Data Space 4 Mobility Models integration

Project Acronym:	**23-ES-TG-DS4MOBMODELS**
Project ID:	**101176007**

Deliverable number:	**D5.2**
Deliverable name:	**Technical Specifications of the Mobility Data Space Infrastructure**
Work Package number:	**WP5 - Mobility Data Space**
Due date:	**11/30/2025**
Delivery date:	**28/07/2026**
Lead Beneficiary:	**INFONET**
Main author:	**Alberto Garabato Sixto**

Co-funded by the European Union

Document fiche	
Authors:	Alberto Garabato Sixto, INFONET
Internal reviewers:	Marcos Vázquez, INFONET; Juan Carlos Armas
Work package:	WP5
Task:	T5.2
Nature:	R
Dissemination:	PU

Document History			
Version	**Date**	**Contributor(s)**	**Description**
V 0.1	21/04/2026	INFONET	Initial draft – VDC deployment
V 0.2	25/04/2026	INFONET	Architecture updated following NTT DATA meeting (21/04/2026)
V 0.3	17/05/2026	INFONET	Added monitoring stack, network details, access users
V 1.0	22/05/2026	INFONET	Final version for submission
V 1.1	22/05/2026	INFONET	
V 1.2	15/06/2026	INFONET	Revised following internal reviewers' comments
V 1.3	26/06/2026	INFONET	Revised following EYSA review: section structure, naming, IP/network consistency, backup encryption and retention, alerting tool, expanded references
V 1.4	24/07/2026	INFONET	Revised following Project Officer comments: added project/WP context and relation to other deliverables, non-discriminatory access and technology dependency clarifications; monitoring platform corrected to Zabbix; network diagram regenerated at print resolution
V 1.5	24/07/2026	INFONET	Network data aligned with the Cloud.gal console: BI Pre-production VM

			confirmed at 10.3.12.194 on VL146; VM naming restored to console values; VL145 documented as the reserved segment; network diagram updated accordingly
V2	28/07/2026	EYSA	Final review

Keywords:	Cloud Infrastructure, Virtual Data Center, VDC, Mobility Data Space, DS4MOBMODELS, Cloud.gal, DevSecOps, VPN, VLAN, Pure Storage, Monitoring, Zabbix, Grafana, Prometheus, Loki
Abstract:	This deliverable describes the cloud infrastructure deployed by INFONET / Cloud.gal for the DS4MOBMODELS project (WP5, T5.2). It presents the Virtual Data Center VDC.DS4MOB provisioned on the Cloud.gal private cloud platform, incorporating the updated architecture agreed with NTT DATA. The document details the six active virtual machines across the BI Development, BI Test, BI Pre-production, BI Production, Data Space (DES+Test) and Monitoring environments; the four network segments (VL144–VL147); the centralised SSD storage backed by Pure Storage; VPN-based access for NTT DATA; and the Zabbix infrastructure monitoring platform operated by INFONET and the dedicated monitoring instance running Grafana, Prometheus, Loki, Fluentd, cAdvisor, Portainer and Cockpit. Pending actions include credential delivery, bastion host deployment, MFA rollout, and CI/CD pipeline integration via NTT DATA internal Git.

Table of Contents

1 EXECUTIVE SUMMARY 9

2 INTRODUCTION 10

2.1 Relation to Other Deliverables and Public Results 11

2.2 Non-Discriminatory Access 11

2.3 Technology Dependency and Vendor Lock-In 11

3 VIRTUAL DATA CENTER OVERVIEW 13

4 DEPLOYED INFRASTRUCTURE BY ENVIRONMENT 14

4.1 BI Development Environment 14

4.2 BI Test Environment 15

4.3 BI Pre-production Environment 15

4.4 BI Production Environment 15

4.5 Data Space Environment (DES + Test) 16

5 NETWORK ARCHITECTURE 17

5.1 Access Method 19

6 STORAGE AND BACKUP 20

6.1 Storage by Environment 20

6.2 Backup Policy 20

7 MONITORING AND LOGGING 22

7.1 7.1 Deployed Monitoring Stack 22

7.2 Alerting and Incident Notification 23

8 SECURITY CONFIGURATION 25

8.1 Implemented Controls 25

8.2 Pending Security Controls 25

8.3 Proactive Security: Threat Hunting and Advanced Threat Detection 25

9 SERVICE CONTINUITY AND SLA 27

9.1 Redundancy Architecture – Three Independent Levels 27

9.2 SLA Commitments 27

10 INFRASTRUCTURE AS CODE AND AUTOMATION 29

11 SCALABILITY AND CAPACITY PLANNING 30

11.1 Current Resource Utilisation 30
11.2 Planned Scalability Steps 30
12 ENVIRONMENT ISOLATION SUMMARY 32
13 CONCLUSIONS AND NEXT STEPS 33
14 REFERENCES 34

Table of figures

Figure 1. VDC.DS4MOB – Virtual Machines overview (Cloud.gal console) 13
Figure 2 Network 18
Figure 3. VDC.DS4MOB – Network segments / VLANs (Cloud.gal console) 18
Figure 4 Backup job execution report VDC-DS4mob-6 of 6 VMs processed successfully. 21
Figure 5. Infrastructure monitoring dashboard – latency and availability per datacentre (MAD1, MAD3). 22

Table of tables

Table 1. Resources 13
Table 2.Deployed 14
Table 3. BI Development Environment 14
Table 4. BI Test Environment 15
Table 5. BI Pre-production 15
Table 6. BI Production Environment 15
Table 7. Data Spaces 16
Table 8. Vlans Network 18
Table 9.Storage Infrastructure 20
Table 10. Deployed Monitoring Stack 22
Table 11. Alerting and Incident 23
Table 12. SLA 27
Table 13. Current Resource 30
Table 14. .Environment 32
Table 15. Next Steps 33

Definitions, Acronyms and Abbreviations

Acronym	Title
API	Application Programming Interface – Set of protocols allowing applications to communicate with each other.
BI	Business Intelligence – Technology and processes for analysing data to support decision-making.
cAdvisor	Container Advisor – Google tool for collecting container resource usage and performance metrics.
CI/CD	Continuous Integration / Continuous Delivery – DevOps practice for automating build, test and deployment pipelines.
CPU	Central Processing Unit – Primary processor of a virtual machine, measured in vCPUs.
DEV	Development environment – Environment used for active software development and unit testing.
DES	Test environment (Development) – Environment used for integration and automated testing.
DevSecOps	Development Security Operations – Practice integrating security into every phase of the DevOps lifecycle.
HTTPS	Hypertext Transfer Protocol Secure – Encrypted version of HTTP using TLS to secure web communications.
IaC	Infrastructure as Code – Management of infrastructure through machine-readable configuration files.
IP	Internet Protocol – Numerical label assigned to each device on a network.
MFA	Multi-Factor Authentication – Authentication method requiring two or more verification factors.
PRE	Pre-production environment – Environment mirroring production, used for final validation before go-live.
PRO	Production environment – Live operational environment serving end users.
RAM	Random Access Memory – Volatile memory used by virtual machines for active workload processing.
SSD	Solid State Drive – High-performance storage device with no moving parts.
SSH	Secure Shell – Cryptographic network protocol for secure remote access to servers.
TLS	Transport Layer Security – Cryptographic protocol securing data transmitted over networks.

VDC	Virtual Data Center – Logical grouping of virtualised compute, network and storage resources.
VLAN	Virtual Local Area Network – Network segment isolated at layer 2, used to segregate traffic between environments.
VM	Virtual Machine – Software emulation of a physical computer running on a hypervisor.
VPN	Virtual Private Network – Encrypted tunnel enabling secure remote access to a private network.
WP	Work Package – Defined unit of work within a European project, grouping related tasks and deliverables.
ENS	Esquema Nacional de Seguridad – Spanish National Security Framework. ENS Alto is the highest certification level for cloud providers operating with public entities.
NGFW	Next-Generation Firewall – Advanced firewall providing deep packet inspection, IPS/IDS, application control and integrated threat intelligence.
NVMe	Non-Volatile Memory Express – High-performance storage protocol designed for solid-state drives, delivering sub-millisecond latency.
RPO	Recovery Point Objective – Maximum acceptable data loss measured in time.
RTO	Recovery Time Objective – Maximum acceptable time to restore a system after an incident.
SLA	Service Level Agreement – Contractual commitment defining availability, performance and support obligations.
vLCM	vSphere Lifecycle Manager – VMware tool for standardised, automated firmware and software updates across all cluster hosts.
Zabbix	Open-source infrastructure monitoring platform – Used by INFONET to supervise compute health, availability, network latency and storage occupancy across the VDC, and to generate and route operational alerts.

1 Executive Summary

This deliverable (D5.2) documents the cloud infrastructure provisioned by INFONET / Cloud.gal for the DS4MOBMODELS project (Work Package 5, Task T5.2). It provides a complete technical record of the Virtual Data Center VDC.DS4MOB deployed on the Cloud.gal private cloud platform, covering the agreed architecture, the deployed virtual machine inventory, network topology, storage configuration, backup policy, monitoring stack, security posture and pending actions.

The infrastructure was provisioned following the technical requirements agreed with NTT DATA at the project coordination meeting. Six virtual machines are currently active across the VDC, consuming 52 vCPUs, 136 GB RAM and approximately 3.1 TB of provisioned All-Flash NVMe storage. All environments are operational and confirmed in Powered On / Normal state.

The platform delivers a sovereign, certified infrastructure: 100% hosted in Spain on Digital Realty MAD1/MAD3 (Tier III, ENS Alto), built on AMD EPYC Gen4 compute, Pure Storage All-Flash NVMe, VMware vSphere 8.x and Fortinet NGFW. The proactive Threat Hunting capability, native to the Cloud.gal security architecture, provides continuous behavioural monitoring and incident response beyond conventional perimeter-only approaches.

2 Introduction

This document provides a comprehensive technical description of the cloud infrastructure deployed by INFONET / Cloud.gal for the DS4MOBMODELS project. DS4MOBMODELS (Data Space 4 Mobility Models Integration, project ID 101176007) is a European co-funded initiative under the Connecting Europe Facility (CEF) programme, aimed at building an interoperable mobility data space supporting advanced analytics, business intelligence and data exchange between mobility stakeholders.

Within Work Package 5 (Mobility Data Space), Task T5.2 assigns to INFONET the responsibility of provisioning and operating the cloud infrastructure on which NTT DATA deploys the data space building blocks: Identity Service, Vocabulary Hub, Data Catalogue, Connector, Observability Service and the BI analytics stack.

The infrastructure was provisioned on Cloud.gal, operated by INFONET from the Digital Realty MAD1/MAD3 datacentre in Madrid. The architecture reflects requirements agreed between INFONET and NTT DATA at the project coordination meeting, which established the definitive environment topology, resource sizing and access model. The architecture separates Business Intelligence workloads (four environments: Development, Test, Pre-production, Production) from the Data Space instance (a single combined DES+Test VM), with a dedicated Monitoring instance serving the full stack. This segregation ensures environment independence, simplifies access control and supports safe code promotion from development through to production.

The document is structured as follows:

- Section 3: Virtual Data Center (VDC.DS4MOB) overview.
- Section 4: Deployed infrastructure per environment.
- Section 5: Network architecture and VPN access model.
- Section 6: Storage and backup policy.
- Section 7: Monitoring and logging stack.
- Section 8: Security configuration and access management.
- Section 9: Service continuity and SLA.
- Section 10: Infrastructure as Code and automation.
- Section 11: Scalability and capacity planning.
- Section 12: Environment isolation summary.
- Section 13: Conclusions and next steps.
- Section 14: References.

2.1 Relation to Other Deliverables and Public Results

D5.2 documents the cloud infrastructure layer of the project: the Virtual Data Center (VDC.DS4MOB) provisioned and operated by INFONET / Cloud.gal, on which NTT DATA deploys the data space building blocks. It therefore sits below, and provides the technical foundation for, the functional and governance deliverables of Work Package 5.

The onboarding processes and access policies that govern how third-party stakeholders join the mobility data space are defined in D5.1 and further detailed in D5.3, which specify the Connector, the Identity Service and the associated access policies. The role of D5.2 is to ensure that the underlying infrastructure imposes no technical barrier to that onboarding.

The infrastructure described in this document corresponds to the development and construction phase of the project. The production topology, and the access model associated with it, will be specified in D5.5 once that topology is finalised. Readers interested in the functional layer of the data space, rather than the infrastructure that hosts it, should therefore refer to D5.1, D5.3 and D5.5.

2.2 Non-Discriminatory Access

In line with the principle of non-discriminatory access set out in the Grant Agreement (Section 5), access for third-party stakeholders is guaranteed at the operational / data space layer rather than at the infrastructure layer. The infrastructure documented here is a hosting platform: it does not mediate, filter or prioritise stakeholder access to the data space itself.

Access is governed by the onboarding processes defined in D5.1 and detailed in D5.3. What D5.2 contributes to that principle is the guarantee that the underlying platform introduces no technical barrier to onboarding: the network architecture, the VPN access model and the environment isolation scheme described in Sections 5, 8 and 12 are designed so that additional participants can be connected without re-architecting the platform.

This is further reinforced by the Connector-as-a-Service research line developed by NTT DATA, which reduces the residual technological friction that a new stakeholder might otherwise face when connecting to the data space.

2.3 Technology Dependency and Vendor Lock-In

At the physical infrastructure layer there is a single-vendor dependency: the platform runs on the Cloud.gal private cloud, built on VMware vSphere, Pure

Storage and hosted in the Digital Realty datacentre. This deliverable states that dependency explicitly rather than understating it.

It should be noted, however, that this dependency is not different in nature from the one that arises when deploying on any single hyperscaler, such as Azure, Google Cloud or Oracle Cloud. Migrating a production platform between any of these providers involves a non-trivial re-architecture; it is a general property of cloud infrastructure rather than a constraint specific to Cloud.gal. At the layers above the infrastructure, the use of containerised workloads and open-source components in the monitoring and data space stacks limits the extent to which the project is tied to any single provider.

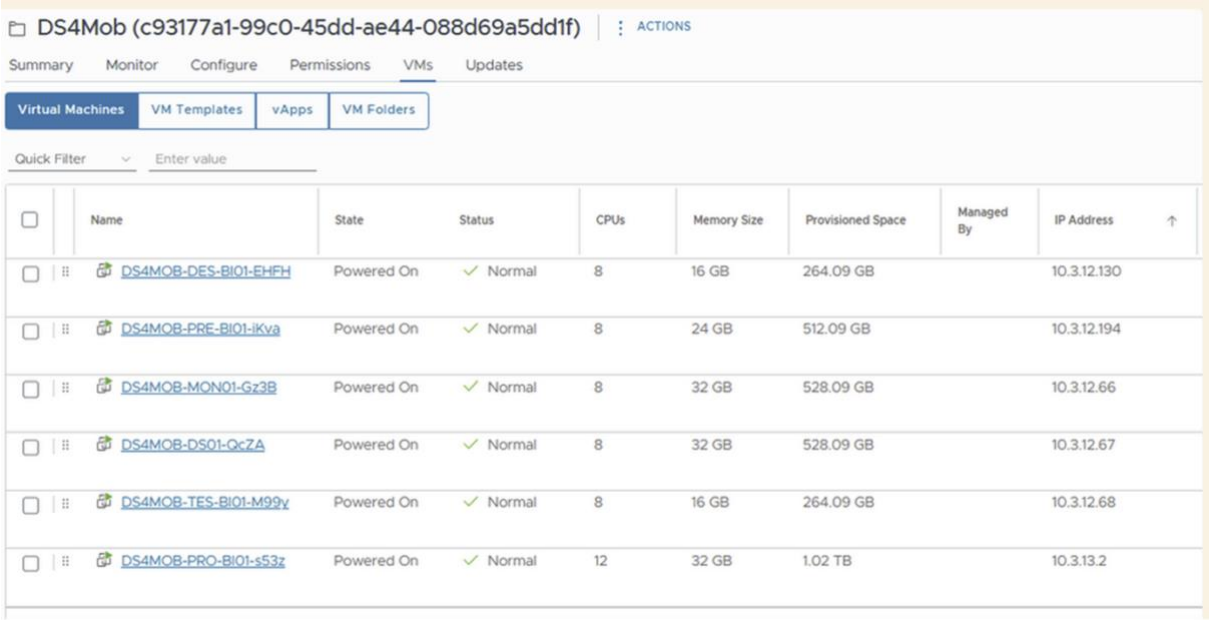
3 Virtual Data Center Overview

The VDC.DS4MOB (identifier: c93177a1-99c0-45dd-ae44-088d69a5dd1f) is provisioned on the Cloud.gal platform. It currently hosts six virtual machines, all in Powered On / Normal state, distributed across four dedicated network segments.

Table 1. Resources

Resource	Allocated
Active VMs	6
Total vCPUs	52
Total Memory	136 GB
Total provisioned storage	~3.1 TB
Network segments	4 (VL144–VL147)

Figure 1. VDC.DS4MOB – Virtual Machines overview (Cloud.gal console)



4 Deployed Infrastructure by Environment

The following table summarises all active virtual machines observed in the Cloud.gal vSphere console. Data reflects the actual provisioned state.

Table 2.Deployed

VM Name	Environment	vCPUs	Memory	Storage	IP Address	Network
DS4MOB-DES-BI01-EHFH	BI – Test	8	16 GB	264.09 GB	10.3.12.130	VL144-DS4Mob
DS4MOB-PRE-BI01-iKva	BI – Pre-production	8	24 GB	512.09 GB	10.3.12.194	VL146-DS4Mob
DS4MOB-MON01-Gz3B	Monitoring	8	32 GB	528.09 GB	10.3.12.66	VL144-DS4Mob
DS4MOB-DS01-QcZA	Data Space (DES+Test)	8	32 GB	528.09 GB	10.3.12.67	VL144-DS4Mob
DS4MOB-TES-BI01-M99y	BI – Development	8	16 GB	264.09 GB	10.3.12.68	VL144-DS4Mob
DS4MOB-PRO-BI01-s53z	BI – Production	12	32 GB	1.02 TB	10.3.13.2	VL147-DS4Mob

4.1 BI Development Environment

Hosts the Business Intelligence development workloads. Aligned with NTT DATA specification: 8 vCPUs, 16 GB RAM, 256 GB SSD, 1 Gbps network.

Table 3. BI Development Environment

Parameter	Specified	Deployed
CPU	8 vCPUs	8 vCPUs
Memory	16 GB	16 GB
Storage	256 GB SSD	264.09 GB
Network	1 Gbps	VL144-DS4Mob (10.3.12.65/27)
IP Address	—	10.3.12.68

4.2 BI Test Environment

Hosts the Business Intelligence test workloads. Aligned with NTT DATA specification: 8 vCPUs, 16 GB RAM, 256 GB SSD, 1 Gbps.

Table 4. BI Test Environment

Parameter	Specified	Deployed
CPU	8 vCPUs	8 vCPUs
Memory	16 GB	16 GB
Storage	256 GB SSD	264.09 GB
Network	1 Gbps	VL144-DS4Mob (10.3.12.65/27)
IP Address	—	10.3.12.130

4.3 BI Pre-production Environment

Hosts the Business Intelligence pre-production workloads, sized as a production replica for final validation. Aligned with NTT DATA specification: 8 vCPUs, 24 GB RAM, 500 GB SSD, 1 Gbps.

Table 5. BI Pre-production

Parameter	Specified	Deployed
CPU	8 vCPUs	8 vCPUs
Memory	24 GB	24 GB
Storage	500 GB SSD	512.09 GB
Network	1 Gbps	VL146-DS4Mob (10.3.12.193/27)
IP Address	—	10.3.12.194

4.4 BI Production Environment

Hosts the live Business Intelligence production workloads. Aligned with NTT DATA specification: 12 vCPUs, 32 GB RAM, 1 TB SSD, 1 Gbps.

Table 6. BI Production Environment

Parameter	Specified	Deployed
CPU	12 vCPUs	12 vCPUs
Memory	32 GB	32 GB

Storage	1 TB SSD	1.02 TB
Network	1 Gbps	VL147-DS4Mob (10.3.13.1/27)
IP Address	—	10.3.13.2

4.5 Data Space Environment (DES + Test)

Single combined instance hosting the Data Space DES and Test workloads, per NTT DATA specification: 8 vCPUs, 32 GB RAM, 512 GB storage.

Table 7. Data Spaces

Parameter	Specified	Deployed
CPU	8 vCPUs	8 vCPUs
Memory	32 GB	32 GB
Storage	512 GB SSD	528.09 GB
Network	—	VL144-DS4Mob (10.3.12.65/27)
IP Address	—	10.3.12.67

5 Network Architecture

Four dedicated network segments (VLANs) ensure environment isolation within VDC.DS4MOB. All segments are operational (Status: Normal) as confirmed in the Cloud.gal console.

The VDC.DS4MOB network is designed around the principle of strict environment isolation. Four dedicated VLAN segments ensure that each environment group operates within its own layer-2 domain, with inter-VLAN traffic controlled and filtered by the Fortinet NGFW. This segmentation prevents lateral movement between environments in the event of a security incident and provides an independent blast radius for any network-layer fault.

All virtual machines connect via NVIDIA Mellanox ConnectX-6 NICs (100/200G) with RDMA and RoCE v2 support. Each ESXi host has redundant uplinks to both switches in the MLAG/vPC pair, ensuring no single NIC or switch failure can disrupt VM connectivity. Traffic planes are segregated: vMotion/DRS, management, NVMe-oF/RoCE storage and backup traffic each operate on dedicated virtual switches.

The separation of BI Production (VL147) onto a dedicated VLAN with distinct IP addressing is a deliberate security decision. It enables stricter firewall rules for the production segment, limits permitted source addresses for administrative access and ensures a compromise of a development or test environment cannot directly reach production assets.

VL145 is currently reserved and carries no workloads. It is provisioned and active to support horizontal scalability: new environments can be onboarded into VL145 without any changes to the existing routing or firewall policy baseline.

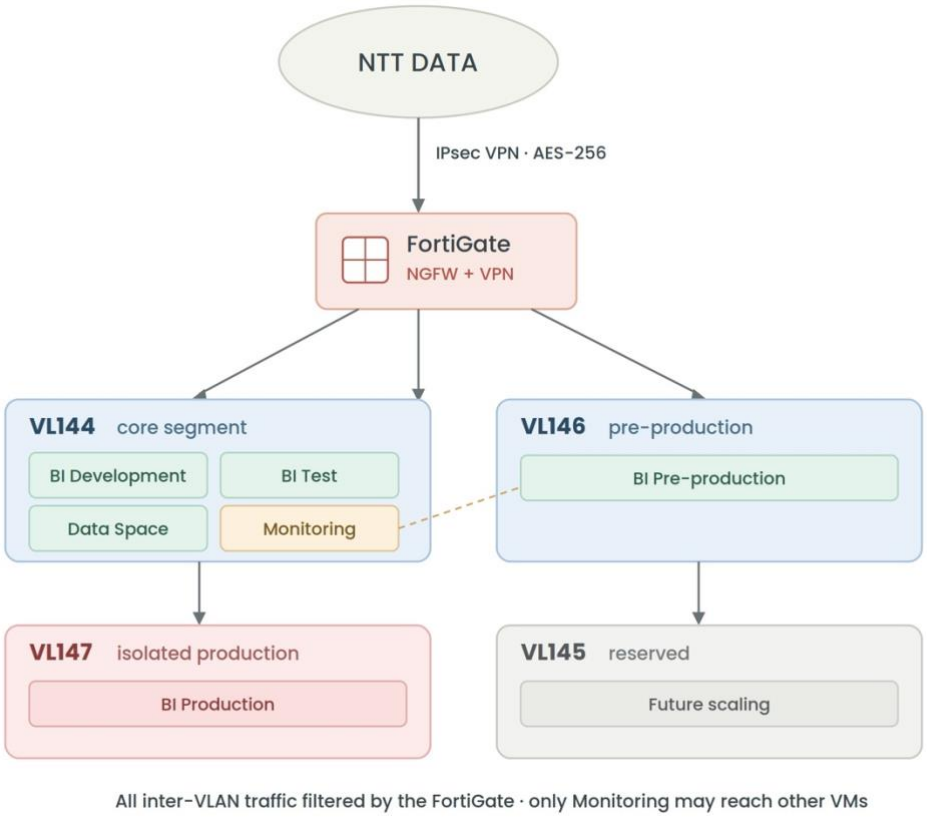


Figure 2 Network

Table 8. Vlans Network

Segment	CIDR Gateway	Environment(s)	Status
VL144-DS4Mob	10.3.12.65/27	BI Development, BI Test, Data Space, Monitoring	Normal
VL145-DS4Mob	10.3.12.129/27	Reserved / future use	Normal
VL146-DS4Mob	10.3.12.193/27	BI Pre-production	Normal
VL147-DS4Mob	10.3.13.1/27	BI Production	Normal

Name	Status	Gateway CIDR
VL144-DS4Mob	Normal	10.3.12.65/27
VL145-DS4Mob	Normal	10.3.12.129/27
VL146-DS4Mob	Normal	10.3.12.193/27
VL147-DS4Mob	Normal	10.3.13.1/27

Figure 3. VDC.DS4MOB – Network segments / VLANs (Cloud.gal console)

5.1 Access Method

As agreed with NTT DATA, all NTT DATA access to VDC.DS4MOB is provided exclusively via IPsec VPN (AES-256), terminated on the Fortinet FortiGate cluster. This decision was made to avoid exposing any VM management ports directly to the internet and to provide a single, auditable access channel for all NTT DATA operations. SSH access to individual VMs is routed through the VPN tunnel; direct public SSH is explicitly blocked at the firewall for all environments. This broad access model applies during the deployment phase, so that NTT DATA can operate autonomously throughout the build-out and service commissioning of the VDC. Once the platform transitions to the on-going operations phase, a more restricted, role-based access scope can be established by mutual agreement, limiting access to the specific environments and services required for run-time operations.

A bastion host for the PRE and PRO environments is planned as an additional hardening measure (see Section 9.2). The bastion will provide a single monitored SSH jump point for administrative access to those environments, with full session logging.

6 Storage and Backup

All virtual machines in the VDC.DS4MOB use centralised storage provisioned from the Cloud.gal Pure Storage FlashArray X50 All-Flash NVMe array. Storage is presented to VMware as NVMe-oF (NVMe over Fabrics) over RoCE v2, using dedicated NVIDIA Mellanox ConnectX-6 NICs on a separate storage VLAN, completely isolated from VM data and management traffic. This design eliminates storage I/O contention and provides deterministic sub-millisecond latency for all VMs regardless of concurrent workload activity on other environments.

6.1 Storage by Environment

Table 9.Storage Infrastructure

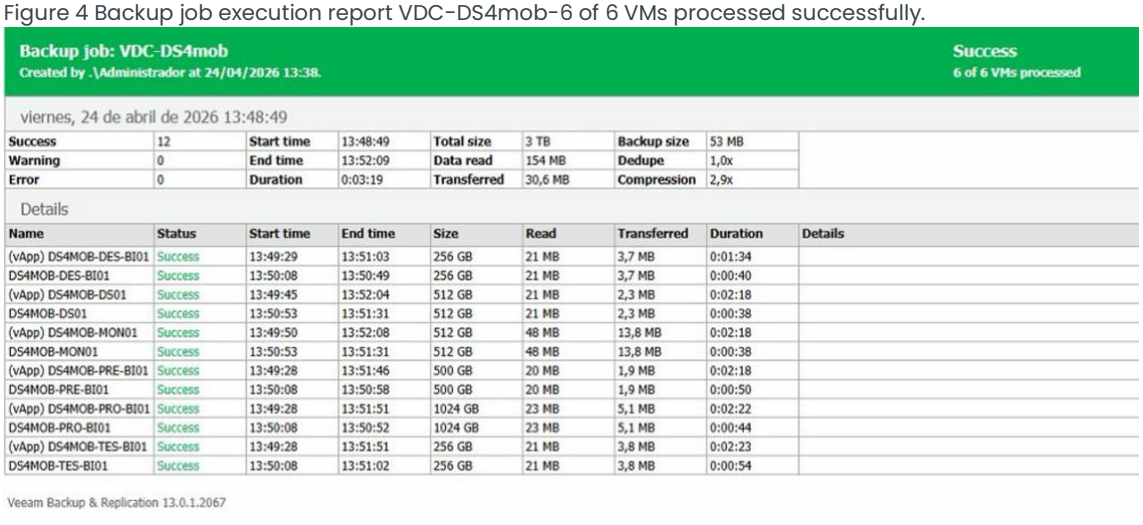
VM	Environment	Provisioned Storage	Technology
DS4MOB-TES-BI01-M99y	BI – Development	264.09 GB	Pure Storage SSD
DS4MOB-DES-BI01-EHFH	BI – Test	264.09 GB	Pure Storage SSD
DS4MOB-PRE-BI01-iKva	BI – Pre-production	512.09 GB	Pure Storage SSD
DS4MOB-PRO-BI01-s53z	BI – Production	1.02 TB	Pure Storage SSD
DS4MOB-DS01-QcZA	Data Space (DES+Test)	528.09 GB	Pure Storage SSD
DS4MOB-MON01-Gz3B	Monitoring	528.09 GB	Pure Storage SSD

6.2 Backup Policy

- Frequency: automated daily snapshots for all active VMs (6 of 6 VMs processed in the last run; duration: 3 min 19 s)
- Retention: 30 days for Production; 7 days for all other environments. Total protected size: 3 TB; backup size: 53 MB (deduplication 1.0x; compression 2.9x)
- Encryption: data-at-rest encryption is provided natively by the Pure Storage FlashArray at array level for all volumes across every environment; immutable SafeMode snapshot protection is applied per the retention policy above (30 days for Production, 7 days for all other environments).

- Recovery: snapshots are managed through the Pure Storage array management interface.
- The restore procedure follows a defined sequence:
- The INFONET operations team identifies the recovery point from the retained snapshot catalogue (daily snapshots, up to 30 days for Production);
- The affected VM is restored from the selected snapshot, either as an in-place rollback or as a parallel clone for validation before cut-over;
- Integrity and service checks are performed before the environment is returned to service. **Granular file-level recovery** is also supported by mounting the snapshot volume and extracting individual datasets without a full VM restore. Restore operations are initiated via a change request from NTT DATA or triggered directly by INFONET in the event of an incident and are targeted to complete within the agreed RTO; the daily snapshot cadence sets the effective RPO.

Figure 4 Backup job execution report VDC-DS4mob-6 of 6 VMs processed successfully.



Backup job: VDC-DS4mob — **Success**
Created by .\Administrador at 24/04/2026 13:38. — 6 of 6 VMs processed

viernes, 24 de abril de 2026 13:48:49

Success	12	Start time	13:48:49	Total size	3 TB	Backup size	53 MB
Warning	0	End time	13:52:09	Data read	154 MB	Dedupe	1,0x
Error	0	Duration	0:03:19	Transferred	30,6 MB	Compression	2,9x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
(vApp) DS4MOB-DES-BI01	Success	13:49:29	13:51:03	256 GB	21 MB	3,7 MB	0:01:34	
DS4MOB-DES-BI01	Success	13:50:08	13:50:49	256 GB	21 MB	3,7 MB	0:00:40	
(vApp) DS4MOB-DS01	Success	13:49:45	13:52:04	512 GB	21 MB	2,3 MB	0:02:18	
DS4MOB-DS01	Success	13:50:53	13:51:31	512 GB	21 MB	2,3 MB	0:00:38	
(vApp) DS4MOB-MON01	Success	13:49:50	13:52:08	512 GB	48 MB	13,8 MB	0:02:18	
DS4MOB-MON01	Success	13:50:53	13:51:31	512 GB	48 MB	13,8 MB	0:00:38	
(vApp) DS4MOB-PRE-BI01	Success	13:49:28	13:51:46	500 GB	20 MB	1,9 MB	0:02:18	
DS4MOB-PRE-BI01	Success	13:50:08	13:50:58	500 GB	20 MB	1,9 MB	0:00:50	
(vApp) DS4MOB-PRO-BI01	Success	13:49:28	13:51:51	1024 GB	23 MB	5,1 MB	0:02:22	
DS4MOB-PRO-BI01	Success	13:50:08	13:50:52	1024 GB	23 MB	5,1 MB	0:00:44	
(vApp) DS4MOB-TES-BI01	Success	13:49:28	13:51:51	256 GB	21 MB	3,8 MB	0:02:23	
DS4MOB-TES-BI01	Success	13:50:08	13:51:02	256 GB	21 MB	3,8 MB	0:00:54	

Veeam Backup & Replication 13.0.1.2067

7 Monitoring and Logging

A dedicated monitoring instance (DS4MOB-MON01-Gz3B, 8 vCPUs / 32 GB / 528 GB, IP 10.3.12.66, VLAN VL144) hosts the complete observability stack. By isolating monitoring workloads to a dedicated VM, the platform ensures observability overhead does not impact production performance and that monitoring data is collected even under stress conditions on observed VMs.

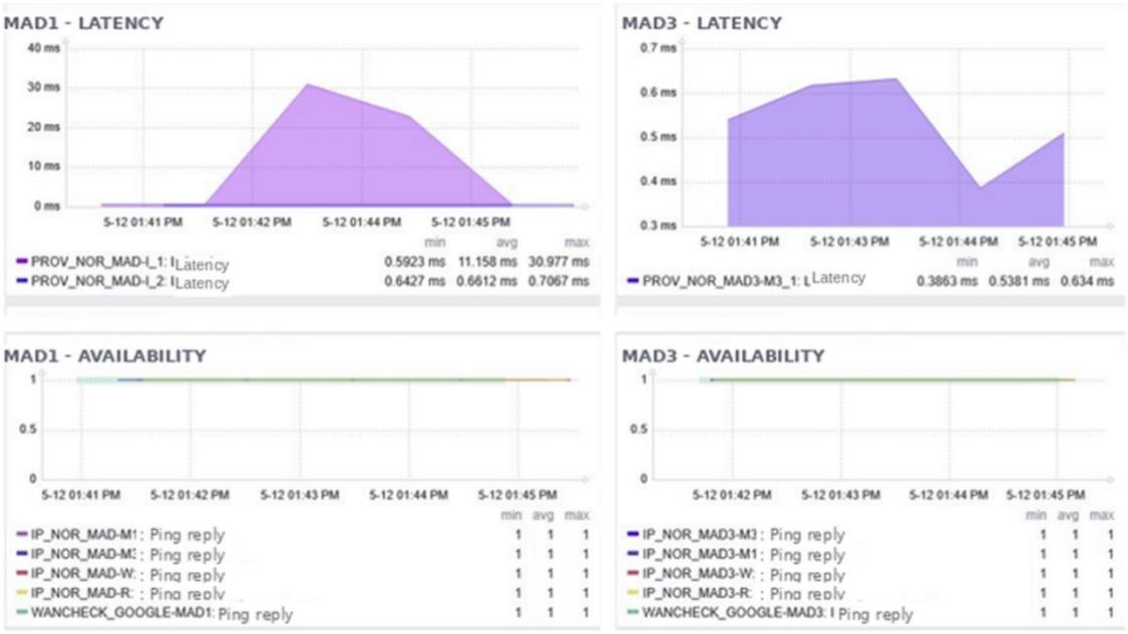


Figure 5. Infrastructure monitoring dashboard – latency and availability per datacentre (MAD1, MAD3).

The monitoring instance has controlled access to all other environments via inter-VLAN routing rules that permit only monitoring-specific traffic (metrics scraping, log forwarding) from the monitoring VM's IP. All other inter-VLAN traffic is blocked by the Fortinet NGFW.

7.1 7.1 Deployed Monitoring Stack

The following tools are deployed on the monitoring instance, per the NTT DATA technology specification, forming a fully integrated observability pipeline:

Table 10. Deployed Monitoring Stack

Tool	Category	Function in DS4MOBMODELS
Grafana	Dashboards & Visualisation	Centralised dashboards for metrics, logs and traces. Primary observability UI for NTT DATA and INFONET operations teams.
Prometheus	Metrics & Alerting	Scrapes metrics from all VMs and containerised services. Evaluates alerting rules and routes notifications.

Zabbix	Infrastructure Monitoring & Alerting	Infrastructure-level monitoring platform operated by INFONET. Supervises compute health, host and service availability, network latency and storage occupancy across the VDC, and routes alerts to the INFONET operations team.
Loki	Log Aggregation	Centralised log store for all VMs, queryable via Grafana. Retains structured and unstructured log streams.
Fluentd	Log Forwarding	Collects and routes logs from all environments to Loki. Handles format normalisation and filtering.
cAdvisor	Container Metrics	Per-container resource usage (CPU, memory, network, disk I/O) for all Docker workloads across the VDC.
PgAdmin	DB Management	Web-based administration interface for PostgreSQL databases in the Data Space environment.
MongoDB Compass	DB Management	GUI management for MongoDB instances used by the Data Space building blocks.
Portainer	Container Management	Web UI for managing Docker containers, images and volumes across VDC environments.
Cockpit	System Management	Linux server management providing system health, journal logs and resource metrics per VM.

7.2 Alerting and Incident Notification

The Zabbix monitoring platform operated by INFONET is configured with alerting rules across four infrastructure categories: compute health (VM CPU and memory), availability (host and service reachability), network latency, and storage occupancy. Each alert is assigned a severity level (Info / Warning / Critical) and routed to the INFONET operations team following the escalation matrix below.

Table 11. Alerting and Incident

Category	Info	Warning	Critical
Compute VM/CPU/RAM	Normal usage within range	CPU >85% sustained 5 min · RAM >90%	CPU >95% sustained · VM unresponsive
Availability ICMP /Service	Service responding (ping OK)	Intermittent packet loss	Host / Service down (no response)
Latency Network RTT	RTT within expected range	RTT > 2X reference average	RTT >5× average or timeouts
Storage Disk occupancy	Occupancy <75%	Occupancy >80%	Occupancy >90%

Grafana dashboards provide real-time and historical views of all collected metrics, with pre-built panels for: per-VM resource utilisation, container health across all environments, storage I/O and latency from Pure Storage, backup job status, and network throughput per VLAN segment.

8 Security Configuration

8.1 Implemented Controls

- VLAN isolation: each environment operates on a dedicated network segment with independent routing rules
- VPN access: all NTT DATA access to VMs is routed exclusively via VPN tunnel
- Firewall rules: least-privilege rules per VLAN segment
- TLS: HTTPS endpoints secured via Let's Encrypt certificates

8.2 Pending Security Controls

- Bastion host deployment for PRE and PRO environments
- MFA rollout for all administrative access
- Definition of SSH key rotation schedule
- Granular IAM role-based access per environment
- Centralised audit logging with encryption and versioning

8.3 Proactive Security: Threat Hunting and Advanced Threat Detection

The Cloud.gal platform incorporates active Threat Hunting capabilities as a native component of its security architecture. Security is not limited to blocking known threats: the platform continuously identifies anomalous behaviours and advanced threats before they materialise. This capability combines two complementary layers. The first is automated detection at the network perimeter: the FortiGate NGFW performs deep packet inspection, intrusion prevention and detection (IPS/IDS) and application control on all inter-VLAN and VPN traffic, while FortiGuard threat intelligence feeds keep signatures and reputation data current, responding to known threat patterns and predefined thresholds. The second layer is Threat Hunting, a security service included as standard across all Cloud.gal services and operated by the INFONET security team. Unlike automated detection, Threat Hunting is a human-led process: analysts proactively search the infrastructure telemetry for indicators of threats that have not triggered any automated alert. This search is guided by hypotheses based on the MITRE ATT&CK framework — the techniques and tactics attackers use to move laterally, escalate privileges, exfiltrate data or stage ransomware — and is able to surface intrusions that operate stealthily over weeks or months without raising any conventional alarm. This proactive approach is essential in environments where data availability and integrity are critical, such as the DS4MOBMODELS infrastructure.

- **Continuous log and event analysis:** real-time correlation of network, endpoint and storage events to detect anomalous patterns across the VDC.DS4MOB environments.
- **Lateral movement and privilege escalation detection:** identification of MITRE ATT&CK techniques that bypass traditional perimeter controls, including cross-environment movement between the six VDC.DS4MOB instances.
- **Integrated Threat Intelligence:** continuously updated IOC (Indicators of Compromise) feeds applied in real time across the client infrastructure, providing proactive defence against emerging threat campaigns.
- **Guided incident response:** upon detection of an active threat, the INFONET security team acts immediately with containment, forensic analysis and remediation procedures, with response to critical incidents under 1 hour.
- **Immutable data protection:** the combination of active Threat Hunting with Pure Storage SafeMode immutable snapshots ensures that even if an attacker reaches the storage layer, backup data remains intact and unrecoverable by ransomware throughout the 30-day Production retention period (7 days for non-Production environments).

9 Service Continuity and SLA

The Cloud.gal platform is architected for mission-critical continuity. No single component failure – host, NIC, switch, storage controller, firewall or carrier – causes a service interruption. The following subsections document the specific continuity mechanisms and SLA commitments applicable to the DS4MOBMODELS VDC.

9.1 Redundancy Architecture – Three Independent Levels

Level 1 – Compute (VMware cluster active-active): all cluster nodes participate actively. Failover upon host failure is immediate and automatic (VMware HA), with no manual intervention. DRS rebalances workloads continuously. vMotion enables planned maintenance without VM downtime.

Level 2 – Internal network (dedicated planes + redundant NICs): dedicated NVIDIA Mellanox ConnectX-6 NICs (100/200G) with RDMA and RoCE v2 for storage traffic. MLAG/vPC uplink redundancy to the switch pair. Automatic failback between physical NICs on incident. Management, storage, vMotion and backup traffic planes fully segregated.

Level 3 – Data (Pure Storage + immutability + Veeam): primary storage on Pure Storage FlashArray X50 in active-active controller mode. Immutable SafeMode snapshots. Dedicated backup on Pure Storage C50R4 All-Flash with Veeam B&R v13 – 100% independent from primary storage. SureBackup automated recoverability verification after each backup run.

9.2 SLA Commitments

Table 12. SLA

SLA Parameter	Commitment	Notes
Platform availability	99.982% annual uptime	Tier III Uptime Institute guarantee – datacentre layer
VM availability (HA)	99.9% (excl. planned maintenance)	VMware HA N+1 – automatic restart on host failure
Critical incident response	< 1 hour	24×7×365 INFONET operations team
Planned maintenance notice	≥ 48 hours	Communicated to NTT DATA technical lead in advance
Backup frequency	Daily automated	All 6 VMs – Veeam B&R v13
RTO (full VM restore)	< 30 minutes	All-Flash NVMe backup repository enables rapid restoration
RPO (maximum data loss)	< 24 hours	Daily backup cycle; reducible to hourly via snapshot schedule

Backup retention – Production	30 days immutable	Pure Storage C50R4 SafeMode – cannot be overridden
Backup retention – Other envs	7 days immutable	Pure Storage C50R4 SafeMode – cannot be overridden
Security incident response	< 1 hour (critical)	Threat Hunting + INFONET security team
Escalation to vendor (L3)	Same business day	Direct channel to VMware, Pure Storage, Fortinet, Veeam

10 Infrastructure as Code and Automation

NTT DATA will use its internal Git repositories and CI/CD pipelines for automation, reusing pipeline definitions from similar prior projects. This avoids duplication of effort and accelerates delivery.

- Version control: NTT DATA internal Git
- CI/CD: NTT DATA internal pipelines (existing, reused)
- Configuration management: coordinated with INFONET for infrastructure-level provisioning
- Quality gates: automated build, unit and integration tests executed on each pipeline run, with test management and traceability through QMetry; a release is only promoted when its quality gate passes.

The CI/CD workflow follows the standard NTT DATA delivery process: changes are committed to the internal Git repository and trigger a pipeline that builds the artefacts, runs the automated test suite and validation steps, and, on success, deploys to the target environment following the promotion path (Development → Test → Pre-production → Production). Each stage requires its quality gate to pass before promotion, with test execution and results tracked in QMetry for full traceability. Infrastructure-level changes that fall outside the application pipeline (resource sizing, network or storage provisioning) are coordinated with INFONET through the change-request procedure described in the Scalability and Capacity Planning section.

11 Scalability and Capacity Planning

The VDC.DS4MOB architecture has been designed with explicit scalability headroom to accommodate project growth without architectural redesign.

11.1 Current Resource Utilisation

Table 13. Current Resource

Resource	provisioned (VDC)	Currently consumed	Available headroom
vCPUs	Cluster capacity (scalable)	52 vCPUs across 6 VMs	Expandable on request
Memory (RAM)	Cluster capacity (scalable)	136 GB across 6 VMs	Expandable on request
Primary storage	Pure Storage FlashArray X50	~3.1 TB provisioned	Additional volumes on request
Backup storage	Pure Storage C50R4 (dedicated)	~53 MB/day effective	Large headroom given 2.9x compression
Network segments	4 VLANs provisioned	3 active (VL144, VL146, VL147)	VL146 reserved – immediately available
IP addressing (VL144)	/27 – 30 usable addresses	4 addresses in use	26 addresses available for new VMs
IP addressing (VL146)	/27 – 30 usable addresses	0 in use	Fully available for new environment

11.2 Planned Scalability Steps

- **VL145 activation:** the reserved VLAN (10.3.12.129/27) is available for immediate assignment. Candidate use cases: a dedicated Data Space DES instance, a staging environment for Connector stack updates, or additional BI tenant isolation.
- **VM horizontal scaling:** new VMs can be provisioned into any existing VLAN without firewall reconfiguration. Storage volumes are allocated from the existing FlashArray X50 on demand.
- **Compute node expansion:** the Cloud.gal cluster can absorb additional ESXi hosts without service interruption, providing additional vCPU and RAM capacity as project workloads grow.
- **Data Space instance split:** the current combined DES+Test instance (DS4MOB-DS01-QcZA) can be split into two independent VMs and assigned to VL146, following the same specification currently deployed.

All scalability operations are performed by INFONET and completed within agreed SLA windows. NTT DATA submits a change request through the INFONET support channels — a Freshdesk ticket, e-mail, or telephone for urgent cases — specifying the requested change, target environment and required date.

INFONET reviews, provisions and confirms completion back to the requester within the agreed lead time (standard: next business day; urgent: same day with prior agreement).

12 Environment Isolation Summary

Table 14. .Environment

VM	Environment	Network Segment	IP	vCPUs	RAM	Storage
DS4MOB-TES-BI01-M99y	BI Development	VL144 (10.3.12.65/27)	10.3.12.68	8	16 GB	264 GB
DS4MOB-DES-BI01-EHFH	BI Test	VL144 (10.3.12.65/27)	10.3.12.130	8	16 GB	264 GB
DS4MOB-PRE-BI01-iKva	BI Pre-production	VL146 (10.3.12.193/27)	10.3.12.194	8	24 GB	512 GB
DS4MOB-PRO-BI01-s53z	BI Production	VL147 (10.3.13.1/27)	10.3.13.2	12	32 GB	1.02 TB
DS4MOB-DS01-QcZA	Data Space DES+Test	VL144 (10.3.12.65/27)	10.3.12.67	8	32 GB	528 GB
DS4MOB-MON01-Gz3B	Monitoring	VL144 (10.3.12.65/27)	10.3.12.66	8	32 GB	528 GB

13 Conclusions and Next Steps

The DS4MOB cloud infrastructure is fully operational across all six environments. All VMs are in Powered On / Normal state as confirmed in the Cloud.gal management console. The architecture reflects the decisions agreed with NTT DATA (last requirements review: 21/04/2026) and provides the compute, storage, network and security foundation required to support the Data Space and Business Intelligence workloads specified in D5.3. The platform delivers a sovereign, certified stack: 100% hosted in Spain (Digital Realty MAD1/MAD3, Tier III, ENS Alto), built on AMD EPYC Gen4, Pure Storage All-Flash NVMe, VMware vSphere 8.x and Fortinet NGFW. The proactive Threat Hunting capability native to Cloud.gal provides continuous behavioural monitoring and incident response beyond conventional perimeter-only security approaches.

Additionally, the internal deployment of connectors as a service is currently being evaluated and will be described in detail in deliverable D5.7. As next steps, the optimal deployment model will be assessed: a single shared instance for multiple connectors or a dedicated instance per connector, based on the isolation, performance and scalability requirements of each one.

Table 15. Next Steps

Action	Status	Responsible
VPN configuration and credential delivery to NTT DATA users	In progress	INFONET
Bastion host deployment (PRE, PRO)	Pending	INFONET
MFA rollout and SSH key rotation	Pending	INFONET / NTT DATA
Monitoring stack validation by NTT DATA	Pending	NTT DATA
CI/CD pipeline integration (NTT DATA internal Git)	Pending	NTT DATA
BI Production environment validation	Pending	NTT DATA / INFONET

14 References

[1] Pure Storage (2025). FlashArray Technical Overview. Available at: https://www.purestorage.com

[2] CNCF (2024). Prometheus documentation. Available at: https://prometheus.io/docs

[3] Grafana Labs (2024). Grafana documentation. Available at: https://grafana.com/docs

[4] VMware (2024). vSphere 8.0 Documentation. Available at: https://docs.vmware.com/en/VMware-vSphere

[5] Fortinet (2024). FortiGate / FortiOS Administration Guide. Available at: https://docs.fortinet.com

[6] Fortinet (2024). FortiGuard Security Services. Available at: https://www.fortiguard.com

[7] Veeam (2024). Veeam Backup & Replication User Guide. Available at: https://www.veeam.com/documentation-guides-datasheets.html

[8] Grafana Labs (2024). Loki documentation. Available at: https://grafana.com/docs/loki

[9] Fluentd Project (2024). Fluentd documentation. Available at: https://docs.fluentd.org

[10] Google (2024). cAdvisor – Container Advisor. Available at: https://github.com/google/cadvisor

[11] Portainer.io (2024). Portainer documentation. Available at: https://docs.portainer.io

[12] Cockpit Project (2024). Cockpit documentation. Available at: https://cockpit-project.org/documentation.html

[13] MITRE (2024). MITRE ATT&CK Framework. Available at: https://attack.mitre.org

[14] Centro Criptológico Nacional (2022). Esquema Nacional de Seguridad (ENS) – Nivel Alto, RD 311/2022. Available at: https://www.ccn-cert.cni.es