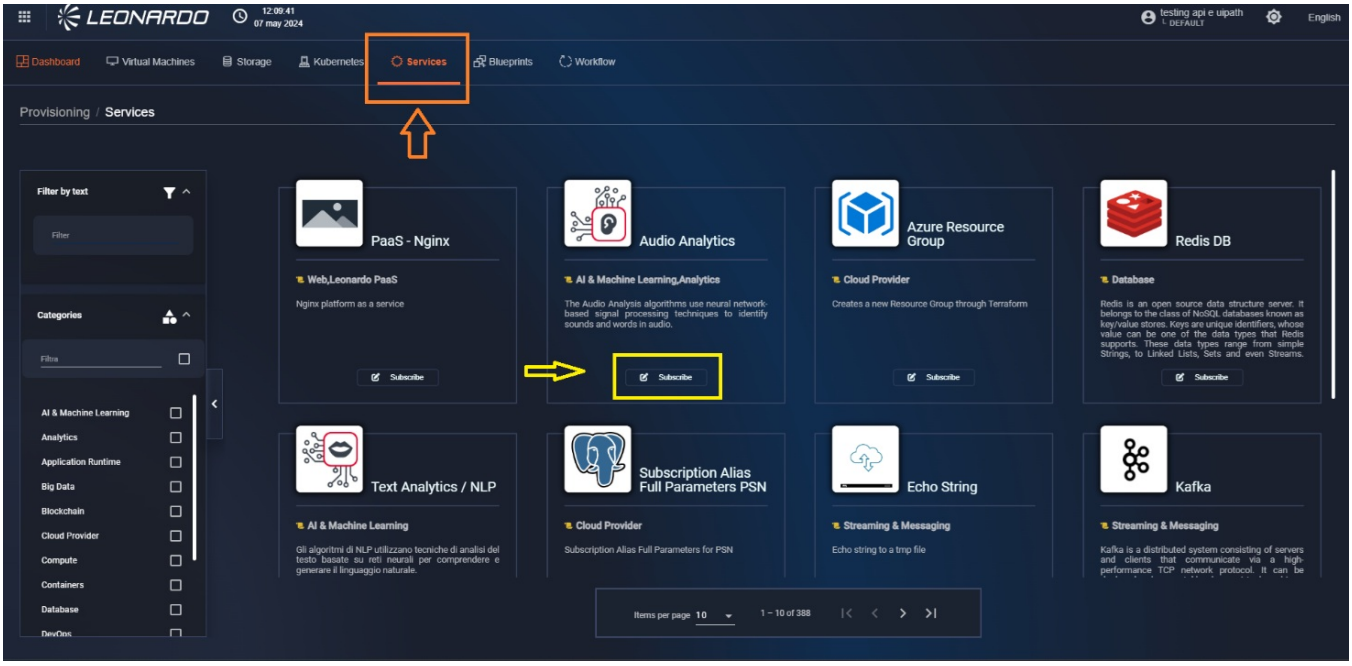


Figura 65 – List of cards

On the page, a list of components called "Card" is displayed. Each card refers to a specific type of service; in particular, the following information is displayed:

- Service name;
- Service icon;
- Type of script used for service provisioning;
- Service description;
- "Subscribe" button to proceed with service creation.

Depending on the type of service selected, the steps for provisioning change; these will be analyzed in detail below.

9.1.4 "Standard" Services

Click the "Subscribe" button corresponding to a "standard" service. The user will be redirected to step 1 of the service creation page, and all instantiable versions of the service by SCMP will be displayed. In particular, various blocks will be shown, each with a list of configurations:

- Name and version of the service that will be instantiated.
- Name and version of the operating system that will be installed on the machine.
- Belonging provider on which the service will be provisioned.

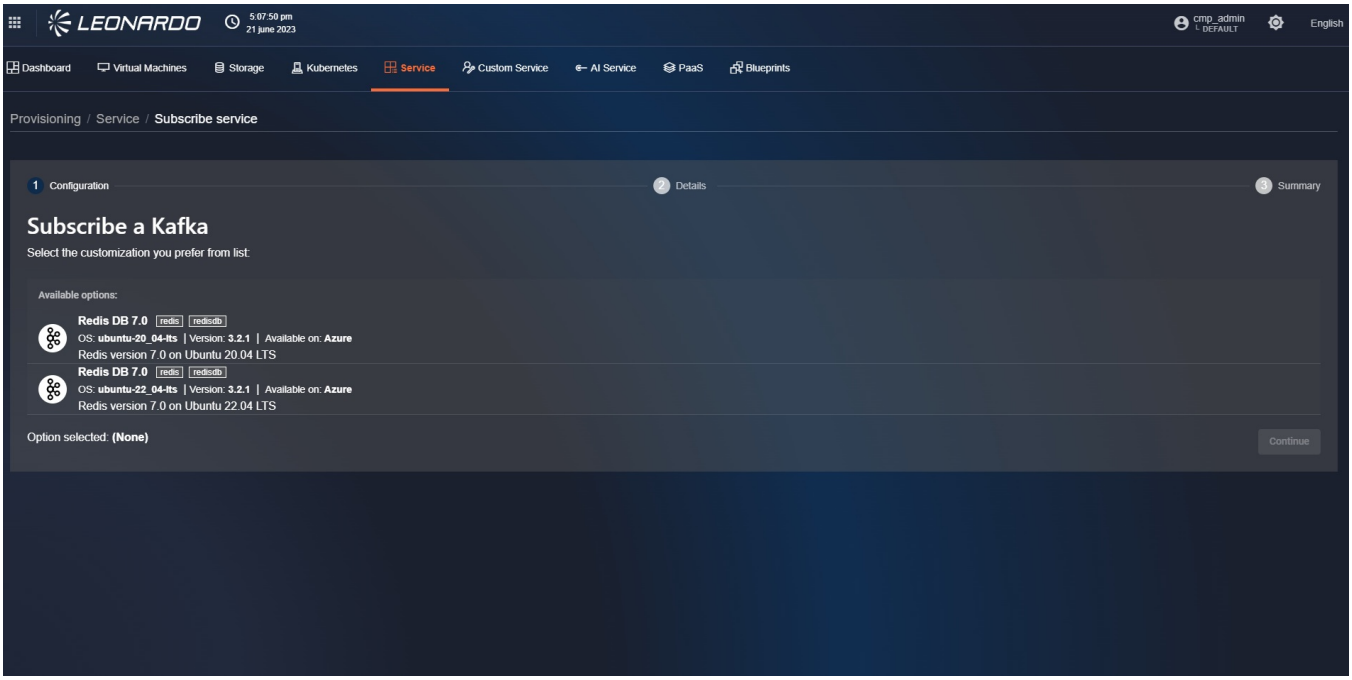


Figura 66 – Provisioning of a "standard" service

Select a software version and press the "Continue" button; the user is redirected to step 2 of service provisioning.

In step 2, it will be necessary to select a subsystem and fill out the form with the details of the chosen subsystem.

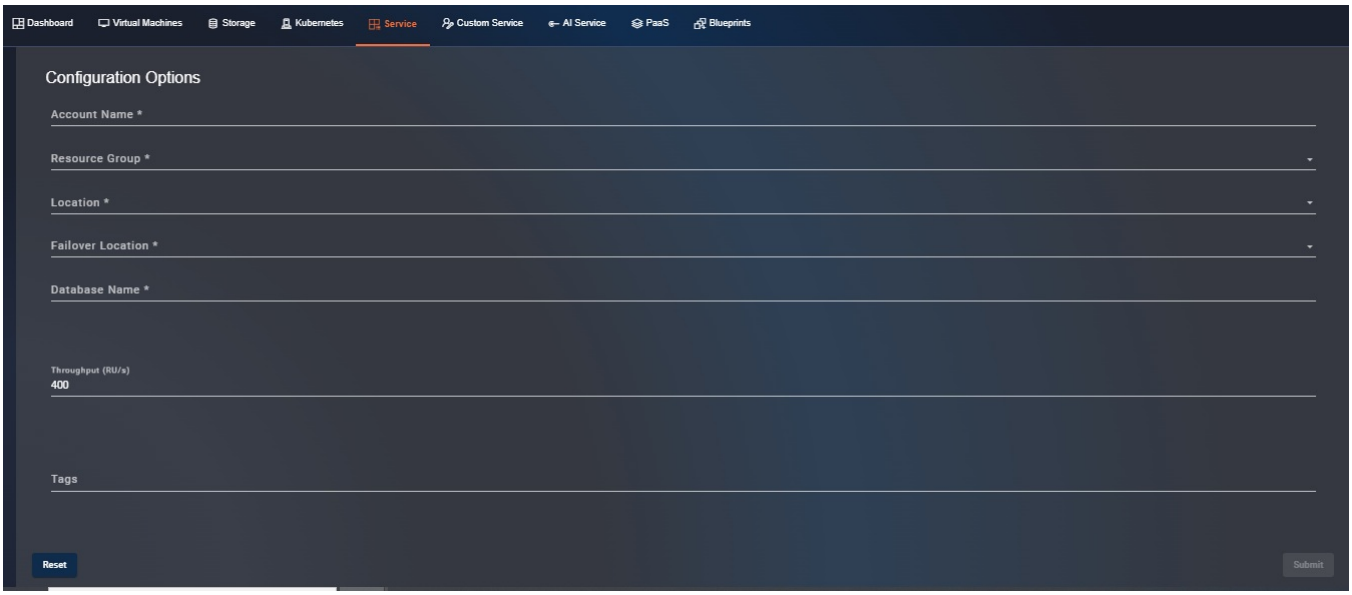


Figura 67 – Configuration of a

"standard" service

After completing all the form fields, click "Submit".

A request will be sent to the Terraform service, which will validate the activation configuration of the indicated flow and return the result.

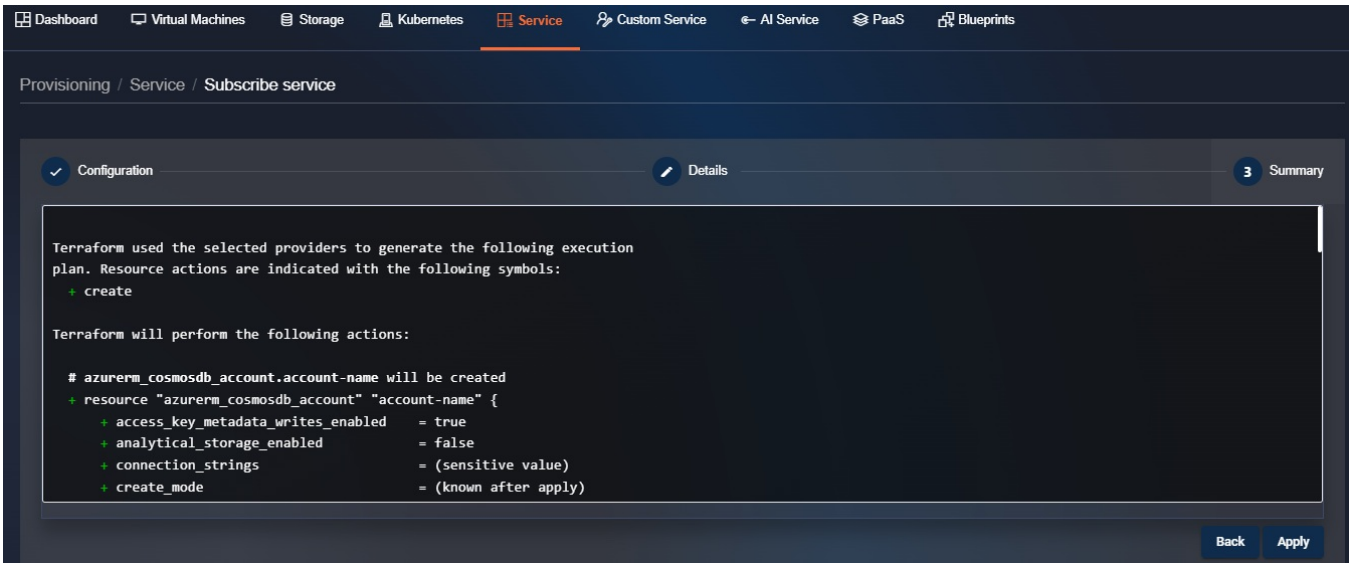


Figura 68 – Service configuration summary

Click "Apply" to validate the flow and activate the service subscription.

The dashboard page will open with the list of all subscribed services and their relative statuses. Specifically, the newly provisioned service will have a "Running" status in yellow, and subsequently, depending on the result, the status will also be updated to "Completed" in green or "Error" in red.

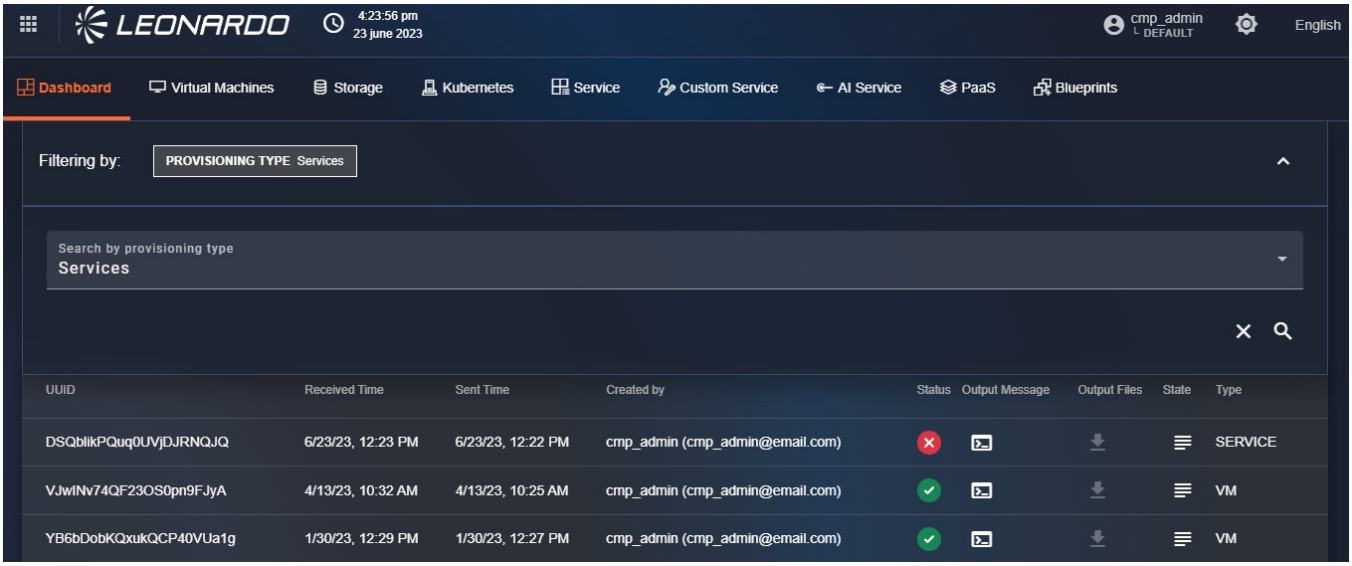


Figura 69 – Dashboard with the list of all subscribed services and their relative statuses

9.1.5 "Custom" Services

Click the "Subscribe" button corresponding to a "custom" service. The user will be redirected to step 1 of the service creation page where the subsystem can be selected, in which to perform the provisioning, from the dropdown in the center of the page.

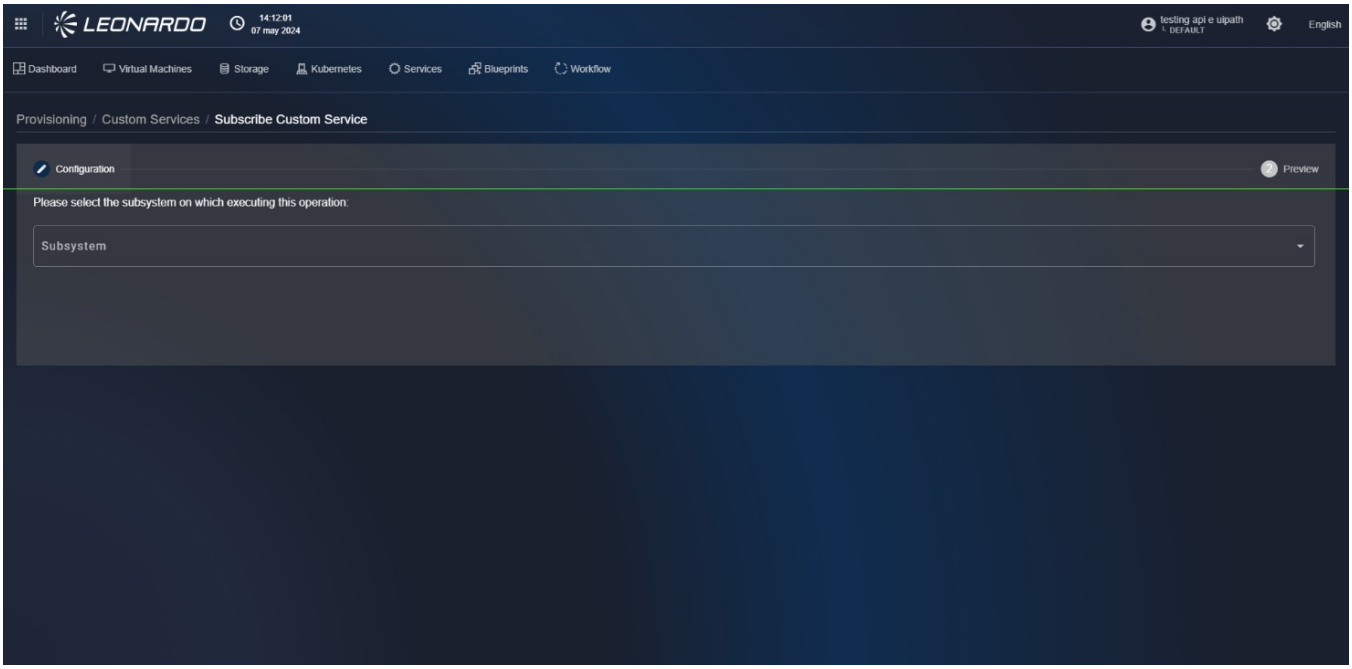


Figura 70 – Provisioning of a "Custom" service

By selecting the subsystem, the page updates to proceed to step 2 of service provisioning.

In this step 2, it will be necessary to fill out the form with the specific configuration parameters of the selected service.

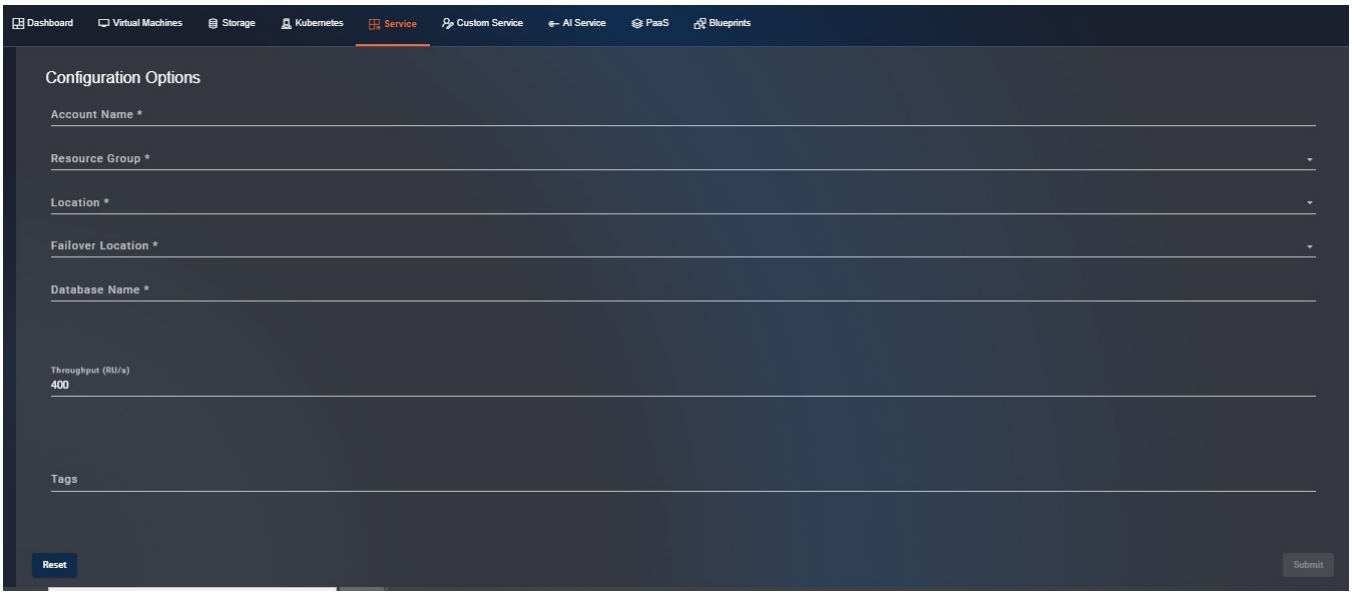


Figura 71 – Configuration of a "custom"

service

After completing all the form fields, click "Launch".

A request will be sent to the Terraform service, which will validate the activation configuration of the indicated flow and return the result.

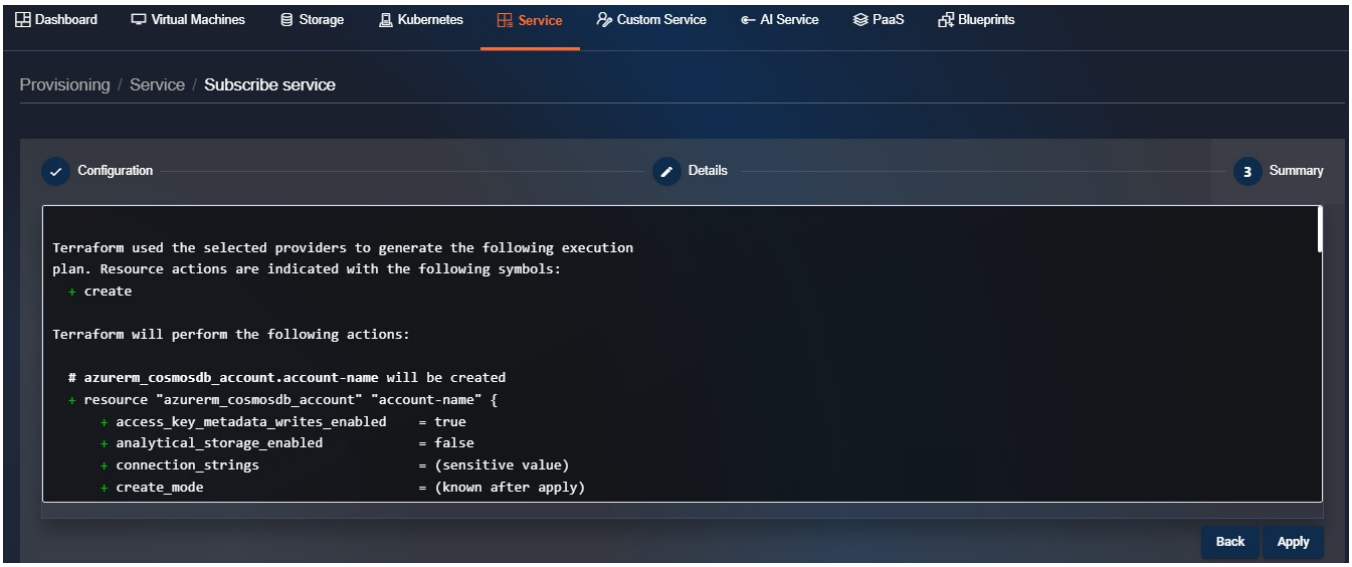


Figura 72 – Service configuration summary

Click "Apply" to validate the flow and start the automatic configuration operations.

The dashboard page will open with the list of all subscribed services and their relative statuses.

Specifically, the newly provisioned service will have a "Running" status in yellow, and subsequently, depending on the result, the status will also be updated to "Completed" in green or "Error" in red.

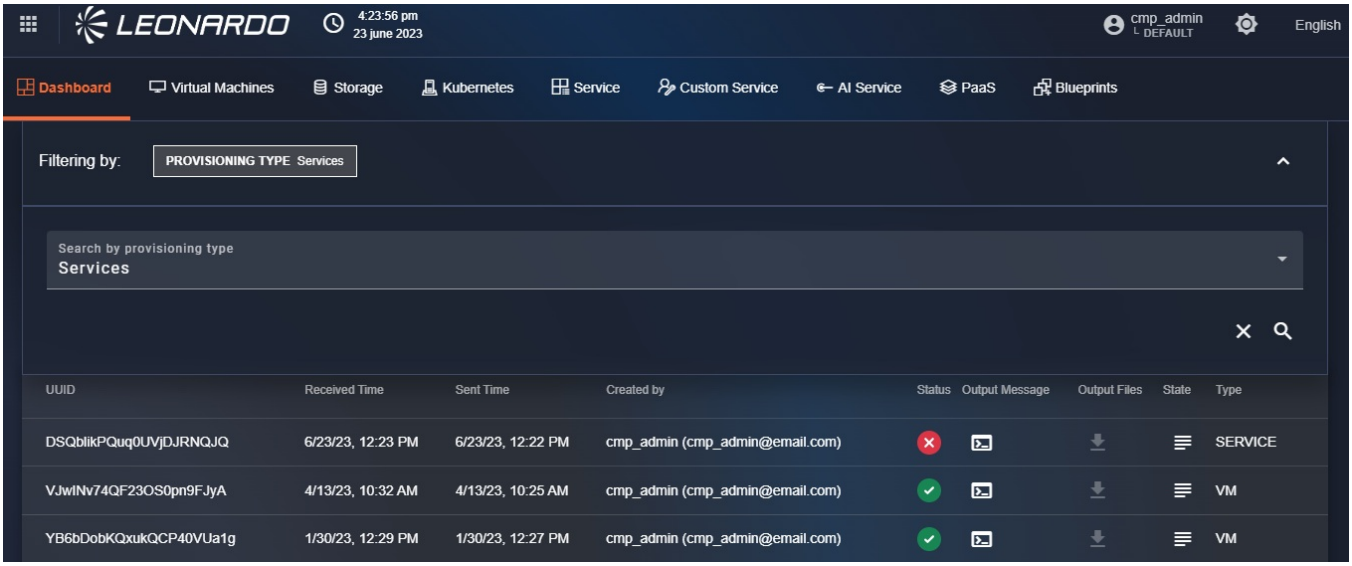


Figura 73 – Dashboard with the list of all subscribed services and their relative statuses

9.1.6 "PaaS" and "AI Services"

Click the "Subscribe" button corresponding to a "PaaS" service. The user will be redirected to step 1 of the service creation page where it will be necessary to fill out the form with the specific configuration parameters of the selected service.

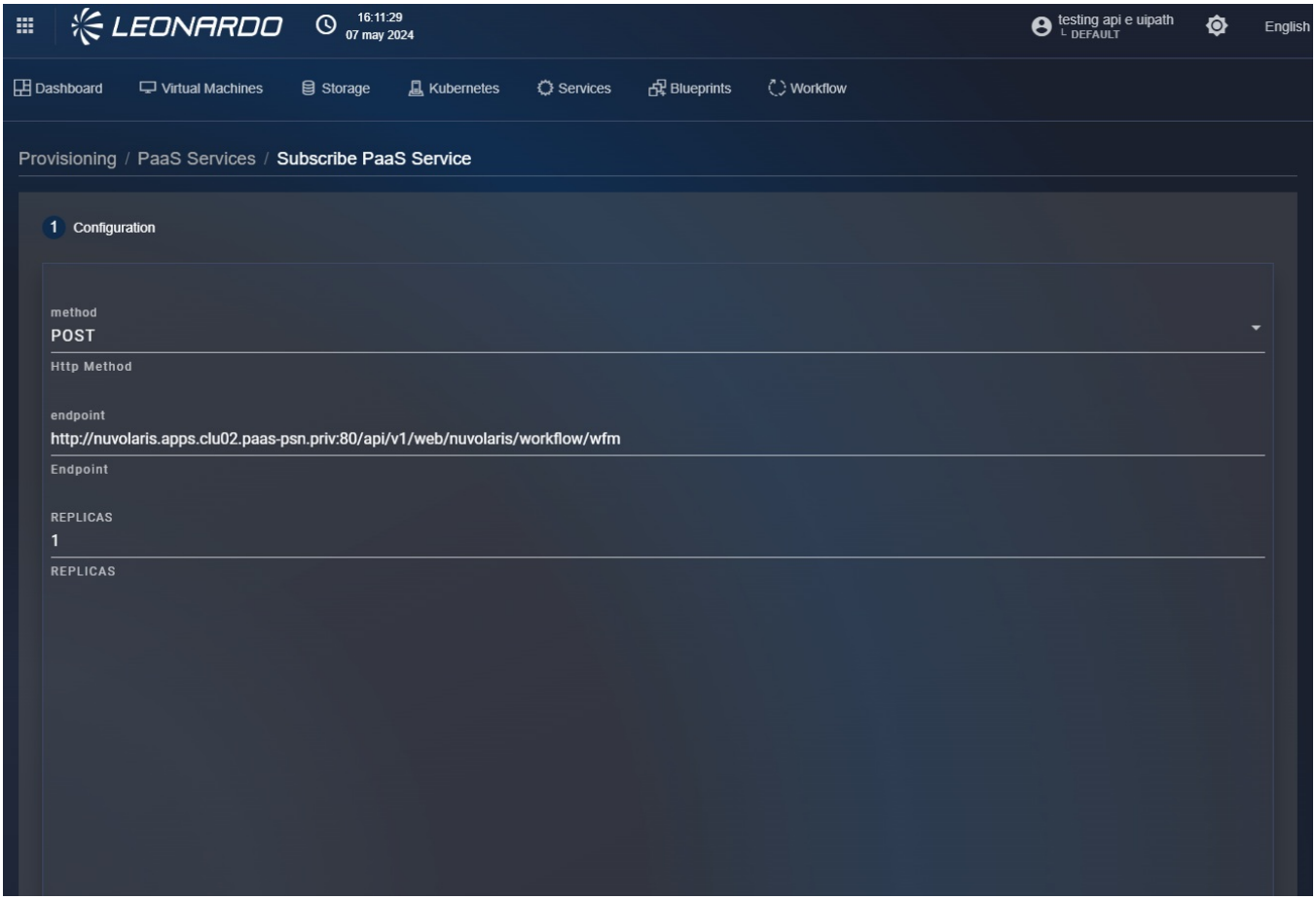


Figura 74 – Configuration of a "PaaS" service

After completing all the form fields, click "Launch".

The dashboard page will open with the list of all subscribed services and their relative statuses.

Specifically, the newly provisioned service will have a "Running" status in yellow, and subsequently, depending on the result, the status will also be updated to "Completed" in green or "Error" in red.

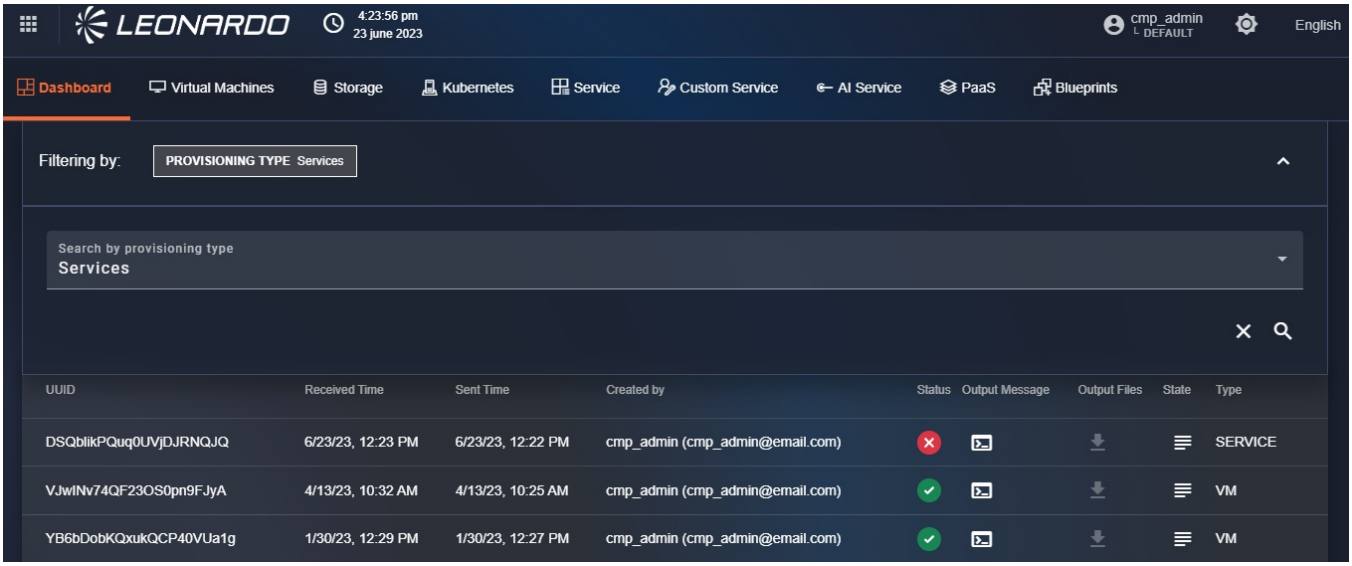


Figura 75 – Dashboard with the list of all subscribed services and their relative statuses

9.1.7 Modification of a performed provisioning

For a provisioning that has been carried out and has failed, it is possible to modify it.

Provisioning modification is only available for resource types.

To start modifying a provisioning, click on a failed forecast.

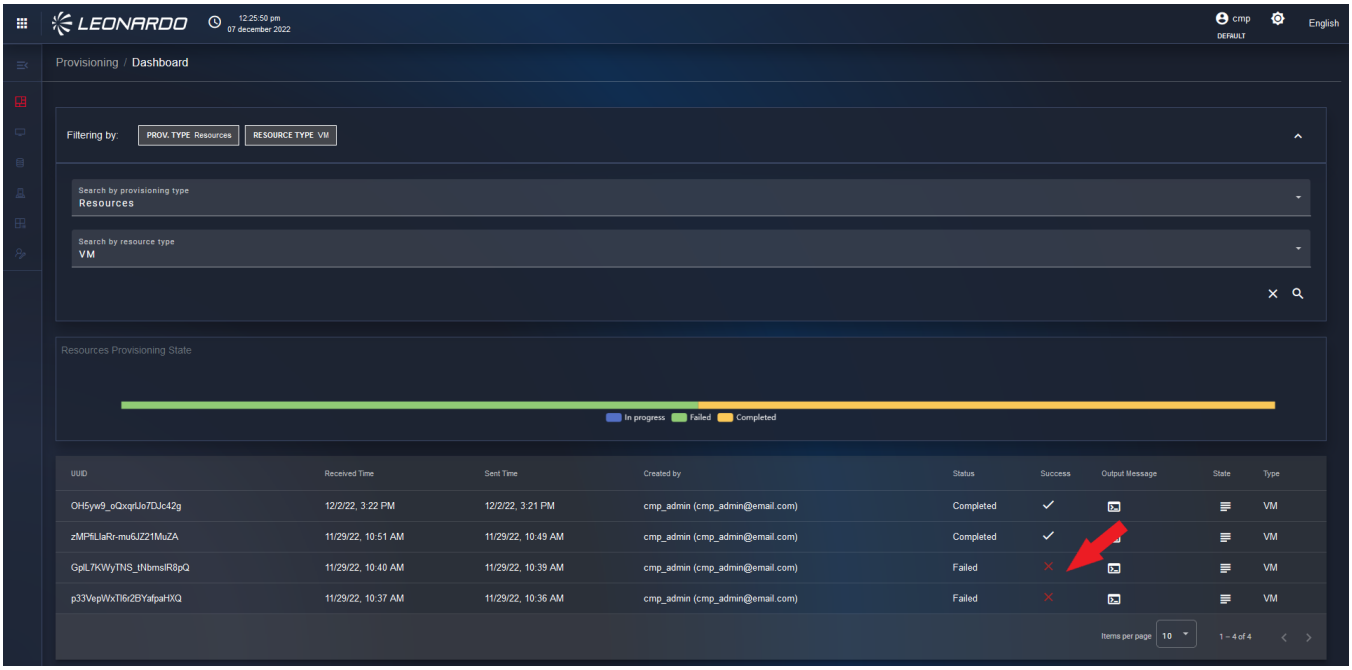


Figura 76 – Start modification of a Provisioning

After doing so, you will find yourself on the "Config" page of step 2 where you can modify the previously entered parameters.

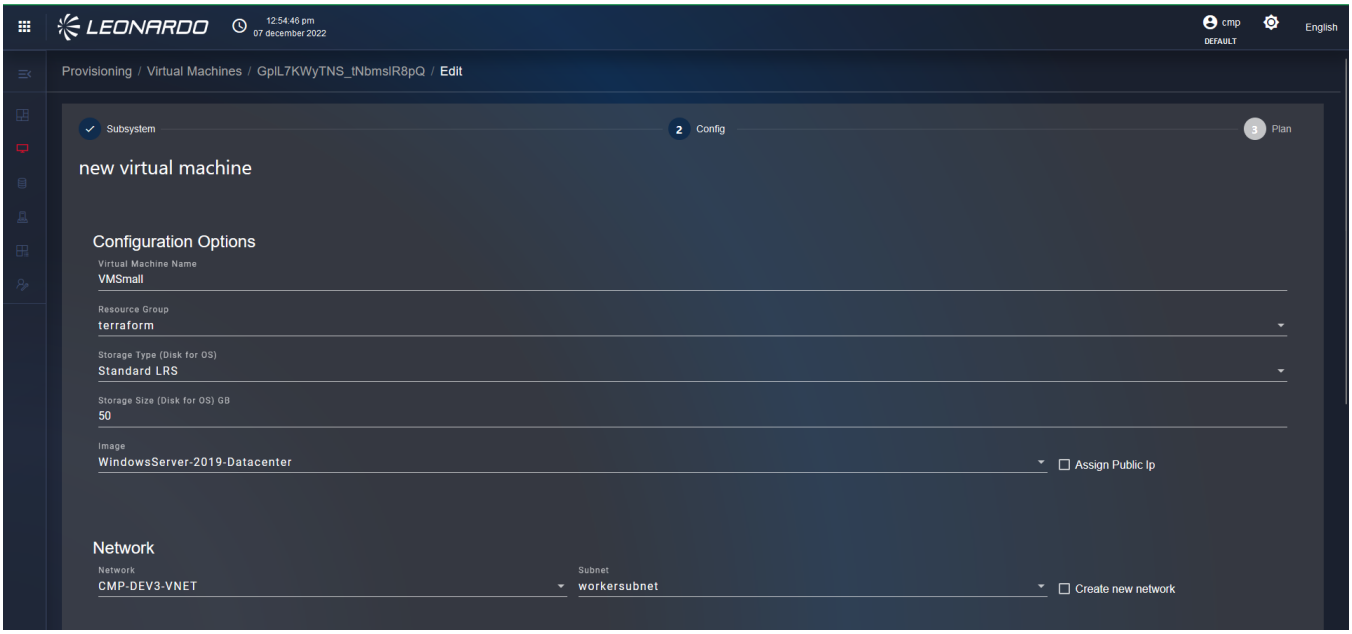


Figura 77 – Configuration parameters

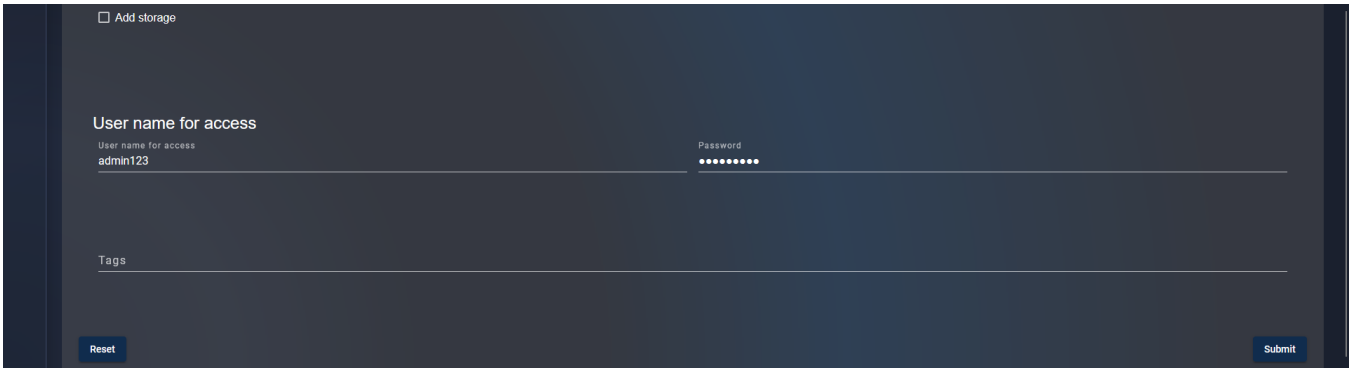


Figura 78 – Modification of parameters

After modifying the necessary parameters, at the bottom right, click the "Submit" button.

By doing so, you will find yourself on the "Plan" page of step 3, where the forecast is present, and below, the quote table.

At the bottom right, click the "Apply" button. After clicking the "Apply" button, you will find yourself on the "Dashboard" tab page.

Subsequently, from the "Dashboard" page, the user notes that the modification was successful.

It is also possible to modify a failed provisioning for other elements managed by SCMP.

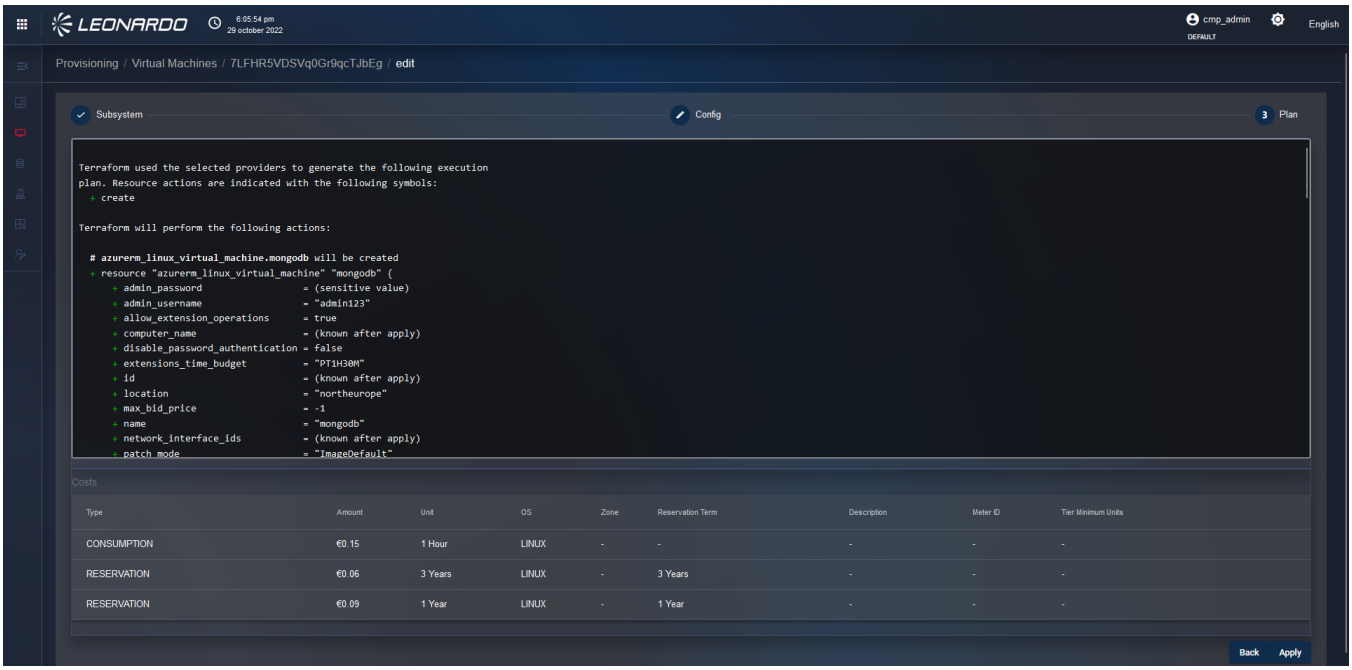


Figura 79 – Provisioning summary and

quote table

10 IT Service Management (ITSM)

The IT Service Management (ITSM) defines the process of the activities, responsibilities, and controls required to manage customer support requests in a structured, timely, and traceable manner.
It applies to all types of tickets submitted by customers, including:

- Incidents (service disruptions or malfunctions).
- Service Requests (standard operational requests).
- Access Requests.
- Information Requests.
- Change-related inquiries.
- Other support needs requiring tracking and resolution.

The objective is to ensure consistent quality of service, reduce resolution times, improve resource coordination, and maintain complete traceability of customer interactions
Each phase includes defined roles, expected outputs, and quality criteria.
Leonardo's methodology for delivering and supporting its services is inspired by ITIL®. The ITIL® framework has been used as a reference for delivering and improving services, particularly in the areas of Service Operation and Service Transition.

10.1 Process steps

This section lists the process sequences for customer support requests.

1) **Ticket Intake**
The customer sends a request via email to the support address listed here: Send an email

Upon receipt, the Service Desk (or designated support function) performs:

- Logging of the request into the ticketing system.
- Attribution of a unique ticket ID.
- Initial verification of provided information.

All tickets are timestamped and stored for auditability.

2) **Classification and Prioritization**
The Service Desk categorizes the ticket into one of the predefined classes (Incident, Request, Access, etc.).
Priority is determined using criteria such as:

- Impact (number of users/services affected).
- Urgency (time sensitivity of the issue).
- Service criticality (business relevance of the affected system).

This ensures coherent treatment of tickets and alignment with Service Level Agreements (SLAs).

3) **Assignment**
After classification, the ticket is routed to the appropriate resolver group (e.g., Infrastructure, Application Support, Network Operations, Security, Service Delivery).
Assignment criteria include:

- Required technical expertise.
- Workload distribution.
- Escalation rules.
- Operational hours and on-call availability.

The resolver group assumes ownership of the ticket until resolution.

4) **Investigation and Resolution**
The assigned team performs root-cause investigation, corrective actions, or fulfillment activities depending on the ticket type.
Typical activities include:

- System checks and diagnostics.
- Configuration adjustments.
- User guidance or remote assistance.
- Deployment of fixes or patches.
- Coordination with third-party vendors when applicable.

Progress is continuously updated in the ticketing system.

5) **Customer Communication**
The customer is informed throughout the lifecycle of the ticket, including:

- Acknowledgement of receipt

- Status updates (especially for high-priority issues)
- Request for additional information
- Notification upon resolution

Communication follows predefined templates and response-time commitments.

6) **Ticket Closure**
A ticket is closed only when:

- The solution has been delivered and validated.
- The customer has been informed.
- Documentation of actions taken is complete.
- Linked tickets (if any) have been updated.

Quality controls ensure closure accuracy and SLA compliance.

10.2 Escalation management

Escalations ensure that prolonged or high-impact issues receive timely attention.
They include:

- Functional escalation to more specialized teams.
- Hierarchical escalation to management when SLA breaches or major impacts are imminent.
- Vendor escalation for third-party system dependencies.
- Escalation paths and thresholds are predefined within the support framework.

10.3 Monitoring and quality assurance

Performance of the Ticket Management Process is monitored through KPIs such as:

- Ticket resolution time
- SLA compliance rate
- First Contact Resolution rate
- Backlog volume and aging
- Customer satisfaction feedback

Periodic reviews identify improvement opportunities and ensure adherence to service standards.

10.4 Roles and responsibilities

This section defines the roles, responsibilities, and operational boundaries for managing cloud services in accordance with a Shared Responsibility Model.
The goal is to establish a clear framework that enables the secure, compliant, and efficient adoption of cloud services within the organization.
The principles described here apply to all services offered and described in this documentation.

Cloud security is a joint commitment between Leonardo, as a cloud service provider, and the organization, as a customer.
Leonardo is responsible for cloud security, including physical infrastructure, network control layers, and platform services.
The organization is responsible for cloud security, including data protection, identity and access management, workload configuration, and governance.

The distribution of responsibilities varies depending on the service model. As the organization adopts higher-level services (from IaaS to PaaS), Leonardo assumes a greater share of operational responsibility, while the organization retains responsibility for data, identity, and access governance.

10.4.1 Organizational roles

To ensure effective management of shared responsibilities, the following internal roles are established:

A) Platform/Cloud team

Dedicated to the design, implementation, and management of the core cloud infrastructure.
- Implements shared technical controls, including network configurations, platform security baselines, and monitoring frameworks. - Ennsures that Cloud environments comply with the organization's policies and technical standards.

B) Workload/Application team

Owns the design, security, and operation of specific workloads hosted in the cloud.
- Manages application configurations, secure coding practices, updates, and lifecycle management. - Ensures appropriate data classification, protection, retention, and deletion practices.

C) Security and compliance team

Defines organizational security policies, standards, and regulatory controls.

- Conducts risk assessments and oversees compliance across cloud deployments.
- Implements identity and access management policies, encryption standards, and mandatory security controls.

D) Governance and risk management

Maintains the cloud governance framework, including the shared responsibility matrix.

- Ensures that cloud operations remain aligned with legal, regulatory, and organizational requirements.
- Coordinates reviews and audits to validate compliance and role execution.

E) Operations and incident response team

Provides monitoring and operational support for cloud environments and deployed workloads.

- Manages incident response procedures, including triage, remediation, and coordination with Microsoft where required.
- Ensures proper execution of change management policies.

10.4.2 Responsibility matrix

A responsibility matrix is maintained to explicitly document which responsibilities fall to Leonardo, which to the organization, and which are shared.

Responsibility Matrix				
	IaaS	**CaaS**	**PaaS**	**Hybrid**
Customer	▫ Information and Data ▫ Devices (Mobiles or PCs) ▫ Accounts and Identities ▫ Identity and directory infrastructure ▫ Applications ▫ Network controls ▫ Operating System	▫ Information and Data ▫ Devices (Mobiles or PCs) ▫ Accounts and Identities	▫ Information and Data ▫ Devices (Mobiles or PCs) ▫ Accounts and Identities	▫ Physical datacenter ▫ Information and Data ▫ Devices (Mobiles or PCs) ▫ Identity and directory infrastructure ▫ Applications ▫ Operating System
Both		▫ Identity and directory infrastructure ▫ Applications ▫ Network controls	▫ Identity and directory infrastructure ▫ Applications ▫ Network controls	▫ Accounts and Identities ▫ Physical hosts ▫ Physical network
Leonardo	▫ Physical hosts ▫ Physical network ▫ Physical datacenter	▫ Operating System ▫ Physical hosts ▫ Physical network ▫ Physical datacenter	▫ Operating System ▫ Physical hosts ▫ Physical network ▫ Physical datacenter	▫ Network controls

Figura 80 – Division of responsibilities

The matrix includes, but is not limited to, the following domains:

- Data protection and classification
- Identity and access management
- Security monitoring and threat detection
- Network and host security
- Application configuration and secure development
- Backup, restore, and recovery
- Compliance, auditing, and reporting

This matrix is reviewed regularly and updated whenever service models, technologies, or organizational structures change.

10.4.3 Operational processes

The organization adopts a shared management operating model. The Platform Team provides standardized and secure environments and security barriers; the Workload Teams manage their solutions within these constraints. The Security and Governance Teams define mandatory controls and oversee compliance.

Identity governance remains the organization's responsibility. The principles of least privilege, role-based access control (RBAC), and secure authentication must be implemented. Microsoft provides the identity platform, while the organization manages users, groups, and access permissions.

The Workload Teams are responsible for ensuring the correct data classification and implementing the necessary protections, such as encryption, retention controls, and deletion policies.

The Platform Team provides the technical capabilities for encryption, secure storage, and backup.

Monitoring activities are shared:

- Leonardo monitors the security of the underlying cloud platform.
- The organization monitors workload behavior, user activity, configuration changes, and potential threats using security tools and logs.

Incident responsibilities are divided by domain:

- Cloud infrastructure-related incidents may involve Leonardo.
- Incidents involving data, identities, workloads, or configurations fall within the responsibility of internal teams.
  A coordinated response plan ensures that escalation paths, communication channels, and reporting requirements are clearly defined.

All changes to cloud resources must comply with the organization's change control procedures. Platform-level changes require coordination with the platform team; workload-level changes must be approved by the application teams, while remaining aligned with established Security and Governance policies.

This framework is reviewed on a periodic basis to ensure continued relevance.
Updates may be required when:

- new cloud services are introduced,
- organizational roles evolve,
- regulatory obligations change, or lessons learned from audits and incidents highlight areas for improvement.

Continuous improvement is essential to maintaining a secure and well-governed cloud environment.

11 Service Level Agreement (SLA)

This section defines the terms, metrics, and service commitments applicable to the services offered and described.

11.1 Availability calculation

The Uptime Annual Percentage of the services is determined as follows:

$$Annual\ Uptime\ \% = \frac{(\text{Maximum Available Minutes-Downtime})}{\text{Maximum Available Minutes}}\ x\ 100$$

Figura 81 – Annual Uptime Percentage

The Uptime Percentage is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes, where:

- *"Maximum Available Minutes"* indicates the total number of minutes per year during which the service is active, excluding any communicated maintenance windows.
- *"Downtime"* indicates the total accumulated minutes that fall within the Maximum Available Minutes and are not subject to service availability.

11.2 Service credits refunds

The Customer is entitled to the following credits refunds in the event of failure to meet the following availability levels:

Uptime Percentage	Service Credit
< 99.90%	5%
< 99%	10%
< 90%	15%

12 Test Account Requests

This section defines the process for provisioning test accounts requested by customers. The process ensures that customer requests for test accounts are handled in a controlled, timely, and secure manner. It includes request intake, validation, approval, provisioning, and delivery.

12.1 Request submission process

Below you can view the sequence of the process for requesting a test account by an authorized user.

1) The customer sends a request via email to the support address listed here: Send an email

The request must include:

- Purpose of the test account
- Number of accounts required
- Specific access or roles needed
- Contact details of the requester

2) The request is logged in the ticketing system upon receipt.

3) The Service Desk reviews the request to ensure completeness and technical feasibility. If additional information is required, the customer is contacted. The 10-day SLA starts once the request is validated as complete.

4) The Technical Team creates the test account(s) and applies:

- Minimum required permissions
- Applicable security policies
- Expiration settings (if required)

A functionality check is performed to confirm proper access.

5) Within 10 business days, the customer receives an email including:

- Credentials or activation instructions
- Overview of assigned permissions
- Account validity period
- Contact information for support

The ticket is now then closed.

12.2 Limitations

The following are some limitations regarding test account requests:

- Creation of a maximum of 4 small-scale VMs.
- Creation of a maximum of 1 K8S cluster.
- PaaS services can be added on request to the K8S cluster.

Not all PaaS services can be requested in the test environment.

13 Certifications and Compliance

This section lists the certifications and security compliances of the services described.

13.1 ISO certifications

Below are the available ISO certifications:

- ISO 9001 certification
- ISO 27001 certification
- ISO 27017 and 27018 certifications
- ISO 22301 certification - Business Continuity
- ISO/IEC 20000 certification - Service Management

13.2 Compliance

Below are the compliances with European regulations:

- General Data Protection Regulation (GDPR)-compliance privacy policy
- Network and Information Systems Directive 2 (NIS2)-compliance obligations

14 Cyber Security Services

This section lists the Cyber Security specifications and services provided by Leonardo Security Operation Centre (SOC).

14.1 Security services for detection

14.1.1 Real time Security Monitoring (RTSM)

Real time security incident management services provided by Leonardo Security Operation Centre (SOC) assure real time notifications about security alarms, behaviour anomalies and potential threats, leveraging best of breed detection platforms capabilities and Leonardo SOC analysts' skills and knowledge base.

Services' Deliverable

- Security alarms real time notification.
- Periodical reports for misconfigurations and low severity security evidences.
- Tuning process support.
- First level analysis and support in security incidents.

Services Included

- *Real Time Security Monitoring (RTSM)* → delivers continuous monitoring of customer security devices/systems logs in order to quickly identify potentially harmful resources or events.
- *Managed Endpoint Detection & Response (MDR)* → to provide customers with fast and effective protection for their endpoints, leveraging Endpoint Detection and Response cloud-based technologies.

Benefits

- Increases cyber situational awareness and faster identification of compromise whenit occurs.
- Reduce the impact of security incidents through quicker more informed response.
- Continuous monitoring of endpoints' events and activities through advanced analysis.

14.1.2 Threat Intelligence

The Threat Intelligence Services monitor and analyse large amounts of data, both open source and on the deep and dark web, to identify ongoing cyber-attacks or those being planned.
The service also identifies cyber threat actors' activities and information illegally stolen and published on the web.
The solution also provides a comprehensive overview on brand or event sentiment, and guidance on the prevention of cyber frauds.

Services' Deliverable

- Periodical or event-based threat intelligence reports.
- Tailored Investigation reports on customer request.

Services Included

- *Data breach* → detects any data loss relating to a specific target of information through real-time monitoring of the network, including scanning of the deep and dark Web.
- *Black market monitoring* → analyses large quantities of information from open sources, deep and dark Web, in real time, to promptly identify new black markets and illegal activities on specific issues of interest.
- *Pre-planned attack* → allows you to identify and predict possible new cyber-attacks more effectively, through real-time analysis of large quantities of information from open sources and the deep and darknet.
- *Identity fraud detection* → detects unauthorised use of a person's digital dentity to carry out illegal activities and/or defamatory actions without the knowledge of, and to the detriment of the individual.
- *Anti-phishing* → manages the detection of ongoing phishing attacks against the customer, the real-time identification of ongoing fra udtowards their brand and the protection of online reputation.

Benefits

- Increases cyber situational prevention of company-owned data loss.
- Sentiment analysis.
- Black market related illegal activities identification.
- Prevention against new planned cyber-attacks.
- Protection of VIPs' and Company online reputation.
- Customer digital identity protection / identity theft identification.
- Real time detection of cyber frauds and phishing attacks identification.

14.2 Security services for respoding

14.2.1 Computer Security Incident Response Team Services

The Computer Security Incident Response Team Services (CSIRT) identify and analyse the most advanced cyber threats capable of bypassing traditional automatic defensive measures, through the identification of root cause, attacker behaviour, relevant artefacts, and compromised assets within the monitored infrastructures.
The CSIRT services deeply analyse and react to security incidents, minimising the operational and economic impacts of the security incident as effectively as possible, through the definition of the most rapid and effective incident response strategy.

Services' Deliverable

- Artifacts analysis and reports.
- Containment and mitigation activities.
- Incident response reports.
- Remediation and restoration technical support.
- Security evidences and artifacts.
- Compromise assessment report

Services Included

- *Incident Response* → combines specialist capability in incident management and investigation to deliver comprehensive advice and technical analysis in response to any cyber security attack or breach.
- *Malware Analysis* → acquires and classifies suspected malicious files (samples), provides hash control, comparison with known malware, behaviour analysis in order to identify any indicators of compromise and any containment actions to put in place.
- *Threat Hunting* → proactively identifies, isolates and neutralises the most advanced cyber threats that are capable of bypassing traditional automatic defensive measures before they can cause real damage to the organization.
- *Compromise Assessment* → provides the customer with a complete view of the current situation in terms of potential threats or ongoing malicious activities leveraging the capabilities of an Endpoint Detection & Response (EDR) solution.

Benefits

- Identification of Indicators of Compromise and any containment actions to put in place.
- Capability to isolate systems while preserving evidences.
- Specialised support to carry out the remediation and restoration of systems.
- Indications regarding the actions needed to mitigate future incidents.

14.3 Penetration Testing Offering Policy for Managed Services

This policy defines guidelines, requirements, responsibilities, and constraints for performing penetration testing on environments managed by the provider under the following service models:

- IaaS – Infrastructure as a Service
- PaaS – Platform as a Service
- CaaS – Container as a Service
- Hybrid – on-premise + cloud environments

The objective is to ensure a controlled, safe, and authorized approach to offensive security activities without compromising service availability or violating cloud governance rules.

14.3.1 General Principles

1. Penetration testing activities must be **pre-authorized** by the provider and conducted in compliance with applicable laws and contractual conditions.
2. Customers must restrict testing to **resources they fully own or administer**.
3. Activities must not compromise the stability of the provider's core services nor affect other customers.
4. The policy follows the guiding principle: "Test only what you own and only in ways that don't impact other tenants"

14.3.2 Penetration Testing Scope

14.3.2.1 IaaS Services

Allowed: - Vulnerability assessments and penetration testing on:
- Virtual machines, OS configurations, hosted applications
- Virtual network configurations (NSG, firewall, routing)
- Storage, databases, and customer-installed components
- Authentication, authorization, and remote access testing on VMs

Not Allowed / Restricted:

- Real or simulated DoS/DDoS without explicit agreement
- Stress testing shared IaaS platforms
- Targeting physical infrastructure, hypervisors, or fabric-level services

14.3.2.2 PaaS Services

Allowed:

- Testing applications and data deployed by the customer
- Security configuration and identity-related tests
- API, endpoint, permission, and customer-managed storage validation

Not Allowed / Restricted:

- Attacks on the underlying provider-managed PaaS infrastructure
- Attempts to bypass tenant isolation
- Tests that may degrade service SLAs

14.3.2.3 CaaS (Container / Kubernetes) Services

Allowed:

- Analysis of customer-owned container images
- Testing workloads, microservices, ingress, API, and application-level RBAC
- Validation of customer-managed cluster networking
- Testing secrets, config maps, and identity integrations

Not Allowed / Restricted:

- Container escape attempts targeting physical nodes
- Attacks on the control plane if provider-managed
- Testing shared provider-managed components (API server, etc.)

14.3.2.4 Hybrid Services

Allowed:

- Testing customer-owned on-prem components connected to the cloud
- End-to-end testing of hybrid integrations (VPN, DirectConnect, ExpressRoute)
- Identity, SSO, and cross-domain security validation

Not Allowed / Restricted:

- Saturation or intentional overload of hybrid links
- Attacks on cloud infrastructure or provider-managed appliances

14.3.3 Types of Tests Allowed

Allowed (with authorization):

- Black-box, grey-box, and white-box testing
- Authenticated / unauthenticated vulnerability scanning
- Application security testing (OWASP Top 10)
- Lateral movement testing within customer-owned assets
- Privilege escalation and configuration testing
- Phishing/social engineering simulations (if contracted)

Prohibited:

- Real DoS/DDoS
- High-volume port scans
- Attacks on physical infrastructure, hypervisors, or shared services
- Deployment of active malware in production
- Attempts to evade billing or resource management controls

14.3.4 Request and Approval Process

Customers must submit a request at least **10 business days** in advance, including: 1. Test scope (assets + service model)
2. Techniques and methodologies
3. Testing window
4. Customer security team contacts
5. Business-related risks

The provider confirms or denies within 5 business days.

14.3.5 Responsibilities

14.3.5.1 Customer

- Ensure tested assets are owned/administered
- Restrict testing to the authorized scope
- Ensure testing tools do not degrade services
- Provide test reports if requested

14.3.5.2 Leonardo

- Validate and authorize the test scope
- Monitor infrastructure for unexpected impact
- Guarantee tenant isolation
- Suspend tests if critical risks arise
- Provide SOC/NOC contact during the test window

14.3.6 Test Suspension Terms

The provider may suspend testing if: - Unexpected impacts occur
- The customer exceeds authorized scope
- Risks emerge for other tenants or infrastructure

14.3.7 Reporting

Customers must provide, upon request: - Executive Summary
- List of vulnerabilities
- Methods and tools used
- Proofs of Concept (PoCs)
- Remediation recommendations

14.4 Red Team Exercises

Leonardo provides Red Team exercises on a dedicated infrastructure for each customer.
These activities are managed by Leonardo's internal SOC.

For any further information, please contact us by opening a support request here: Send an email

14.5 Vulnerability assessments

Leonardo provides Vulnerability assessments on a dedicated infrastructure for each customer, where the methods and type of execution will be defined. These activities are managed by Leonardo's internal SOC.

For any further information, please contact us by opening a support request here: Send an email

14.6 Vulnerability disclosure program and policy

Regarding disclosure of vulnerabilities discovered by Leonardo, its behavior depends on the context in which they occur.
Specifically:

- If the vulnerabilities found affect its own infrastructure used to provide services, Leonardo will promptly inform the designated Italian Computer Security Incident Response Team (CSIRT).
- If the vulnerabilities found affect customer workloads, Leonardo will provide vulnerability assessments on a dedicated infrastructure for each customer, where the methods and type of execution will be defined.
  For this point, please see the section above regarding the Vulnerability Assessments process.

15 Frequently Asked Questions (FAQ)

15.1 1. Infrastructure as a Service (IaaS)

1.1 What does Leonardo's IaaS offer?

Leonardo provides compute, storage, and network resources suitable for cloud and hybrid environments.
You can consult the list of services in the dedicated section Infrastructure as a Service (IaaS).

1.2 What is "Confidential Private IaaS"?

A highly secure environment that uses confidential computing to isolate and protect virtual machines.
You can consult the details here Confidental Private IaaS.

1.3 Does the IaaS support hybrid scenarios?

Yes, resources can be distributed across cloud and Edge Location nodes.
You can consult the details here Edge Location - Pool Small (Confidential).

15.2 2. Container as a Service (CaaS)

2.1 Which orchestration platform is used?

A fully managed Kubernetes environment.
You can consult the details here Kubernetes Confidential Computing.

2.2 Is confidential computing supported for containers?

Yes, workloads can run in isolated and secure environments.

15.3 3. Platform as a Service (PaaS)

3.1 Which database services are available?

PostgreSQL, MariaDB, MS SQL Server, MongoDB, GraphDB, Redis in-memory.
You can consult the complete list here Platform as a Service (PaaS).

3.2 What does the Middleware PaaS include?

API management, CMS, workflow orchestration, and application integration.
You can consult the complete list here Platform as a Service (PaaS).

3.3 Are ETL or Data Lake services available?

Yes, Data Lakes, ETL Pipelines, and governance tools are included.
You can consult the details here Platform as a Service (PaaS).

15.4 4. Artificial Intelligence & Machine Learning

4.1 Which AI services are available?

OCR, NLP, translation, speech-to-text, vector search, LLMs, workflow AI.
You can consult the complete list here Platform as a Service (PaaS).

4.2 Can I integrate custom models?

Yes, depending on the specific service selected.

4.3 Are AI document-processing services available?

Yes — including OCR, text extraction, and semantic analysis.
You can consult the complete list here Platform as a Service (PaaS).

15.5 5. Security Services

5.1 Which security services are offered?

You can consult the complete list here Platform as a Service (PaaS).

5.2 Is IAM included?

Yes, Identity and Access Management as a Service is included.
You can consult the details here Identity & Access Management (IAM) Service.

5.3 Can security testing be automated?

Yes, with automated vulnerability scans and assessments.

15.6 6. Networking

6.1 Which network features are included?

IP, DNS, load balancers, CDN, advanced connectivity are some network services available.
You can consult the complete list here Platform as a Service (PaaS).

6.2 Is centralized traffic management supported?

Yes, via load balancing and DNS services.
You can consult the complete list here Platform as a Service (PaaS).

6.3 Are hybrid and edge scenarios supported?

Yes, with integration across cloud, edge, and data centers.

15.7 7. Storage & Data Protection

7.1 What storage options are available?
Block storage, high-performance storage, archiving are some storage services available.
You can consult the complete list here Platform as a Service (PaaS).

7.2 Is a native backup service available?
Yes, Data Protection provides managed backups.

7.3 Can backup integrate with IaaS and PaaS?
Yes, it is compatible with all service families.

15.8 8. Big Data

8.1 Which Big Data services are provided?
Data Lakes, ETL Pipelines, Data Governance, catalogs, analytics are some Big Data services available.
You can consult the complete list here Platform as a Service (PaaS).

8.2 Can external data be imported?
Yes, via ETL pipelines supporting multiple sources.

8.3 Is metadata management included?
Yes, through a built-in data catalog.

15.9 9. DevSecOps

9.1 What does the DevSecOps offering include?
CI/CD, automated testing, code analysis, configuration management are some DevSecOps services available.
You can consult the complete list here Platform as a Service (PaaS).

9.2 Can configurations be centrally managed?
Yes, through Configuration Management services.

9.3 Are code quality and security scans available?
Yes, tools for scanning and verifying code are provided.

15.10 10. Collaboration Services

10.1 Which collaboration tools are included?
Cloud-based instant messaging and enterprise communication features.
You can consult the details here Instant Messaging.

15.11 11. Hybrid & Edge Services

11.1 What are Edge Services?

Edge nodes (“Edge Location – Pool Small”) offering localized cloud capabilities.
You can consult the details here Instant Messaging.

11.2 When are edge services useful?

Low-latency needs, distributed facilities, industrial sites, defense use cases. You can consult the details here Edge Location - Pool Small (Confidential)

15.12 12. Service Management (SLA, Ticketing, Monitoring)

12.1 Where can I find the SLAs?

You can find it on the Service Level Agreement (SLA) section of the documentation.

12.2 How do I activate a new service?

By following instructions in the Service Provisioning section.

12.3 Is a test account available?

Yes — under Test Account Management with access here Test Account Management.

12.4 How can I open a support ticket?

Via the Ticket Management interface. You can consult the process here Service Management.

15.13 13. Data Center Description

13.1 Where are Leonardo’s Data Centers located?

In secure, redundant, protected facilities. You can consult all details and specifications here Data Center Description.

13.2 Which security standards are applied?

Physical and logical protections, monitoring, redundancy, fire suppression, controlled access. You can consult all security details here Data Center Description.

13.3 What availability level is ensured?

High availability through infrastructure redundancy. You can consult all details here Data Center Description.

13.4 Are multiple geographic areas supported?

Yes, including Data Centers and Edge nodes. You can consult all Data Center architecture and interconnectionhere Data Center Description.

13.5 What networking capabilities are included?
Advanced routing, segmentation, load balancing, perimeter security. You can consult all details here Data Center Description.

15.14 14. Provisioning

14.1 How do I request service activation?
By following steps in the Service Provisioning section. By following instructions in the Service Provisioning section.

14.2 Is manual approval required?
Yes, for selected services.

14.3 How long does provisioning take?
From minutes/hours (IaaS/CaaS) to longer deployments (AI, Big Data). By following instructions in the Service Provisioning section.

14.4 Can provisioning be automated?
Yes, via APIs, pipelines, and scripts. By following instructions in the Service Provisioning section.

14.5 Where can I check request status?
In the Service Management dashboard.

15.15 15. Certifications

15.1. What certifications does Leonardo have for its services? You can consult all the certifications in the dedicated section Certifications

15.2. What does the ISO/IEC 20000 certification mean for customers? This certification ensures that Leonardo's IT Service Management processes follow strict international quality standards—providing higher reliability, structured support processes, and strong governance over delivered cloud services.

15.3. Does Leonardo hold certifications related to information security? Yes. Leonardo invests heavily in information security and aligns its practices with global standards. The Cyber & Security division continuously monitors systems and ensures compliance with internationally recognized frameworks.

15.4. Does Leonardo have its own CERT? Yes. Leonardo operates the **LDO-CERT** (Leonardo Cyber Defence), which functions as both a Security Operation Center (SOC) and a Cyber Emergency Readiness Team, offering threat monitoring, detection, and incident response services.

15.5. How does Leonardo ensure quality and regulatory compliance in Cyber & Security activities? Leonardo implements strict governance policies, risk assessments, continuous audits, and monitoring of critical security processes. Certifications and the presence of an internal CERT reinforce Leonardo's ability to deliver proactive cybersecurity.

15.6 Is Leonardo compliant with national or international regulatory requirements? Yes. Through Leonardo's certifications and robust security frameworks, the platform is aligned with key international standards and is designed for regulated sectors such as defense, public administration, and critical infrastructures.

15.16 16. Cyber Security Services

16.1 What security measures does Leonardo offer? - Data encryption with secure key management (KMS).
- Continuous monitoring and incident response via Leonardo's LDO-CERT SOC.
- Built-in resilience policies, including disaster recovery and business continuity.
- Software-defined architectures that improve isolation, automation, and control.

16.2 Does Leonardo supports a Zero Trust security model? Yes. Leonardo is strengthening its cyber portfolio toward a **Zero Trust** architecture, where access is continuously validated, regardless of the user's position inside or outside the network.

16.3. How does Leonardo manage cybersecurity emergencies? Leonardo's **LDO-CERT** performs: - Incident classification and response
- Digital forensics
- Threat analysis
- Operational readiness for critical cyber events

16.4. Does Leonardo provide Cyber Resilience services? Yes. Leonardo provides a comprehensive Cyber Resilience model that includes risk identification, assessment, response, and continuous monitoring to ensure service continuity even during cyberattacks.

16.5. Are the data stored on Leonardo protected and "sovereign"? Yes: - Data is encrypted, and encryption keys can be customer-managed.
- Geo-distributed storage enhances sovereignty and reduces single-point risk.
- Security policies include continuous reviews and alignment with global standards.

16.6 Does Leonardo collaborate with partners to enhance cloud security? Yes. For example: - Leonardo works with **Aruba** to deliver sovereign, high-performance cloud services enriched with cybersecurity capabilities.
- Collaboration ensures national data residency and adherence to strict security standards.

16.7 What international security standards does Leonardo follow? Leonardo follows industry best practices and global standards (including ISO frameworks), adopting modern governance, risk management, and compliance methodologies suitable for the current cybersecurity landscape.