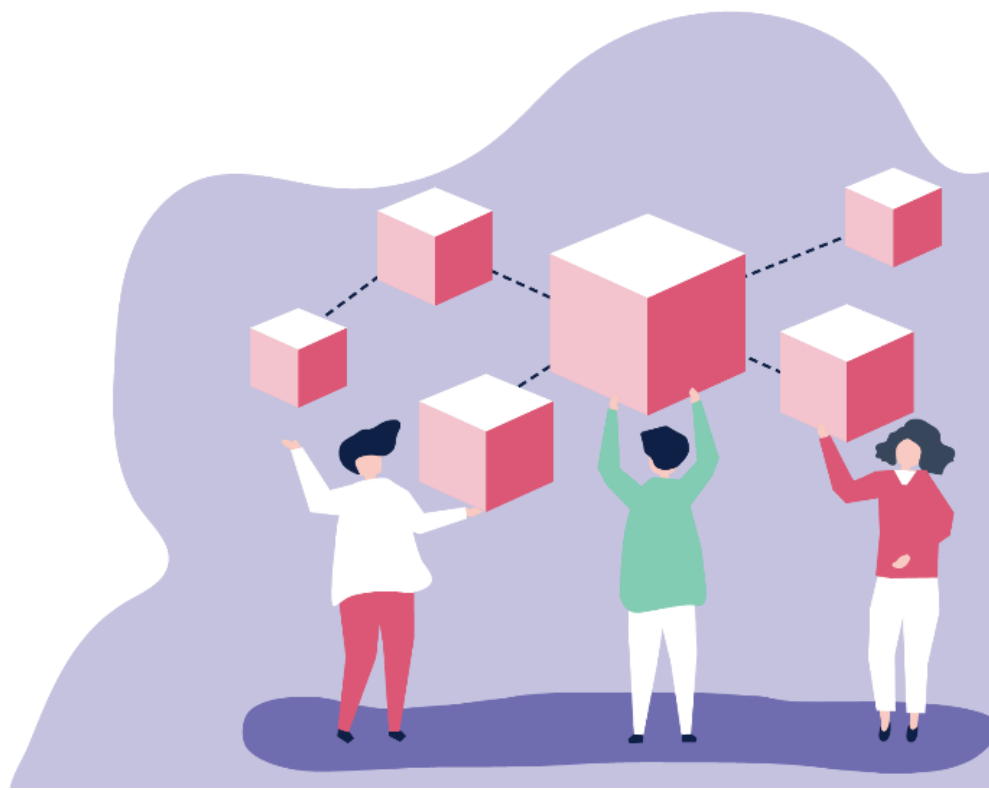




## D4.7 Microservices Containerization & Deployment

Deliverable No.	D4.7	Due Date	31/03/2022
Description	Microservices Containerization & Deployment		
Type	Other	Dissemination Level	PU
Work Package No.	WP4	Work Package Title	GATEKEEPER Things Management Infrastructure & Development
Version	1.0	Status	Final





## Authors

Name and surname	Partner name	e-mail
Claudio Caimi	HPE	<a href="mailto:claudio.caimi@hpe.com">claudio.caimi@hpe.com</a>
Mirko Manea	HPE	<a href="mailto:mirko.manea@hpe.com">mirko.manea@hpe.com</a>
Giovanni Saponara	HPE	<a href="mailto:giovanni.saponara@hpe.com">giovanni.saponara@hpe.com</a>
Mario Bartolucci	HPE	<a href="mailto:mario.bartolucci@hpe.com">mario.bartolucci@hpe.com</a>
Fausto Peverelli	HPE	<a href="mailto:fausto.peverelli@hpe.com">fausto.peverelli@hpe.com</a>
Patrizia Ciampoli	HPE	<a href="mailto:patrizia.ciampoli@hpe.com">patrizia.ciampoli@hpe.com</a>

## History

Date	Version	Change
01/20/2022	0.1	Table of content and initial content
02/02/2022	0.2	Revision of ToC and contributions
02/21/2022	0.3	Integration of content up to the date
02/28/2022	0.4	Integration of 1 <sup>st</sup> round of contributions
03/10/2022	0.5	Integration of contributions
18/03/2022	0.6	Incorporated comments from internal reviewers
21/03/2022	1.0	Revision of content after quality review

## Key data

<b>Keywords</b>	Data Centre Infrastructure
<b>Lead Editor</b>	<i>See Authors</i> (HPE)
<b>Internal Reviewer(s)</b>	Carlo Allocca (SAM), Alessio Antonini (OU)

## Abstract

This deliverable is the second version of D4.1 and contains a description of the GATEKEEPER Infrastructure that is currently hosting the GATEKEEPER Platform and the execution of the Pilots projects.

It describes the status of the setup of the Cloud Services of the GATEKEEPER Data Centre, their technical and organizational security measures, the Continuous Integration and Continuous Deployment setup, the Containerization platform, and the Ticketing Support System.

The GATEKEEPER Infrastructure is continuously updated and user manuals are provided to the users to allow the optimal exploit of the provided resources. A new updated and final version of this document is expected at M40, describing the final version of the infrastructure.

This deliverable accompanies the release of the actual hardware and software release of cloud service infrastructure for the GATEKEEPER platform.

## Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

# Acronyms

Table 1 – List of acronyms

Acronym	Description
2FA	Two-Factor-Authentication
CA	Certification Authority
CE	Community Edition
CIFS	Common Internet File System
CPE	Common Platform Enumeration
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DoW	Description of Work, i.e. the GATEKEEPER proposal document
DC	Data Centre
DDI	DNS, DHCP, and IPAM
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
GK	GATEKEEPER
iSCSI	Internet Small Computer Systems Interface
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPAM	IP Address Management
I/O	Input/Output
IT	Information Technology
IRF	Intelligent Resilient Framework
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
NIC	Network Interface Card
OS	Operating System
OSS	Open Source Software
OWASP	Open Web Application Security Project

PKI	Public Key Infrastructure
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
SCA	Software Composition Analysis
SMTP	Simple Mail Transfer Protocol
ToC	Table of Content
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VTL	Virtual Tape Library

# Table of contents

<b>TABLE OF CONTENTS.....</b>	<b>7</b>
<b>LIST OF TABLES .....</b>	<b>8</b>
<b>LIST OF FIGURES .....</b>	<b>9</b>
<b>1 INTRODUCTION.....</b>	<b>10</b>
<b>2 GATEKEEPER DATA CENTRE INFRASTRUCTURE .....</b>	<b>11</b>
2.1 PROVISION AND SETUP OF CLOUD SERVICES .....	11
2.1.1 <i>Data Centre Layout</i> .....	11
2.1.2 <i>Security Organizational Measures</i> .....	13
2.1.3 <i>Security Technical Measures</i> .....	19
2.2 CONTINUOUS INTEGRATION AND CONTINUOUS DELIVERY .....	36
2.2.1 <i>CI/CD Implementation</i> .....	36
2.3 CONTAINERIZATION IMPLEMENTATION.....	40
2.4 SUPPORT AND TICKETING SYSTEM .....	42
<b>3 GATEKEEPER USER MANUALS .....</b>	<b>45</b>
3.1 GATEKEEPER DATA CENTRE INFRASTRUCTURE .....	45
3.1.1 <i>Data Centre Access User Manual</i> .....	45
3.2 CONTINUOUS INTEGRATION AND CONTINUOUS DELIVERY .....	45
<b>4 CONCLUSIONS .....</b>	<b>47</b>
<b>5 REFERENCES .....</b>	<b>48</b>
<b>APPENDIX A ANNEXES.....</b>	<b>50</b>
<b>APPENDIX B USER REGISTRATION FORM TEXT FOR S2S VPNS .....</b>	<b>51</b>
<b>APPENDIX C USER REGISTRATION FORM FIELDS FOR S2S VPNS .....</b>	<b>52</b>
<b>APPENDIX D INTERNAL HPE PORTAL HOME PAGE .....</b>	<b>53</b>

## List of tables

TABLE 1 – LIST OF ACRONYMS .....	5
TABLE 2 – AUTHORIZATION LIST (AS ON MARCH 2022).....	17
TABLE 3 – DPA SECURITY REQUIREMENTS DESCRIPTION .....	18
TABLE 4 – INTEGRATED SOURCES ON SIDECARS.....	22
TABLE 5 – BACKUP STRUCTURE.....	25



## List of figures

FIGURE 1 – DC PHYSICAL LAYOUT (R0=RACK 0, R1=RACK 1) .....	12
FIGURE 2 – DC LOGICAL LAYOUT .....	13
FIGURE 3 – PREFACE OF THE S2S USER REGISTRATION FORM .....	14
FIGURE 4 – FIELDS OF THE S2S USER REGISTRATION FORM .....	15
FIGURE 5 – EXTENDED FIELD FOR OPEN CALLERS USER REGISTRATION FORM .....	16
FIGURE 6 – INTERNAL HPE PORTAL .....	19
FIGURE 7 – LOG MANAGEMENT ARCHITECTURE .....	21
FIGURE 8 – GRAYLOG CUSTOM DASHBOARDS .....	22
FIGURE 9 – AUTHENTICATION DASHBOARD .....	23
FIGURE 10 – CI/CD MANAGEMENT DASHBOARD .....	23
FIGURE 11 – BRUTE FORCE ATTACK DETECTION .....	24
FIGURE 12 – BAREOS DASHBOARD .....	25
FIGURE 13 – BAREOS CONFIGURED CLIENTS .....	26
FIGURE 14 – BAREOS STORAGE VTL .....	26
FIGURE 15 – BAREOS RESTORE .....	27
FIGURE 16 – HPE STOREONCE DASHBOARD .....	29
FIGURE 17 – BACKUP PERFORMANCE EVALUATION .....	29
FIGURE 18 – MAIN DASHBOARD .....	30
FIGURE 19 – ALL-HOSTS DASHBOARD .....	31
FIGURE 20 – NEXUS REPOSITORY .....	38
FIGURE 11 – JENKINS INFRASTRUCTURE .....	38
FIGURE 22 – GATEKEEPER CI/CD PIPELINES DIAGRAM .....	38
FIGURE 23 – STAGES OF THE BUILD PIPELINE .....	39
FIGURE 24 – STAGES OF THE DEPLOY PIPELINE .....	39
FIGURE 25 – STAGES OF THE SECURITY PIPELINE .....	40
FIGURE 26 – SEGREGATION FOR GATEKEEPER PILOTS .....	40
FIGURE 27 – LIST OF GATEKEEPER PILOTS PROJECTS (TENANTS) .....	41
FIGURE 28 – SAMPLE PROJECT WITH AVAILABLE COMPONENTS .....	42
FIGURE 29 – SUPPORT PROJECTS' LABELS .....	43
FIGURE 30 – ISSUE BOARDS .....	44
FIGURE 31 – ISSUE TEMPLATE PROTOTYPE .....	44
FIGURE 32 – GATEKEEPER-WP4-GK_DATA_CENTRE_ACCESS_SITE_To_SITE_HPE DOCUMENT TOC .....	45
FIGURE 33 – AGENDA HPE CI/CD WEBINAR .....	46

# 1 Introduction

This deliverable is the second version of D4.1 and contains the updates, improvements and novelties that have been implemented until M30 of the GATEKEEPER project execution, under the WP4 activities umbrella (in particular T4.1).

It defines the current GATEKEEPER Infrastructure architecture with the components and services that build the HPE GK Data Centre for GATEKEEPER.

The GATEKEEPER Infrastructure at the time of this deliverable (M30) has greatly matured with respect to the previous reporting period (M18) and it is currently satisfying the needs of the GATEKEEPER Pilot's projects at production level as its main target objective.

With respect to T4.1 objective of "*provision and setup of high-performance cloud services*", the GATEKEEPER Infrastructure is now hosting 15 Pilot's projects (as independent tenants), as well as a development, a testing and a general production environment.

Both the Pilot's projects tenants and the developers' tenants are hosted on the OpenShift/OKD Kubernetes environment ("*the containers clustering techniques and orchestration mechanisms*") and are deployed thanks to the "*definition of the continuous integration and continuous delivery pipelines*" which has been fully implemented and is daily used by the GATEKEEPER developers' team. Each tenant hosts part or all of the GATEKEEPER core components defined in T4.2 (Thing Management System), T4.4 (Data Federation Framework), T4.5 (GATEKEEPER Trust Authority), depending on the specific Pilot needs and requirements.

Specific activities are also in progress with respect to the integration of T4.1 and T4.3 (about Big Data Services), where T4.1 data from tenants will be integrated with the Big Data platform for AI modelling. These will be reported on the next version of D4.3 which is expected at M36.

The T4.1 task results have been organized following the structure described below:

**Section 1** – this introduction.

**Section 2** – focuses on describing the Data Centre setup, with the provided tools and services.

**Section 3** - reports the user manuals useful for the GATEKEEPER partners to access and work with the Data Centre tools and services.

**Section 4** - shows the conclusions and future work.

**Section 5** - is the bibliography.

Finally, **Appendices** show the collateral material (annexes) and additional information.

## 2 GATEKEEPER Data Centre Infrastructure

This document describes the GATEKEEPER Infrastructure setup at HPE Data Centre for GATEKEEPER. The infrastructure runs the GATEKEEPER Platform as a show case of the project-developed functionalities and provides the environment for the execution of the GATEKEEPER Pilots.

The Data Centre and the associated equipment are dedicated to the GATEKEEPER project and are configured following the project requirements as well as the applicable regulations and HPE policies, as you can see from the sections related to the technical and organizational security measures.

All hardware equipment is composed by devices manufactured by Hewlett Packard Enterprise (HPE) group. We are in the progress of extending the hardware devices to introduce enhanced computing capabilities for Artificial Intelligence/Machine Learning, as demanded by the AI/ML requirements of GATEKEEPER partners. This will result in the addition of new servers and Graphical Processing Units (GPUs) specifically optimized to address such need.

We follow the same road described in D4.1, where mostly Open Source software is used along with HPE-branded software for *infrastructure management*, *network* and *storage devices*, and *big data services*. As of now, the experience with Open Source software has demonstrated to be very positive and we consider very high the level of maturity of the selected tools (e.g., OKD for Kubernetes, oVirt for virtualization, etc. - more in the next sections). Both Open Source tools and HPE hardware/software are operated by a team of highly-skilled HPE professionals that has an extensive experience from the field in the different required sectors.

The choice of both hardware equipment and software tools have been a trade-off between security and reliability of advanced hardware technologies (commercial off-the-shelf HPE products), the associated costs, and the openness of the software services.

### 2.1 Provision and Setup of Cloud Services

This section describes updates to the provision and the setup of the Cloud Services offered to the GATEKEEPER project by HPE partner hosted at its Italian premises.

#### 2.1.1 Data Centre Layout

In this section we describe the updated configuration of the Infrastructure, where the GATEKEEPER resources reside. Please refer to D4.1 for all the other details.

Mainly we are going to add 2 new Synergy servers to the Compute Block with GPU support to enhance the computation of AI/ML algorithms for both training and inference needs. These design for these new servers plans to extend the oVirt virtualization cluster to both add new computing capabilities (CPU and RAM), exploit the GPU processing power and reserve it for HPE Ezmeral Big Data and Machine Learning service (part of T4.3).

### 2.1.1.1 Physical and Logical layout

The updated Physical Layout of the DC is represented in the Figure 1 diagram:

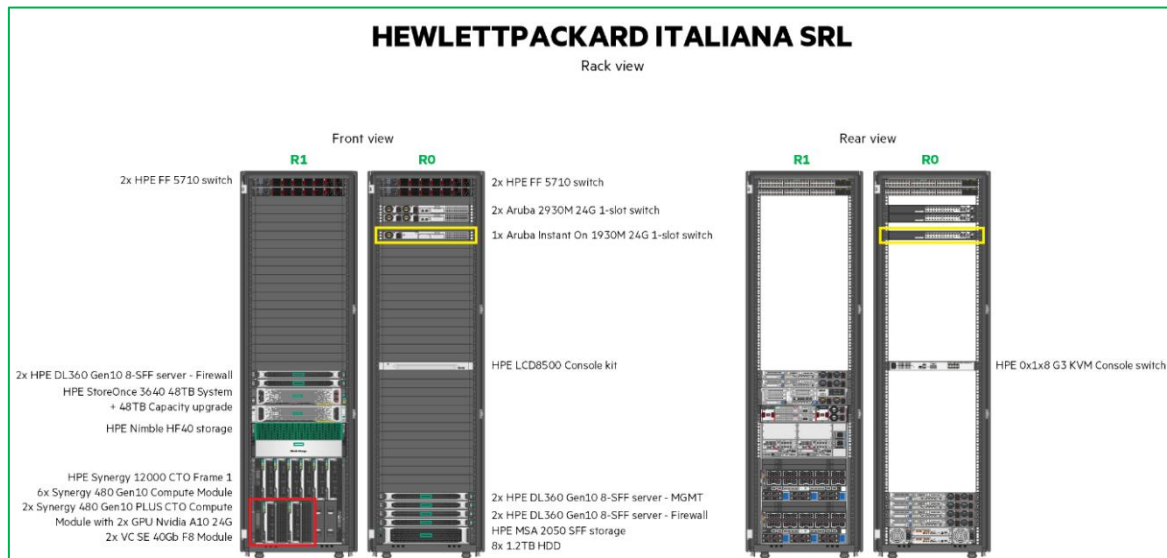


Figure 1 – DC Physical Layout (R0=Rack 0, R1=Rack 1)

As you can see in Figure 1, there are two Racks shown both in front and rear view. With respect to D4.1, we added a new low end switch to connect to Uninterruptible Power Supply (UPS) monitoring card (boxed in yellow). In this way we are able to assess the UPS health and when UPS goes to battery mode from the GATEKEEPER Monitoring System (see 2.1.3.4). Also the schema has been already updated to host two new computing node with GPUs (boxed in red, which will be available starting from April/May 2022).

Figure 2 shows the Logical Layout where you can see on the right side Service Block components, that host general Data Centre services, and on the left side the GATEKEEPER Block components (Compute and Storage Blocks). With respect to D4.1, we added the UPS and UPS switch connection, and prepared the design for Bay #7-#10 that will host new computing nodes with Graphical Processing Units (GPUs), that will be used to speed up ML training and inference algorithms.

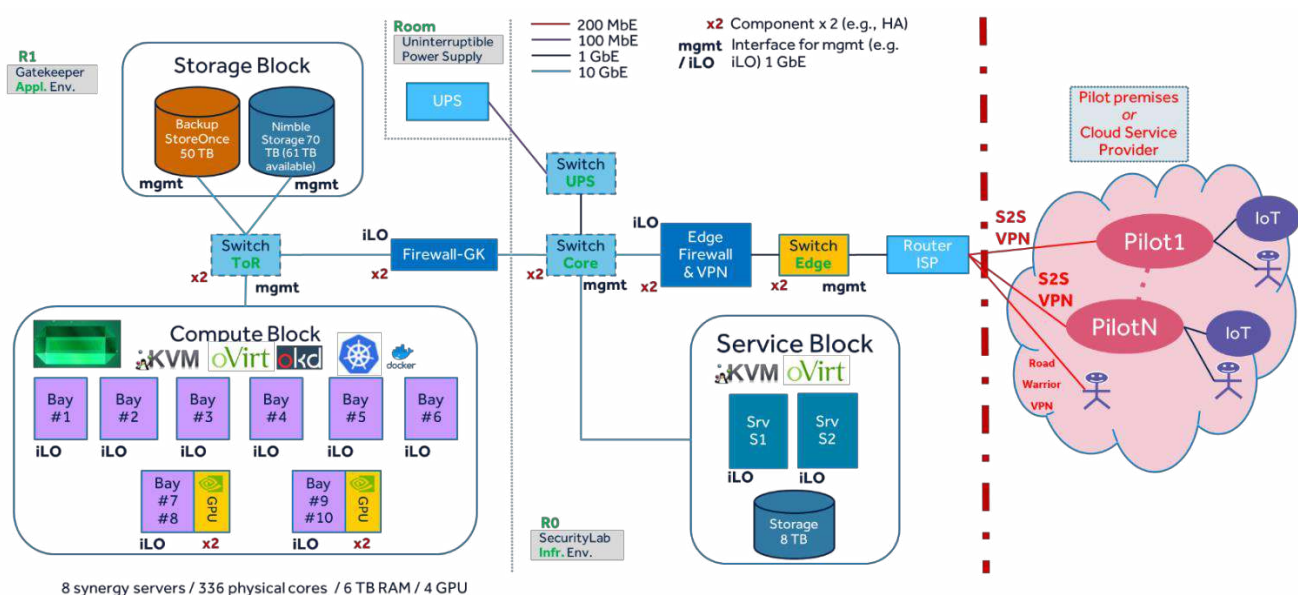


Figure 2 – DC Logical Layout

## 2.1.2 Security Organizational Measures

In D4.1 we discussed the security and organization measures for controlling the Data Centre, in particular related to physical access and roles definition. Here we update to describe how we manage the new scenarios coming from Project Pilots' requirements related to **site-to-site (S2S) connections** and the addition to the **open callers** as new actors in the GATEKEEPER project. Also we describe the impacts of the Data Processing Agreement (DPA) that is currently being established as a legal basis for the proper Pilot execution.

### 2.1.2.1 User Registration Process for S2S VPN

In addition to the VPN services the Data Centre already provides for users (called **road warrior VPN**), the GATEKEEPER Infrastructure has been extended to provide also the functionality to establish a secure encrypted channel for machine-to-machine interaction between a Pilot service and the Data Centre. We call this channel a **Site-to-Site VPN** and is used by those Pilots that have their own hardware/software infrastructure to connect to the HPE-operated Data Centre.

For those Pilots requiring to obtain an access to setup a direct VPN connection from the Pilot's site to the HPE GK Data Centre, it has been defined a process of request, validation and provision called user registration for S2S VPNs. Process includes de-provision in case of revocation of user access.

Users' accounts are of these kinds:

- GATEKEEPER Pilots for S2S VPN;
- Open Callers.

**Note:** for the specificities regarding the declination of this process for HPE Administrators and GATEKEEPER partner users, see D4.1, Section 1.1.2.2.

Request for user registration to S2S VPN is made by partners filing a registration form. HPE validates the form and then proceeds with the creation of the S2S VPN on HPE GK Data Centre, including credentials and S2S VPN configuration.

Figure 3 shows the preface of the S2S registration form, where the person is informed about the rules of HPE Data Centre access and the Privacy statements (form and text has been approved by HPE Legal Office):





# GATEKEEPER

## HPE Data Centre **Site-To-Site**

### Remote Access Request

Please complete the following form. Your data will be collected by HPE as GATEKEEPER partner for the sole purposes of account management and user access provisioning to HPE Data Centre infrastructure hosting the GATEKEEPER project services. You must give your consent to HPE for processing your data according to the HPE Privacy policy available using the link located at the bottom of the form. The HPE responsibilities are described in the link.

This computer network is provided for authorised use only. Users have no explicit or implicit expectation of privacy. Any or all uses of systems of this computer network and all data in this Data Centre may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised sites and law enforcement personnel, as well as authorised officials of other agencies. By accessing to this computer network, the user consent to such disclosure at the discretion of authorised site personnel. Unauthorised or improper use of this network may result in administrative disciplinary action, civil and criminal penalties. By accessing to this computer network, you indicate your awareness of and consent to these terms and conditions of use. Users are responsible for ensuring that they act in accordance with this policy and other policies and legislation applicable to the HPE network.

Please note that by submitting this form you also agree to have your activities on HPE Data Centre monitored for compliance and security purposes. You must not disable (or attempt to) or change any security control, as well as respect the assigned privileges and not escape the perimeter of your role.

Should you have any inquiry please contact HPE project partner for further information.

Technical details about how to access HPE Data Centre services are published on Alfresco project document management system. You will receive an email as soon as your access will be granted with more information.

Notice: it is strictly forbidden to share this registration link outside involved GATEKEEPER project partners.

HPE GATEKEEPER Team

---

<https://www.gatekeeper-project.eu/>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 857223

Figure 3 – Preface of the S2S User Registration Form

For the sake of readability and accessibility, the full text is reported in Appendix B.

Figure 4 shows the data collection form fields:

\* Required

1. Partner Single Point of Contact - First Name \*

*Please insert your name and optional middle name*

Enter your answer

2. Partner Single Point of Contact - Surname \*

*Please insert your surname*

Enter your answer

3. Partner Single Point of Contact - E-Mail Address \*

Please specify the contact e-mail address (e.g., [user@example.org](mailto:user@example.org)). This e-mail address will be used only for communications about HPE data centre and site-to-site connection. Only valid GATEKEEPER partner e-mail address will be accepted.

Enter your answer

4. Organisation Name \*

*Please specify your organisation:*

Select your answer

5. I have read and I accept the HPE Privacy policy for personal data collection available at the URL:

[https://www.hpe.com/emea\\_europe/en/legal/privacy.html](https://www.hpe.com/emea_europe/en/legal/privacy.html) \*

☐ Yes

You can print a copy of your answer after you submit

Submit

Figure 4 – Fields of the S2S User Registration Form

For the sake of readability and accessibility, the full text of the form is reported in Appendix C.

### 2.1.2.2 User Registration Process for Open Callers

In order to give Open Callers (OCs) access to HPE infrastructure a process of request, validation and provision of a user registration has been defined. Each OC has been assigned to a specific GATEKEEPER partner, taking the role of **Mentor** of the Open Caller. A request for user registration to GATEKEEPER Data Centre services is made by OCs filing a registration form. HPE representative validates the form and asks, with an email, confirmation by the responsible OC Mentor. After approval by the Mentor, HPE proceeds with the creation of the user account for the specific user's role.

The registration form for Open Callers is the same as for GATEKEEPER partner users that has been extended to show the choices of the Open Caller participating organizations. The form fields and screenshots are available in D4.1, Section 1.1.2.2. In particular, field #4 (Organisation Name) now lists also the Open Callers are available organizations.

#### 4. Organisation Name \*

*Please specify your organisation:*



Figure 5 – Extended field for Open Callers User Registration form

### 2.1.2.3 Pilots authorisation for partners

Pilots have to authorise the partners that will need to access their tenant (including their data) for performing administrative tasks, such as GATEKEEPER platform installation and management, or are the technological system integrators for a Pilot business partner (i.e., an hospital that leverages the services of a partners).

The activities in the GATEKEEPER LSP Cluster working group have designed a document related to the **Criteria for pilot qualification** (Toolkit) in which several information has been gathered and shared from and among all partners. In consequence a table has been created to collect authorizations decisions where Pilots' partners grant access to one or more of their available GATEKEEPER Pilot-dedicated services. In particular, the access can be granted to:

- **GATEKEEPER Platform Pilot Tenant:** this grants a partner the access rights to the dedicated tenant of the Pilot on the OKD platform. It is where the GATEKEEPER Platform instance for the Pilot is running (includes the collected data);
- **Big Data Analytics/AI/ML Pilot Tenant:** this grants a partner the access rights to the Pilot Tenant on the Big Data platform (HPE Ezmeral). It is where the AI/ML programs and algorithms are developed and models are trained (includes the collected data).

The process flow is that every Pilot elects a responsible person who authorizes partners willing to grant access to Pilot data, then send the information to HPE which updates the table and perform the technical configurations.



Table 2 illustrates the information about which GK partner is supporting which Pilot(s).

Pilot name	Partner Name	Partner access to: GK Platform Pilot Tenant (OKD/Openshift)	Partner access to: Big Data Analytics/AI/ML Pilot Tenant (Ezmeral)
Puglia	ENG	TRUE	TRUE
Puglia	UPM	TRUE	FALSE
Puglia	UOI	FALSE	TRUE
Puglia	SAMSUNG	TRUE	TRUE
Puglia	CSS	TRUE	TRUE
BANGOR	SAMSUNG	TRUE	TRUE
BANGOR	UoW	TRUE	TRUE
BANGOR	UOI	TRUE	TRUE
BANGOR	OU	TRUE	TRUE
Milton Keynes (UK)	SAMSUNG	TRUE	TRUE
Milton Keynes (UK)	SPIROCCO	TRUE	FALSE
Milton Keynes (UK)	OU	TRUE	TRUE
Greece UC #a	CERTH	TRUE	TRUE
Greece UC #a	UPAT	FALSE	TRUE
Greece UC #a	UOI	FALSE	TRUE
Greece UC #a	BIO	TRUE	TRUE
Greece UC #b	CERTH	TRUE	TRUE
Greece UC #b	UOI	FALSE	TRUE
Greece UC #b	UPAT	FALSE	TRUE
Greece UC #b	BIO	TRUE	TRUE
Cyprus UC #a	CERTH	TRUE	TRUE
Cyprus UC #a	UOI	FALSE	TRUE
Cyprus UC #a	UoW	FALSE	TRUE
Cyprus UC #b	CERTH	TRUE	TRUE
Cyprus UC #b	UoW	FALSE	TRUE
Cyprus UC #b	UOI	FALSE	TRUE
Saxony	TUD	TRUE	TRUE
Saxony	CCS	FALSE	FALSE
Saxony	SAMSUNG	TRUE	TRUE
Basque Country	SAMSUNG	TRUE	TRUE
Basque Country	MyS	TRUE	TRUE
Basque Country	TECNALIA	TRUE	TRUE
Basque Country	OSA	TRUE	TRUE
Basque Country	S4C	TRUE	TRUE
Basque Country	IBERMATICA	TRUE	TRUE
Basque Country	BB	TRUE	TRUE
Basque Country	UPM	TRUE	TRUE
Basque Country	KRONIKGUNE	TRUE	TRUE
Covid-19	UPAT	TRUE	TRUE
Aragon	UPM	TRUE	FALSE
Aragon	ENG	TRUE	TRUE
Aragon	UOI	TRUE	TRUE
Poland	UMED	TRUE	TRUE

Table 2 – Authorization list (as on March 2022)

#### 2.1.2.4 Data Processing Agreement (DPA)

Under the terms of GDPR [34], a data processing agreement is a legally binding contract that states the rights and obligations of each party concerning the protection of personal data. It is described in Article 28 of the GDPR. The GATEKEEPER project, in particular the Pilots projects, collect personal data as described as reported in the DoW. With respect to WP4 and T4.1 in particular, HPE owns the Data Centre where (part of) the data collected from the Pilots are sent for being used by the GATEKEEPER Platform services. It is worth mentioning here that the DoW explains that personal data will be (pseudo-)anonymised before being sent to the Data Centre services.

Nevertheless, HPE takes the role of data processor, while the Pilots are the data controller under the terms of GDPR.

The reader will find more legal details in WP6 deliverables, in this section we concentrate on the HPE security measures (both organizational and technical) for the GATEKEEPER Infrastructure with respect to the DPA document that is currently being finalised.

Table 3 – DPA security requirements description

Section5 Security	- Description
5.1	D4.1 and D4.7 contain the list of physical (D4.1 Section 2.1.2.2), technical and organizational measures (respectively Sections 2.1.2 and 2.1.3) put in place to safeguard collected personal data. Also Pilot isolation measures have been defined in Section 2.3.
5.2	D4.7 contains updated and enhanced security measures with respect to D4.1, and the same will be true for the final version of these documents (D4.8 at M40). In this way, we plan to follow the security evolution of threats and adopt new or updated measures as needed.
5.3	We follow a patch management process that apply as soon as possible the security patches to operating systems, devices and other infrastructure software components. HPE also collects logging information for security and compliance purposes as explained in Section 2.1.3.2.
5.4	People in the HPE group follow periodic and mandatory cybersecurity trainings to improve their skills and react to new threats, as well as to understand how to deal with data privacy aspects.
5.5	The HPE Project Team set up a notification process to follow whenever it is recognised a disruption of the service, loss of data, data breach, etc. Notification is sent to the dedicated HPE Data Centre registered users mailing list or Pilot owner (if it is a disruption related to Pilot only). Registered users and Pilot owners are available as part of processes described in Sections 2.1.2.1, 2.1.2.2, 2.1.2.3 of this deliverable, and also Section 2.1.2.2 of D4.1.

### 2.1.2.5 User Data Centre Landing Page

The internal HPE Portal has been updated respect to the previous version in D4.1 by adding services for HPE Ezmeral Console for Big Data, Artificial Intelligence and Machine Learning. Furthermore it has been provided the access for the configured CI/CD tools such as GitLab, Nexus and Jenkins.

(Note: some content has been removed due to its security sensitiveness and links are available only internally).

**HPE SECLAB**

This page provides helpful links for HPE SECLAB made for [GATEKEEPER](#).

**Identity Management**  
Go here to manage your user account.  
Access Password Change: [https://](#)  
You can change your password or reset it if it expires.

**SECLAB Internal Certification Authority**  
Import the HPE SECLAB into your browser or other services. Download the SECLAB Internal CA to trust the provided services: [hpe-seclab-ca.crt](#)

**For Developers**  
Tools provided for authorised developers only.  
Access OKD Console: [https://](#)  
OKD is a distribution of Kubernetes optimized for continuous application development and multi-tenant deployment.

Access HPE Ezmeral Console for Big Data/AI/ML: [https://](#)  
HPE Software platform designed to run both cloud-native and non-cloud native applications in containers. More [info](#).

Access CI/CD Tools

GitLab: <a href="#">https://</a>	- source code repository
Nexus: <a href="#">https://</a>	- container registry
Jenkins: <a href="#">https://</a>	- build and deploy automation server

Tools to enable project software development.

**Important notice**  
This computer network is provided for authorised use only. Users have no explicit or implicit expectation of privacy. Any or all uses of systems of this computer network and all data in this Data Centre may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised sites and law enforcement personnel, as well as authorised officials of other agencies. By accessing to this computer network, the user consent to such disclosure at the discretion of authorised site personnel. Unauthorised or improper use of this network may result in administrative disciplinary action, civil and criminal penalties. By accessing to this computer network, you indicate your awareness of and consent to these terms and conditions of use. Users are responsible for ensuring that they act in accordance with this policy and other policies and legislation applicable to the HPE network.

**About this Project**  
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857223

**GATEKEEPER** **Hewlett Packard Enterprise**

(c) Copyright 2021 Hewlett Packard Enterprise Development Company, L.P. Valid agreement required.

Figure 6 – Internal HPE Portal

For the sake of readability and accessibility, the full text of Figure 6 is reported in Appendix D.

### 2.1.3 Security Technical Measures

Several technical security measures have been improved with respect to D4.1 to protect the Data Centre infrastructure where the GATEKEEPER Platform runs. This process is still ongoing, because these measures are frequently assessed, refined and improved over time, as the global security landscape evolves.

**Note:** several technical details are not included in this document, because of the sensitivity of such security information. This is mainly due to the Public scope of this document (i.e., Dissemination Level = PU), as specified in the DoW.

In particular:

- **Secure Access:** in addition to user VPN connections handling (i.e., road warrior VPN) reported in D4.1, we extended the VPN service to support site-to-site (S2S) connections for pilots and open callers (for more see Section 2.1.3.1);
- **Identity Management:** we are using successfully the tools implemented in D4.1 and we are managing over 150 user accounts at the time of this deliverable. Users have been enrolled by following the organizational process described in Section 2.1.2, as well as Section 1.1.2 of D4.1;
- **Log Management:** several new log sources have been integrated to support security and compliance needs (for more see Section 2.1.3.2);
- **Backup:** keeping safe copy of installed services, components, and data are crucial for the resiliency of the GATEKEEPER Infrastructure and safeguard against human errors and malicious cyberattacks (see Section 2.1.3.3);
- **Monitoring:** having the thermometer of functioning hardware equipment is important to plan support activities, discover broken components, monitoring the most critical software services. This is part of the effort to provide a high degree of resiliency to the delivered Data Centre services.

### 2.1.3.1 Secure Access for Pilots and Open Callers

Access to HPE Data Centre for GATEKEEPER can happen only via secured an encrypted VPN connections. As described in D4.1, users (e.g., GATEKEEPER developers, GATEKEEPER data scientists, etc.) need to use a VPN client and authenticate via a Multi-Factor Authentication (user/password + one-time passcode).

In addition to this methods, we had the need to enable machine-to-machine VPN connection (as described in Section 2.1.2.1). This allows a server (e.g., at Pilot premises) to connect via a VPN connection to the HPE Data Centre and then use the GATEKEEPER Platform services. It still uses a Multi-Factor Authentication, now based on user/password and digital certificates.

A detailed how-to guide to setup S2S VPN has been delivered to Consortium partners (see Appendix A), describing step-by-step the procedure to follow under several operating systems for servers (Ubuntu Linux, CentOS, AWS Linux).

At firewall level, the S2S VPN connections can connect only to the services where the GATEKEEPER Platform can be installed and operated, guaranteeing a level of segregation with the rest of the Data Centre services.

### 2.1.3.2 Log Management

The term Log Management identifies the processes of generation, transformation, storage and analysis of logs. In particular, our attention is focused more on security logs. The benefits of implementing such a solution are manifold. First you make sure you keep security logs for an appropriate period of time. Moreover, thanks to Log Management it is possible to review and analyse events in order to identify security incidents, violation of internal policies, fraudulent activity and operational problems.

The previous deliverable D4.1 illustrated the Open Source Graylog as a tool for Log Management services. Figure 7 shows the high-level architecture based on Graylog components that has been implemented:

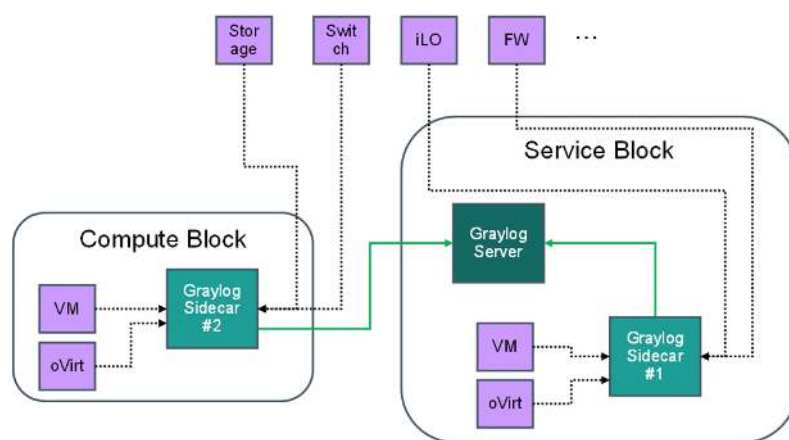


Figure 7 – Log Management Architecture

The implemented solution is made up of three main components (in green), one master node named “Graylog Server” (dark green) and two worker nodes named “Graylog Sidecars” (light green).

The master node represents the core of the architecture from which the orchestration of the other components is based. It is mainly used for operations such as creating or deleting an index on the log database, managing log services, performing queries, and creating dashboards. On the other hand, *sidecars* are a lightweight systems that allows for centralized and stackable configuration, utilizing a log collection agent.

In our case we implemented two *sidecars* following a “proximity” concept:

- **A Service Block sidecar (Graylog Sidecar #1):** to collect logs from all the devices present on the Service Block zone of the infrastructure;
- **A Compute Block sidecar (Graylog Sidecar #2):** to collect logs from devices running on the Compute Block zone of the infrastructure.

The Service and Compute Block are two logical zone (see D4.1) that group general services and for Access/Security/Network/Services management and specific Project block that includes also mass storage services. These blocks are physically grouped in terms of servers and racks. Having a sidecar in each zone implements the “proximity” concept, which allows log collection nearest to log generation and advanced mechanisms like bandwidth optimization, data channel encryption, and queuing mechanism to improve resiliency in case of “Graylog Server” downtime.

The following table shows in detail the split of all sources belonging to the GATEKEEPER project scope. It also give the feeling of the number of difference source types (both physical hardware devices and applications) that have been integrated and from which logs are collected:

Sidecar	Source Device	
<b>Sidecar 1 – Service Block</b>	OPNsense VPN logs	HPE Flex Switch
	Linux OS	HPE iLO
	oVirt	PWDMGMT service



	Nexus YUM/APT repo HPE MSA Bareos	HPE iLO Amplifier FreeIPA Checkmk
<b>Sidecar 2 – Compute Block</b>	OPNsense Access logs Linux OS oVirt GitLab Jenkins	HPE Flex Switch HPE iLO HPE Nimble Nexus GitLab user provisioning tool

Table 4 – Integrated sources on sidecars

The process of integrating a source into Graylog is highly structured and involves the iteration of different configurations.

First of all it is necessary to create an index for storing the received logs from the device. Then create a stream to send events to the index and on the stream create a rule to direct the received device events. The next step is create an input of type beats for the *filebeat* (i.e., the agent collecting events) in order to accept log messages. Then it is necessary to configure the sidecar to make it listen on a chosen receiver port (all collected logs are pushed from the source to the filebeat agents on the sidecars). Last but not least create a pipeline that implements rules to parse the required events. Among all of them, the parsing step is the most important since it allows extracting structured fields from a raw event, that can be later searched and insights can be generated. All these operations can be done easily by accessing the Graylog GUI.

Once the resources have been integrated following the procedure described above, it is important to be able to actively manage, filter and monitor the log events. To do this, in Graylog it is possible to create Dashboards to have clear visualization of your search query results for discovering potential issues and intervening quickly.

In our environment we created two Dashboards, one to keep trace of Authentication events for security purposes and another to monitor CI/CD components:

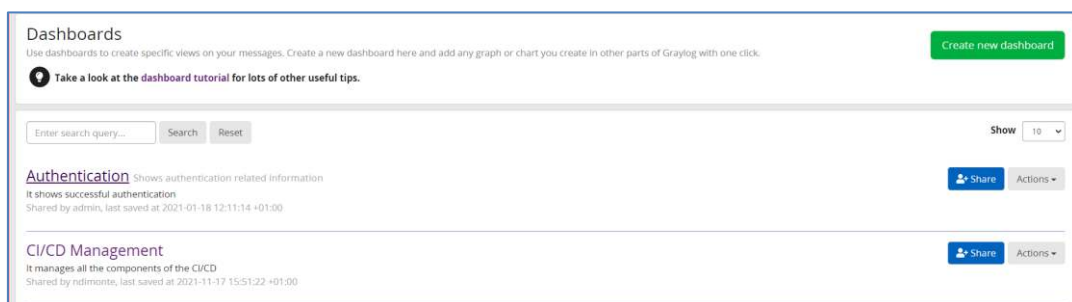


Figure 8 – Graylog custom dashboards

Each dashboard can contain several tabs within it, useful for monitoring specific use cases. Currently on the "Authentication" Dashboard there are three tabs (see Figure 9), but new ones can be added to meet with the continuous project evolutions:

- The first tab "Users Authentication" is used to trace all authentications on every source device in scope;

- The second tab "VPN Users" is focused on users accessing the project VPNs. As shown in the figure it has been added a custom widget with the localization on the map from which the access is done using the IP obtained from the log generated by the VPN;
- The third tab "HPE Portal Password Change" traces the users that have performed the change of the domain password.

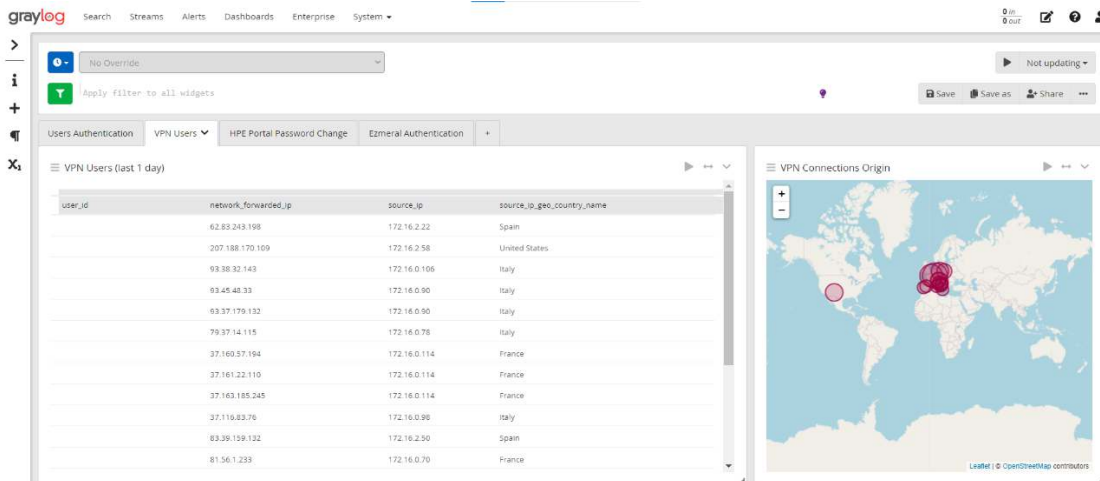


Figure 9 – Authentication Dashboard

On the other Dashboard, "CI/CD Management", at this moment there are five tabs to monitor specific authentications on CI/CD components. We added tabs for GitLab, Nexus and Jenkins authentication. Moreover, for the GitLab component it has been realized a script that synchronizes LDAP users with GitLab users. The result of this script is shown with more attention on the failed user addition on the first two tabs of the figure below. Also in this case widgets are created to help to understand and read the data by giving a more high-level overview.

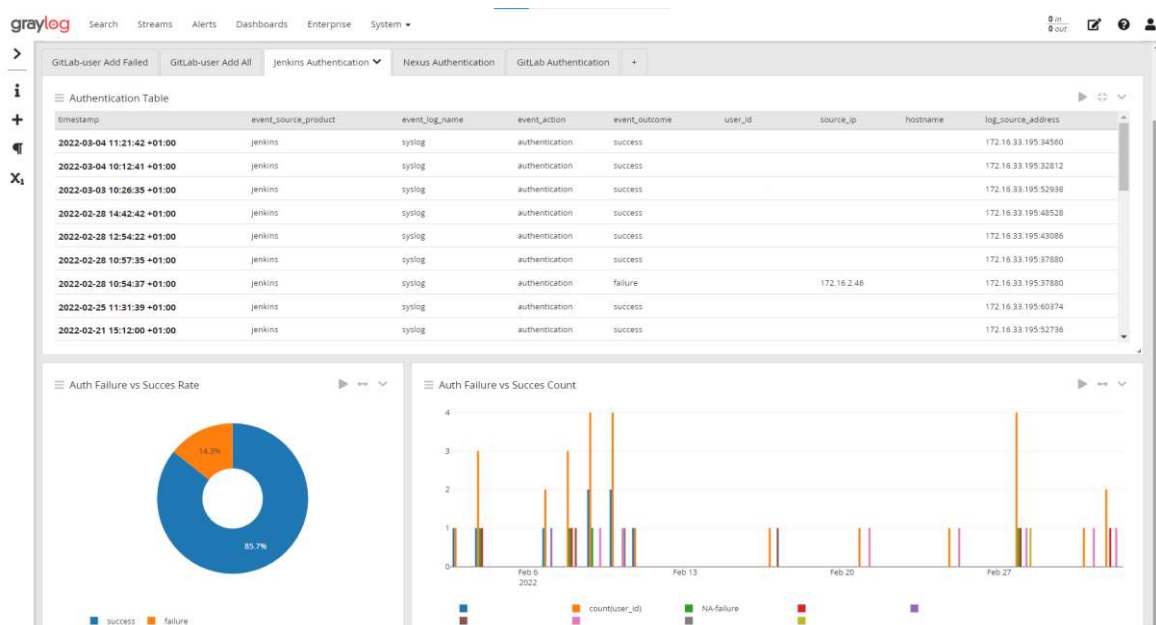


Figure 10 – CI/CD Management Dashboard.

Graylog also gives the possibility to create aggregation rules that are called "Event Definitions" for cyber-attack detections. We created a **brute force rule**<sup>1</sup> based on events with fields that have identical values in a given time range. Going deeper, a filter is applied to the events restricting the analysis only to authentication events with failure outcome. For security reasons, we do not report here further details about how this use case is implemented and configured. When an alert event for this rule is generated, it notifies us of this attack attempt for further investigation.

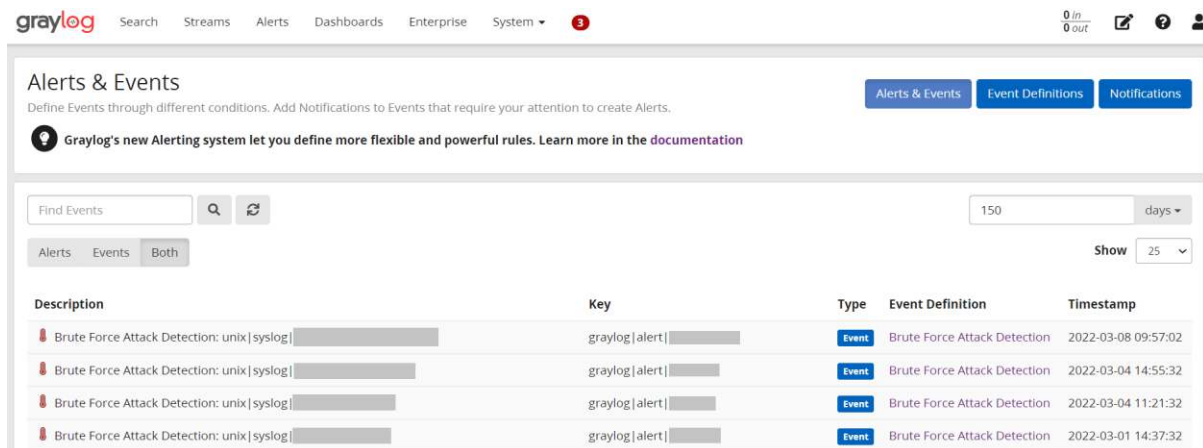


Figure 11 – Brute Force Attack detection

The Log Management service needs to be extended in the next months to be able to recognise others attack patterns from the collected log data.

### 2.1.3.3 Backup

The Backup service is crucial for the resiliency of the whole Data Centre, its services and data. It provides the ability to recover after hardware failures, security incidents, or human mistakes. We started implementing the backup strategy and solution based on the Open Source tool called **Bareos** [16]. This enables to save system files, protect data, assets configuration and others artefacts such in a way it is possible to quickly restore them in case of need. Bareos has currently been integrated with **HPE StoreOnce** solution, to store data files and virtual machines snapshots. Integration with all the Data Centre services is mostly completed and is updated whenever a new service is requested.

Bareos itself is a program tool, Server/Client based, that permits the system administrator to manage backups and restores of virtual machines, disks and files and it supports a lots of Operative Systems and host virtualization Solutions. Bareos can backup to various types of media, including tape and disks.

In this scenario the HPE StoreOnce has been integrated and the same for the oVirt hosts for which a plugin has been implemented to save VMs' snapshots.

HPE StoreOnce offers a set of **CIFS** secure shares (encrypted) by which Bareos creates its volumes to store backups.

<sup>1</sup> A Brute Force Attack is an attempt to gain illegal access to a system by trying to guess the password of a specified user.



In the same time, in order to follow the **3-2-1** implementing backup rule<sup>2</sup>, a **VTL** (Virtual tape Library) has been implemented to store bigger data.

For most of the Virtual Machines a backup policy has been implemented in which a file system backup and Snapshot (via **oVirt Plugin** installed in Bareos) policy has been defined to guarantee a hypothetical restore as granular as possible.

The following Table 5 shows the Backup Structure for the integration of Bareos with the HPE StoreOnce to accommodate both the CIFS (shares) and VTL types of backups:

Table 5 – Backup Structure

Type	Bareos		StoreOnce	
	Path	Use	NAS Shares	VT Libraries
Share (CIFS)	/SHARExx	Production	SHARExx	-
Library Tape	VTL via iSCSI	Production	-	MSL Library

## Bareos

<https://www.bareos.com/>

Here is reported how Bareos **Dashboard** looks like. It allows inspecting the status of the backups with all the details such as start and end time, size, etc.

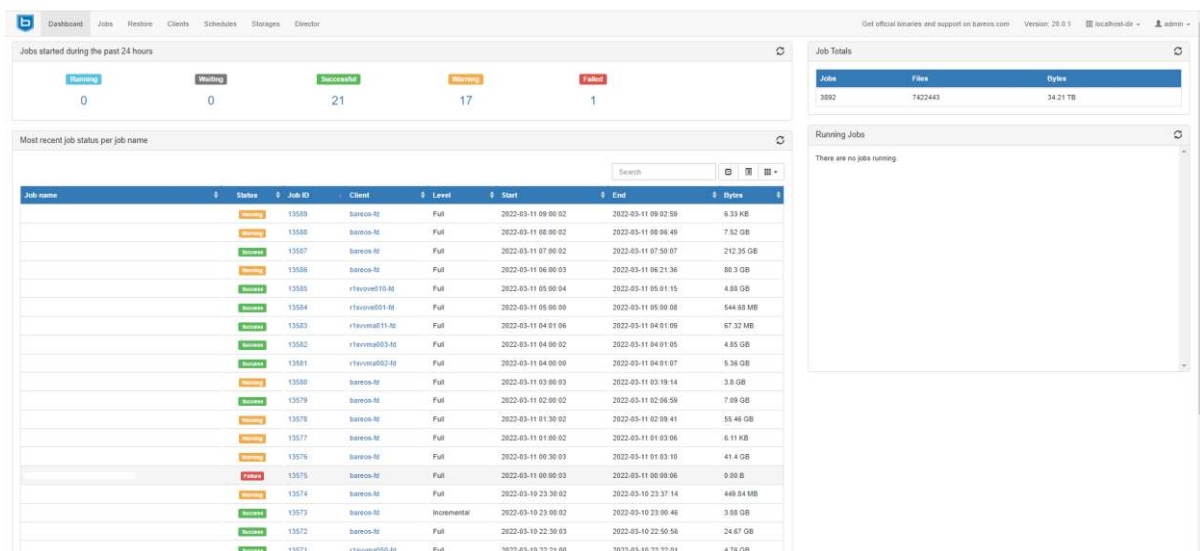


Figure 12 – Bareos Dashboard

<sup>2</sup> [https://en.wikipedia.org/wiki/Backup#3-2-1\\_rule](https://en.wikipedia.org/wiki/Backup#3-2-1_rule)

The next figure shows the configured clients (e.g., servers) that are currently under backup. Names have been hidden for security reasons.

The screenshot shows the Bareos GUI 'Clients' page. It displays a table with columns: Name, OS, Version, Status, and Actions. The table lists 20 clients, all with a status of 'Online'. The names are redacted with 'XXXXXXXXXX'. The OS column shows various operating systems like CentOS, Ubuntu, and Debian. The Version column shows various Bareos versions like 20.0.1, 20.0.2, and 20.0.3. The Actions column contains icons for search, refresh, and delete.

Name	OS	Version	Status	Actions
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]
XXXXXXXXXX	CentOS	20.0.1	Online	[Icons]

Figure 13 – Bareos Configured Clients

Bareos GUI allows to inspect also the status of the Storage Tape VTL, with all the backups that are in the virtual tapes:

The screenshot shows the Bareos GUI 'Storage - Tape' page. It displays a table with columns: Slot, Volume, Bytes, Last written, Expiration, Status, Media Type, Pool, and Actions. The table lists 20 slots, each with a volume name, size, and status. The status column shows various statuses like 'Append', 'Full', and 'Scratch'. The Media Type column shows 'LTO' and 'Scratch'. The Pool column shows 'Full\_Retention\_30' and 'Scratch'. The Actions column contains icons for search, refresh, and delete.

Slot	Volume	Bytes	Last written	Expiration	Status	Media Type	Pool	Actions
1	BEH15A2B	5.07 GB	2021-10-05 12:03:43		Append	LTO	Full_Retention_30	[Icons]
2	BEH15A27	1.69 GB	2021-10-05 12:05:54		Append	LTO	Full_Retention_30	[Icons]
3	BEH15A28	1.6 TB	2022-01-08 08:49:42	2022-02-07 08:49:42	Full	LTO	VTU01-LTO7	[Icons]
4	BEH15A29	1.6 TB	2022-02-12 10:38:50	2022-03-14 10:38:50	Full	LTO	VTU01-LTO7	[Icons]
5	BEH15A2A	1.6 TB	2022-03-20 18:25:22	2022-03-22 18:25:22	Full	LTO	VTU01-LTO7	[Icons]
6	BEH15A2B	1.6 TB	2022-03-05 08:04:37	2022-04-06 08:04:37	Full	LTO	VTU01-LTO7	[Icons]
7	BEH15A2C	1.6 TB	2022-02-08 08:58:06	2022-04-07 08:58:06	Full	LTO	VTU01-LTO7	[Icons]
8	BEH15A2D	1.6 TB	2022-02-06 12:05:33	2022-04-07 13:05:33	Full	LTO	VTU01-LTO7	[Icons]
9	BEH15A2E	1.6 TB	2022-03-06 09:49:30	2022-05-05 10:49:30	Full	LTO	VTU01-LTO7	[Icons]
10	BEH15A2F	870.91 GB	2022-03-06 11:41:54		Append	LTO	VTU01-LTO7	[Icons]
11	BEH15A2G	129.02 KB	2022-03-04 15:33:25		Append	LTO	Full_Retention_7	[Icons]
12	BEH15A2H	64.51 KB			Append	LTO	Scratch	[Icons]
13	BEH15A2I	64.51 KB			Append	LTO	Scratch	[Icons]
14	BEH15A2J	64.51 KB			Append	LTO	Scratch	[Icons]
15	BEH15A2K	64.51 KB			Append	LTO	Scratch	[Icons]
16	BEH15A2L	64.51 KB			Append	LTO	Scratch	[Icons]
17	BEH15A2M	64.51 KB			Append	LTO	Scratch	[Icons]
18	BEH15A2N	64.51 KB			Append	LTO	Scratch	[Icons]
19	BEH15A2O	64.51 KB			Append	LTO	Scratch	[Icons]
20	BEH15A2P	64.51 KB			Append	LTO	Scratch	[Icons]

Figure 14 – Bareos Storage VTL

Bareos finally allows to quickly **restore** an individual file via the GUI, as briefly shown in the following figure:

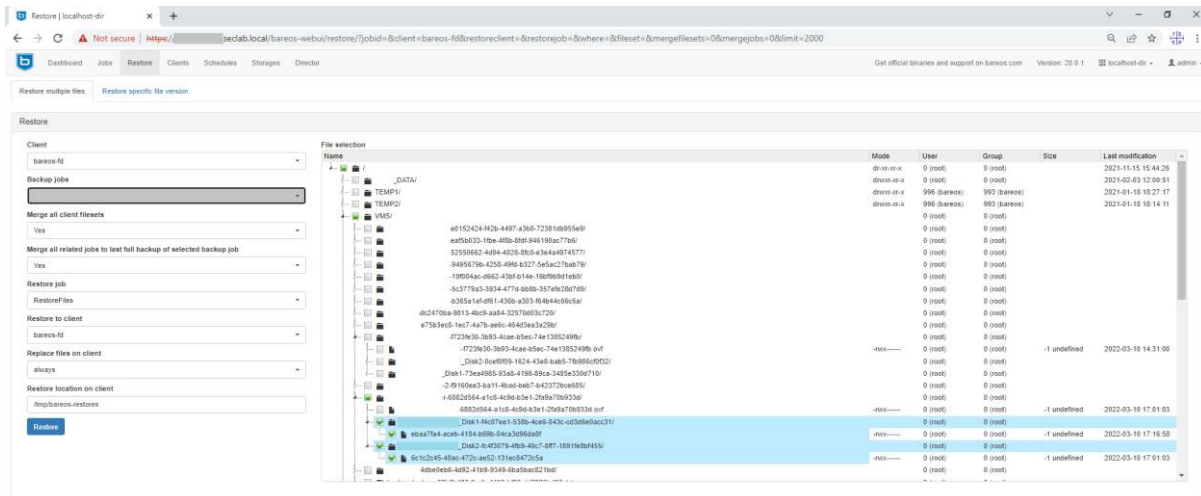
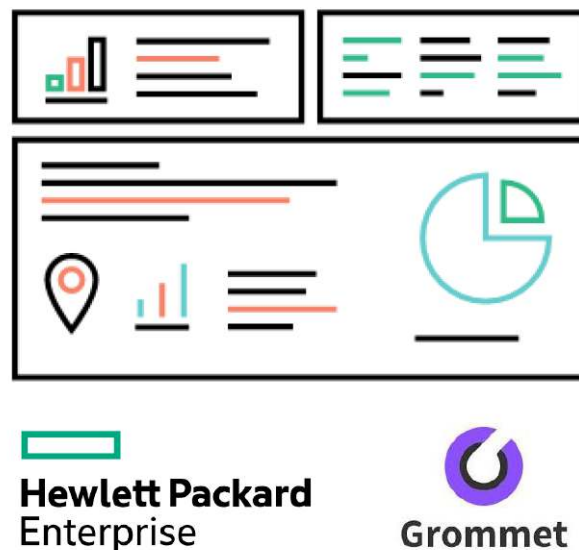


Figure 15 – Bareos Restore

From the GUI you can select the restore of an entire VM or volume or file simply exploring the navigation bar.

## HPE StoreOnce Gen 4








The New StoreOnce GUI (**Grommet**) lets the user have an easy access to all of the library functions as reported below:










<https://www.hpe.com/us/en/insights/articles/getting-to-know-grommet-an-open-source-ui-dev-tool-1808.html>

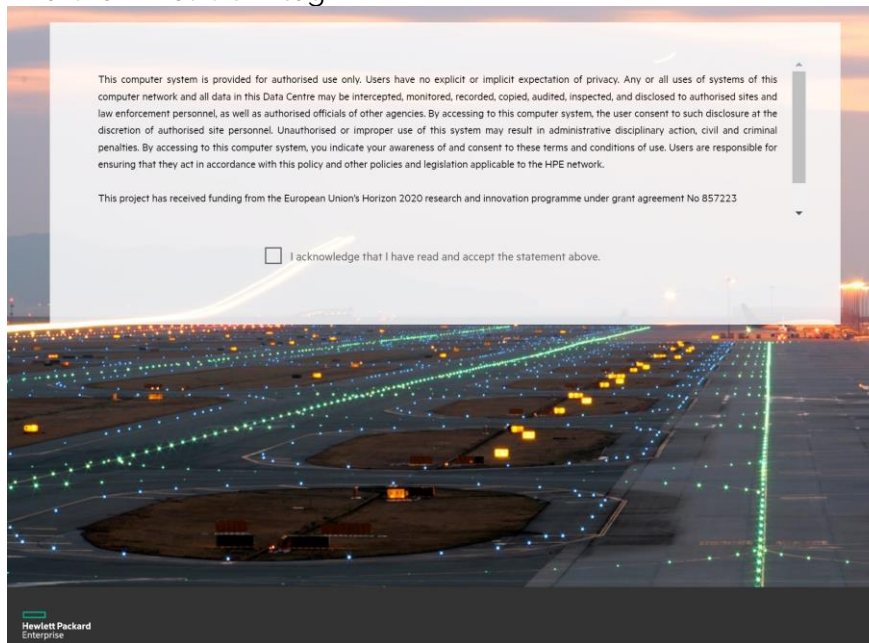
<https://v2.grommet.io/components>

Here is a list of the general icons used in HPE StoreOnce Gen4 GUI:

Icon	Purpose
	System Selector
	Search
	Menu/ Action
	Add
	Option / View
	Edit
	Filter

Icon	Purpose
	Back
	Hide / Show
	Select Column (Display)
	Change View (Tab / Item)
	Management (Federation)
	User / Action
	Close

The Grommet GUI - login:



On the HPE StoreOnce **Dashboard** we can inspect the usage of the storage resources in terms of VTL (**Virtual Tape Library**) and shares (**Catalyst, SMB or NFS**):

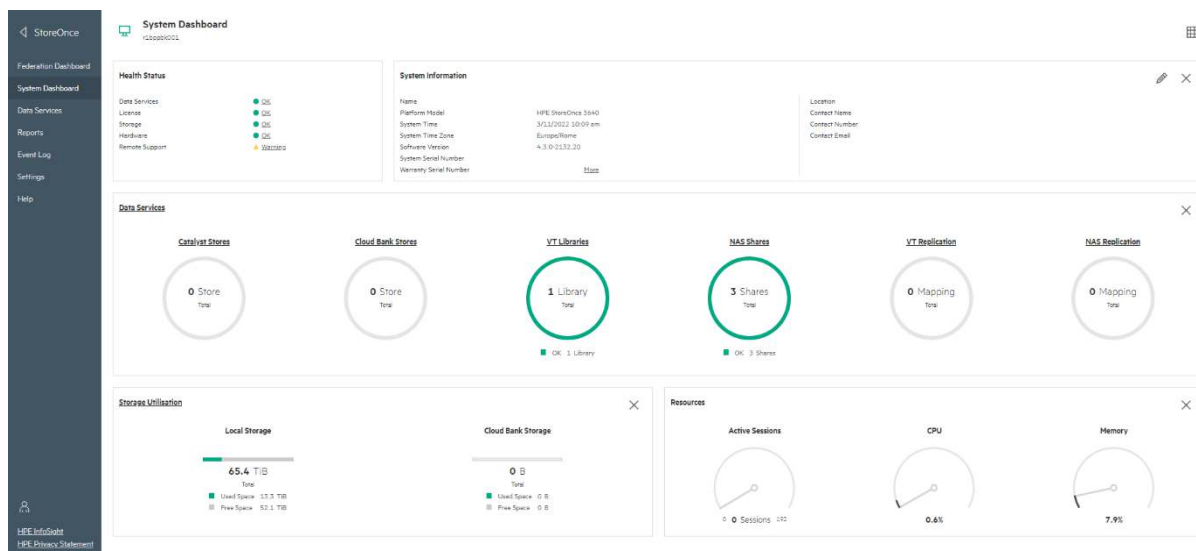


Figure 16 – HPE StoreOnce Dashboard

From here (Figure 16) the **Data Service** status, **Reports**, **Event log** and **Settings** Environments are accessible.

We also inspected the performance of the backup solution by looking at the HPE StoreOnce indicators during the backup operations. An example is reported in the next figure:



Figure 17 – Backup performance evaluation

In the previous figure (Figure 17) you can see when backups are going and how they are distributed in the backup window.

Besides, you can generate reports with **year/month/week/day/hour** granularity, but you can also customize your backup window for past backups or see them in real time (**live**).

Reads and writes are divided but also **VTL/Catalyst & NAS** are distinguished by colour in order to be able to read all the backup activities more easily.

As next step, we do plan to add native a backup solution for **OKD (Kubernetes)**, in addition to **Bareos** general purpose solution. Also we do plan to use **HPE RMC (Recovery Manager Central)** to have an additional layer of protection.

### 2.1.3.4 Monitoring

The monitoring is the process to gather information about the operations of an IT environment's hardware and software to ensure everything functions as expected to support applications and services.

Basic monitoring is performed through device operation checks, while more advanced monitoring gives granular views on operational states, including average response times, number of application instances, error and request rates, CPU usage and application availability.

The software chosen as tool to monitor the entire environment of the GATEKEEPER project is **Checkmk Raw Edition** because it is open source and free to use and it meets all the requirements.

Checkmk is a centralized monitoring system that lets us monitor the entire network in real time from a single machine. If an error occurs, we will be notified immediately and can fix the problem at once.

The central displays for your monitoring in Checkmk are Dashboards. They provide you with both overviews and detailed insights into specific areas. For example, you can visualise the general status of entire network segments, but also simply list which services are generating a load or overload of certain system resources. Checkmk comes with some standard dashboards, such as for problems, Checkmk server statistics and of course a general overview.

Main Dashboard is displayed in Figure 18 and gives the overview of the entire environment.

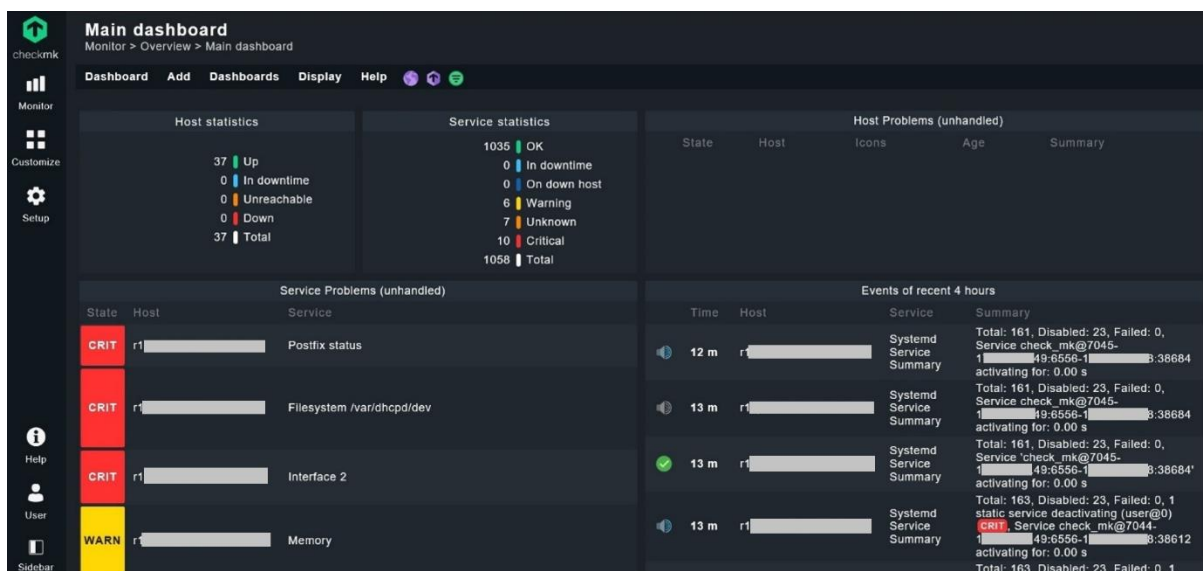


Figure 18 – Main Dashboard



Another useful Dashboard is the All-hosts that gives in a single view the details of all monitored hosts with the number of events divided by type.

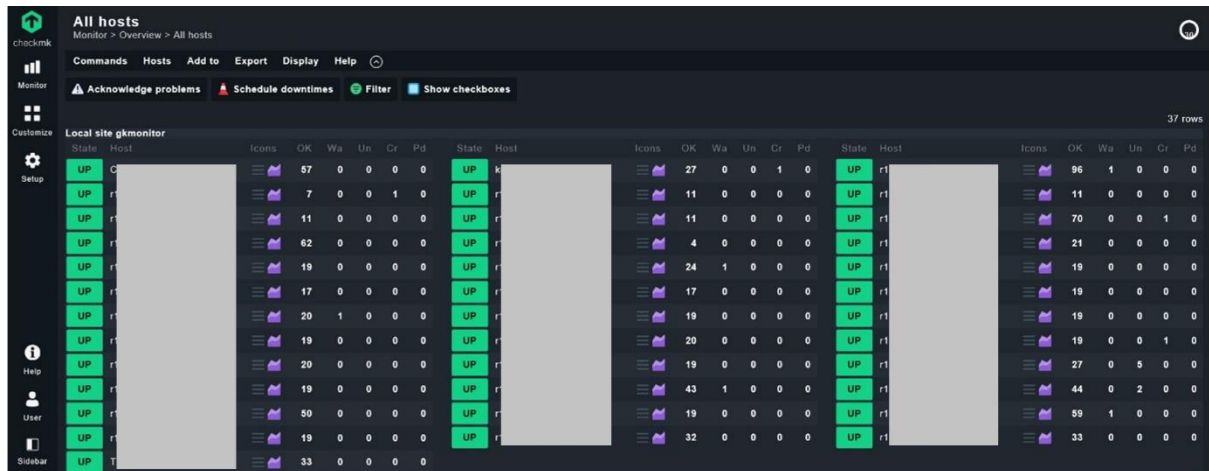


Figure 19 – All-hosts Dashboard

The advantage of incorporating the monitoring process into the project is that it serves a dual purpose, that of identifying real-time problems with systems in production and that of helping to discover bottlenecks or slowdowns on the network that would otherwise be difficult to identify.

Since it was integrated into the infrastructure, the checkmk tool has already helped to solve problems, for example:

- Slowdowns due to errors generated by faulty network cables:



- Prevent filling the filesystems of some machines:



The guideline to implement monitoring into GATEKEEPER project is to integrate at least the lowest layers of the infrastructure (hardware and systems). We are now gradually approaching the integration of other more advanced components (like containers and applications).

The various layers of the infrastructure that are on our integration radar for the monitoring service are:

- Hardware components of Servers/Storage/Switches;
- Hypervisors, e.g., Virtual Machines (VMs);
- Containers orchestration engines, e.g., OKD (containers);
- Other Applications (including databases).

We have setup Checkmk to monitor the first bullet (see next Section 2.1.3.4.1) and we are proceeding with the others in the next period.

### 2.1.3.4.1 Hardware components of Servers and Storage

The role of a hardware monitor is to help to check hardware health by providing instant visibility of the status (up, critical, or warning) and monitor power supply unit (PSU), battery, fans, motherboard, CPU, memory, disks, etc. with the added ability to set baselines and use these values as future points of reference to compare configurations.

Each type of hardware device needs a specific way of integration into Checkmk that depends on the method by which the device makes information available to the outside world. The most common way to query a device is through SNMP, but being an old protocol, some modern systems allow integration only through special agent that use specific APIs.

The systems that make up the GATEKEEPER infrastructure and that have been integrated so far within Checkmk are:

- Uninterruptible Power Supply (UPS): Vertiv UPS EXS;
- Servers: HPE DL360 Gen10 Proliant Server (SNMP agent on ILO);
- Storage: HPE StoreOnce 3640 (SNMP agent on ILO + Special agent via REST API 4.x);
- Storage: HPE Nimble (SNMP agent);
- Storage: HPE MSA 2050 (Special agent via Web Interface);
- Servers: HPE Synergy 12000 (SNMP agent on ILO);
- Switches: HPE 5710 24XGT (SNMP agent).

The next screenshots provide a glance on such integrations:

#### Vertiv UPS EXS

State	Service	Issues	Summary	Age	Checked	Perf.O.Measr
OK	Check_MK		[snmp] Success, execution time 3.7 sec	208 m	35.6 s	3.67 s
OK	Check_MK Discovery		no unmonitored services found, no vanished services found, no new host labels	231 m	102 m	
OK	Battery capacity		4085 years 283 days, On mains, 98.00%	193 m	35.6 s	
OK	Battery state		No battery warnings reported	193 m	35.6 s	
OK	IN frequency phase 1		49.9 Hz	193 m	35.6 s	
OK	IN frequency phase 2		49.9 Hz	193 m	35.6 s	
OK	IN frequency phase 3		49.9 Hz	193 m	35.7 s	
OK	IN voltage phase 1		In voltage: 225V (warn/crit at 210V/180V)	193 m	35.7 s	
OK	IN voltage phase 2		In voltage: 225V (warn/crit at 210V/180V)	193 m	35.7 s	
OK	IN voltage phase 3		In voltage: 225V (warn/crit at 210V/180V)	193 m	35.7 s	
OK	Interface 1		[eth0], (up), MAC: 00:02:99:28:06:63, Speed: 10 Mbit/s (assumed), In: 0.00 B/s (0%), Out: 0.00 B/s (0%)	219 m	35.7 s	0.00 bits/s 0.00 bits/s
OK	Liebert Info		Model: IS-UNITY-OP, Firmware: 8.6.2.0, S/N: 417831G245J2020JAN290007	219 m	35.8 s	
OK	OUT load phase 1		load: 13 (warn/crit at 85/90)	219 m	35.8 s	13.0%
OK	OUT load phase 2		load: 15 (warn/crit at 85/90)	219 m	35.8 s	15.0%
OK	OUT load phase 3		load: 32 (warn/crit at 85/90)	219 m	35.9 s	32.0%
OK	OUT voltage phase 1		out voltage: 231V (warn/crit at 210V/180V)	219 m	35.9 s	
OK	OUT voltage phase 2		out voltage: 230V (warn/crit at 210V/180V)	219 m	35.9 s	
OK	OUT voltage phase 3		out voltage: 228V (warn/crit at 210V/180V)	219 m	35.8 s	
OK	Power phase 1		power: 1700W (warn/crit at 20W/1W)	219 m	36.0 s	1.70 kW
OK	Power phase 2		power: 1900W (warn/crit at 20W/1W)	219 m	36.0 s	1.90 kW
OK	Power phase 3		power: 4200W (warn/crit at 20W/1W)	219 m	36.0 s	4.20 kW
OK	SNMP Info		Uninitialized, Uninitialized, Uninitialized	219 m	36.0 s	
OK	Status EXS 0040KTH16FN01000		System Model Number: EXS 0040KTH16FN01000, System Status: Normal Operation	193 m	36.0 s	
OK	Uptime		Up since Feb 22 2022 10:48:24, Uptime: 3 hours 29 minutes	219 m	36.0 s	209 m



## HPE DL360 Gen10 Proliant Server (SNMP agent on ILO)

r1spsbs002-i.seclab.local					
State	Service	Icons	Summary	Age	Checked
OK	Check_MK		[snmp] Success, execution time 5.4 sec	2022-01-17 10:35:36	43.4 s
OK	Check_MK Discovery		no unmonitored services found, no vanished services found, no new host labels	2021-05-06 17:53:00	45 m
OK	HW Controller 0		Condition: ok, Board-Condition: ok, Board-Status: ok, (Role: other, Model: 92, Slot: 0, Serial: PEYHBOERHDP47U)	2021-05-06 17:56:13	34.4 s
OK	HW CPU 0		CPU0 "Intel(R) Xeon(R) Gold 5215 CPU @ 2.50GHz" in slot 0 is in state "ok"	2021-05-06 17:56:13	34.4 s
OK	HW CPU 1		CPU1 "Intel(R) Xeon(R) Gold 5215 CPU @ 2.50GHz" in slot 0 is in state "ok"	2021-05-06 17:56:13	34.4 s
OK	HW FAN1 system		FAN Sensor 1 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW FAN2 system		FAN Sensor 2 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW FAN3 system		FAN Sensor 3 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW FAN4 system		FAN Sensor 4 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW FAN5 system		FAN Sensor 5 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW FAN6 system		FAN Sensor 6 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW FAN7 system		FAN Sensor 7 "system", Speed is normal, State is ok	2022-01-17 10:35:44	34.4 s
OK	HW Mem 7		Board: 0, Number: 7, Type: unknown (19), Size: 64.0 GiB, Status: good, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Mem 9		Board: 0, Number: 9, Type: unknown (19), Size: 64.0 GiB, Status: good, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Mem 19		Board: 0, Number: 19, Type: unknown (19), Size: 64.0 GiB, Status: good, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Mem 21		Board: 0, Number: 21, Type: unknown (19), Size: 64.0 GiB, Status: good, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/0		Bay: 1, Bus number: 0, Status: ok, Smart status: ok, Ref hours: 11237, Size: 286102MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/1		Bay: 2, Bus number: 0, Status: ok, Smart status: ok, Ref hours: 11237, Size: 286102MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/2		Bay: 3, Bus number: 0, Status: ok, Smart status: ok, Ref hours: 11237, Size: 1716957MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/3		Bay: 4, Bus number: 0, Status: ok, Smart status: ok, Ref hours: 11237, Size: 1716957MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/4		Bay: 5, Bus number: 1, Status: ok, Smart status: ok, Ref hours: 11237, Size: 1716957MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/5		Bay: 6, Bus number: 1, Status: ok, Smart status: ok, Ref hours: 11237, Size: 1716957MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/6		Bay: 7, Bus number: 1, Status: ok, Smart status: ok, Ref hours: 11237, Size: 1716957MB, Condition: ok	2021-05-06 17:56:13	34.4 s
OK	HW Phydrr 0/7		Bay: 8, Bus number: 1, Status: ok, Smart status: ok, Ref hours: 11237, Size: 1716957MB, Condition: ok	2021-05-06 17:56:13	20.9 s
OK	HW Power Meter		Current reading: 212.00 Watts	2021-05-06 17:56:13	20.9 s
OK	HW PSU 0/1		Chassis 0/Bay 1, State: "ok", Usage: 97 Watts	2021-05-06 17:56:13	20.9 s
OK	HW PSU 0/2		Chassis 0/Bay 2, State: "ok", Usage: 115 Watts	2021-05-06 17:56:13	20.9 s
OK	HW PSU Total		Usage: 212 Watts	2021-05-06 17:56:13	20.9 s
OK	Logical Device		Status: OK, Logical volume size: 279.37 GB	2021-05-06 17:56:13	20.9 s
OK	Logical Device 2		Status: OK, Logical volume size: 8.19 TB	2021-05-06 17:56:13	20.9 s
OK	SNMP Info		r1spsbs002-i.seclab.local, Rome, Achille Campanile,	2021-05-06 17:56:13	20.9 s
OK	Temperature 1 ambient		17.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 2 cpu		40.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 3 cpu		40.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 6 memory		25.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 10 memory		31.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 12 system		35.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 15 ambient		18.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 16 system		25.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 17 system		30.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 18 system		23.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 19 system		22.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 20 system		25.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 21 system		24.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 22 system		28.0 °C	2022-01-17 10:35:44	20.9 s
OK	Temperature 23 system		61.0 °C	2022-01-17 10:35:44	17.0 s
OK	Temperature 24 system		33.0 °C	2022-01-17 10:35:44	17.0 s
OK	Temperature 25 system		40.0 °C	2022-01-17 10:35:44	17.0 s
OK	Temperature 26 system		22.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 27 system		48.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 28 ioBoard		85.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 29 system		24.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 31 ioBoard		24.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 33 ioBoard		24.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 37 system		28.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 38 powerSupply		20.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 39 powerSupply		28.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 40 powerSupply		40.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 41 powerSupply		40.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 42 powerSupply		21.0 °C	2022-01-17 10:35:44	17.1 s
OK	Temperature 43 powerSupply		28.0 °C	2022-01-17 10:35:44	17.1 s
OK	Uptime		Up since Sep 19 2021 23:40:45, Uptime: 139 days 21 hours	2021-05-06 17:56:13	149 d

## HPE StoreOnce 3640 (Special agent via REST API 4.x)

r1hppb001.seclab.local					Age	Checked	Perf-O-Meter
State	Service	Icons	Summary				
OK	Check_MK		[special_storeonce4x] Version: unknown, OS: unknown, execution time 2.7 sec		2022-01-05 21:12:09	33.4 s	2.70 s
OK	Check_MK Discovery		no unmonitored services found, no vanished services found, no new host labels		2021-10-26 11:08:59	57 m	
OK	Appliance r1hppb001 License		Status: OK		2021-07-22 11:05:29	26.4 s	
OK	Appliance r1hppb001 Status		State: Reachable, Serial Number: C226280DLW, Software version: 4.3.0-2132.26, Product Name: HPE StoreOnce 3640		2021-07-22 11:05:29	26.4 s	
OK	Appliance r1hppb001 Storage		17.7% used (11.58 of 65.40 TB), trend: +893.19 GB / 24 hours, Total local: 65.40 TB, Free local: 53.82 TB, Dedup ratio: 2.34		12 h	26.4 s	17.7%
OK	Appliance r1hppb001 Summaries		NAS Shares OK (3 of 3), VTL Libraries OK (1 of 1)		2021-12-17 11:00:22	26.4 s	
OK	D2D Services		OverallHealth: Running (active), buffer-manager: Running (active), cat-rpc: Running (active), d2d-iccid: Running (active), d2d-manager-proxy: Running (active), evl-mgr: Running (active), fc-rpc: Running (active), licensing-rpc: Running (active), nls: Running (active), nls-bet: Running (active), nls-rpc: Running (active), nls-share: Running (active), object-store: Running (active), probeapi: Running (active), rep-objectapi: Running (active), rep-rpc: Running (active), replication: Running (active), res-mgr: Running (active), msvc-iccid: Running (active), ssm: Running (active), ssm-rpc: Running (active), vtl: Running (active), vtl-rpc: Running (active)		2021-12-17 11:00:22	26.4 s	

## HPE Nimble (SNMP agent)

r1tppst001.seclab.local					Age	Checked	Perf-O-Meter
State	Service	Icons	Summary				
OK	Check_MK		[snmp] Success, execution time 2.6 sec		2021-11-22 10:45:48	51.8 s	2.58 s
OK	Check_MK Discovery		no unmonitored services found, no vanished services found, no new host labels		2021-04-29 16:40:12	69 m	
OK	Interface 2		[eth0a], (up), MAC: A4:BF:D1:61:C9:27, Speed: 10 GBit/s, In: 169 B/s (<0.01%), Out: 297 B/s (<0.01%)		2021-04-29 16:43:23	43.8 s	1.35 kbit/s 2.37 kbit/s
OK	Interface 4		[eth1a], (up), MAC: B4:96:91:6C:1D:40, Speed: 10 GBit/s, In: 54.9 MB/s (4.39%), Out: 3.92 MB/s (0.31%)		2021-04-29 16:43:23	43.8 s	439 Mbit/s 31.4 Mbit/s
OK	Interface 6		[eth3a], (up), MAC: B4:96:91:6C:17:F0, Speed: 10 GBit/s, In: 61.3 MB/s (4.90%), Out: 6.57 MB/s (0.53%)		2021-04-29 16:43:23	43.8 s	490 Mbit/s 52.5 Mbit/s
OK	Interface 8		[l1], (up), MAC: 56:3E:97:62:59:52, Speed: 40 GBit/s, In: 4.82 kB/s (<0.01%), Out: 2.71 kB/s (<0.01%)		2021-06-24 10:41:28	43.8 s	38.6 kbit/s 1.7 kbit/s
OK	SNMP Info		GK-GROUP, Unknown, @@no.where		2021-04-29 16:43:23	43.8 s	
OK	Uptime		Up since Jun 24 2021 10:32:55, Uptime: 227 days 10 hours		2021-04-29 16:43:23	43.8 s	227 d
OK	Volume Ezmeral-Ephemeral		7.79% used (956.66 GB of 12.00 TB), trend: +2.76 GB / 24 hours		2021-04-29 16:43:23	43.8 s	7.79%
OK	Volume Ezmeral-Ephemeral Read IO		At or above 10-20 ms: 0.77%		2021-04-29 16:43:23	43.8 s	
OK	Volume Ezmeral-Ephemeral Write IO		At or above 10-20 ms: 0.02%		2021-04-29 16:43:23	43.8 s	
OK	Volume Ezmeral-Infrastructure		5.11% used (732.04 GB of 14.00 TB), trend: +581.05 MB / 24 hours		2021-04-29 16:43:23	43.8 s	5.11%
OK	Volume Ezmeral-Infrastructure Read IO		At or above 10-20 ms: 0.37%		2021-04-29 16:43:23	43.8 s	
OK	Volume Ezmeral-Infrastructure Write IO		At or above 10-20 ms: 0.003%		2021-04-29 16:43:23	43.9 s	
OK	Volume Ezmeral-Persistent		48.37% used (19.83 of 41.00 TB), trend: +596.90 GB / 24 hours		2021-04-29 16:43:23	43.9 s	48.37%
OK	Volume Ezmeral-Persistent Read IO		At or above 10-20 ms: 4.55%		2021-04-29 16:43:23	43.9 s	
OK	Volume Ezmeral-Persistent Write IO		At or above 10-20 ms: 0.02%		2021-04-29 16:43:23	43.9 s	
OK	Volume Okd-Infrastructure		32.35% used (828.14 GB of 2.50 TB), trend: +3.37 GB / 24 hours		2021-04-29 16:43:23	43.9 s	32.35%
OK	Volume Okd-Infrastructure Read IO		At or above 10-20 ms: 0.34%		2021-04-29 16:43:23	43.9 s	
OK	Volume Okd-Infrastructure Write IO		At or above 10-20 ms: 0.003%		2021-04-29 16:43:23	43.9 s	
OK	Volume Okd-Pod		2.15% used (15.05 of 700.00 GB), trend: +297.65 MB / 24 hours		2021-04-29 16:43:23	24.1 s	2.15%
OK	Volume Okd-Pod Read IO		At or above 10-20 ms: 0.11%		2021-04-29 16:43:23	24.1 s	
OK	Volume Okd-Pod Write IO		At or above 10-20 ms: 0.002%		2021-04-29 16:43:23	24.1 s	
OK	Volume oVirt-Engine		6.62% used (13.24 of 200.00 GB), trend: +25.92 MB / 24 hours		2021-04-29 16:43:23	24.1 s	6.62%
OK	Volume oVirt-Engine Read IO		At or above 10-20 ms: 0.01%		2021-04-29 16:43:23	24.1 s	
OK	Volume oVirt-Engine Write IO		At or above 10-20 ms: 0.001%		2021-04-29 16:43:23	24.1 s	
OK	Volume Prj-Projects-Data		27.58% used (137.91 of 500.00 GB), trend: +812.95 MB / 24 hours		2021-04-29 16:43:23	24.1 s	27.58%
OK	Volume Prj-Projects-Data Read IO		At or above 10-20 ms: 0.03%		2021-04-29 16:43:23	24.1 s	
OK	Volume Prj-Projects-Data Write IO		At or above 10-20 ms: 0.002%		2021-04-29 16:43:23	24.2 s	
OK	Volume Prj-Services		60.02% used (480.16 of 800.00 GB), trend: +580.86 MB / 24 hours		2021-04-29 16:43:23	24.2 s	60.02%
OK	Volume Prj-Services Read IO		At or above 10-20 ms: 0.23%		2021-04-29 16:43:23	24.2 s	
OK	Volume Prj-Services Write IO		At or above 10-20 ms: 0.004%		2021-04-29 16:43:23	24.2 s	

## HPE MSA 2050 (Special agent via Web Interface)

State	Service	Icons	Summary	Age	Checked	Perf-O-Meter
OK	Check_MK	🔍	[special_hp_msa] Version: unknown, OS: unknown, execution time 8.6 sec	2021-09-23 15:37:26	54.0 s	8.61 s
OK	Check_MK Discovery	🔍	no unmonitored services found, no vanished services found, no new host labels	2021-09-23 14:24:02	80 m	
OK	Controller IO SUMMARY	🔍	Read: 1.72 MB/s, Write: 934.01 kB/s	2021-07-22 18:29:27	40.8 s	1.72 MB/s / 934.01 kB/s
OK	CPU Utilization A	🔍	Total CPU: 3.0%	2021-07-22 18:28:26	40.8 s	3.0%
OK	CPU Utilization B	🔍	Total CPU: 1.0%	2021-07-22 18:28:26	40.8 s	1.0%
OK	Disk Health 1.1	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.2	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.3	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.4	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.5	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.6	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.7	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disk Health 1.8	🔍	Status: OK, serial number: 3050A2F3FF4F, vendor: HP, model: EG001200JWJNK, description: SAS, size: 1200.2 GB, speed: 10 RPM	2021-07-22 18:28:26	40.8 s	
OK	Disks IO SUMMARY	🔍	Read: 3.33 MB/s, Write: 3.19 MB/s	2021-07-22 18:29:27	40.8 s	3.33 MB/s / 3.19 MB/s
OK	Fan Enclosure 1 PSU 1 Left	🔍	Status: up, speed: 3830 RPM	2021-07-22 18:28:26	40.8 s	
OK	Fan Enclosure 1 PSU 2 Right	🔍	Status: up, speed: 3830 RPM	2021-07-22 18:28:26	40.8 s	
OK	Filesystem oVirt-Engine	🔍	A (RAID0), 17.73% used (33.02 of 186.26 GB), trend: -596.40 kB / 24 hours	2021-07-22 18:28:26	40.8 s	17.73%
OK	Filesystem oVirt-VM	🔍	A (RAID0), 7.51% used (349.50 GB of 4.55 TB), trend: +477.60 MB / 24 hours	2021-07-22 18:28:26	40.8 s	7.51%
OK	Interface 1	🔍	[A1] (up), Speed: 1 Gb/s, In: 486 kB/s (0.39%), Out: 244 kB/s (0.20%)	2021-07-22 18:28:26	40.8 s	3.88 MB/s / 1.90 MB/s
OK	Interface 2	🔍	[A2] (up), Speed: 1 Gb/s, In: 444 kB/s (0.35%), Out: 226 kB/s (0.18%)	2021-07-22 18:28:26	40.8 s	3.55 MB/s / 1.81 MB/s
OK	Interface 3	🔍	[A3] (up), Speed: 1 Gb/s, In: 479 kB/s (0.38%), Out: 274 kB/s (0.22%)	2021-07-22 18:28:26	40.8 s	3.83 MB/s / 2.20 MB/s
OK	Interface 4	🔍	[A4] (up), Speed: 1 Gb/s, In: 410 kB/s (0.33%), Out: 384 kB/s (0.32%)	2021-07-22 18:28:26	12.9 s	3.28 MB/s / 3.15 MB/s
OK	Interface 5	🔍	[B1] (up), Speed: 1 Gb/s, In: 0.00 B/s (0%), Out: 0.00 B/s (0%)	2021-07-22 18:28:26	12.9 s	0.00 b/s / 0.00 b/s
OK	Interface 6	🔍	[B2] (up), Speed: 1 Gb/s, In: 0.00 B/s (0%), Out: 0.00 B/s (0%)	2021-07-22 18:28:26	12.9 s	0.00 b/s / 0.00 b/s
OK	Interface 7	🔍	[B3] (up), Speed: 1 Gb/s, In: 0.00 B/s (0%), Out: 0.00 B/s (0%)	2021-07-22 18:28:26	12.9 s	0.00 b/s / 0.00 b/s
OK	Interface 8	🔍	[B4] (up), Speed: 1 Gb/s, In: 0.00 B/s (0%), Out: 0.00 B/s (0%)	2021-07-22 18:28:26	12.9 s	0.00 b/s / 0.00 b/s
OK	Power Supply Health Enclosure 1 Left	🔍	Status: OK	2021-07-22 18:28:26	12.9 s	
OK	Power Supply Health Enclosure 1 Right	🔍	Status: OK	2021-09-10 11:29:55	12.9 s	
OK	System Health r1lpsst001	🔍	Status: OK	2021-09-10 11:29:55	12.9 s	
OK	Temperature Disks	🔍	8 Sensors: Highest: 22.0 °C, Average: 21.2 °C, Lowest: 20.0 °C	2021-07-22 18:28:26	12.9 s	22 °C
OK	Volume Health oVirt-Engine	🔍	Status: OK, container name: A (RAID0)	2021-07-22 18:28:26	12.9 s	
OK	Volume Health oVirt-VM	🔍	Status: OK, container name: A (RAID0)	2021-07-22 18:28:26	12.9 s	
OK	Volume IO SUMMARY	🔍	Read: 1.68 MB/s, Write: 1.11 MB/s	2021-07-22 18:29:27	12.9 s	1.68 MB/s / 1.11 MB/s

## HPE 5710 24XGT (SNMP agent)

State	Service	Icons	Summary	Age	Checked	Perf-O-Meter
OK	Check_MK	🔍	[snmp] Success, execution time 7.9 sec	2021-09-20 19:07:24	47.2 s	7.87 s
OK	Check_MK Discovery	🔍	no unmonitored services found, 6 vanished services (hp_hh3c_ext2, hp_hh3c_ext_cpu2, hp_hh3c_ext_mem2), no new host labels	2021-09-20 19:09:54	85 m	
OK	CPU utilization MODULE LEVEL1 192	🔍	Total CPU: 5.0%	2021-11-10 14:54:31	35.2 s	5.0%
OK	CPU utilization MODULE LEVEL1 210	🔍	Total CPU: 5.0%	2021-11-10 14:54:31	35.2 s	5.0%
OK	Interface 0001	🔍	[ILO/mgmt], (up), MAC: 4C:AE:A3:EE:72:1E, Speed: 1 Gb/s, In: 0.00 B/s (0%), Out: 72.6 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	0.00 b/s / 581 b/s
OK	Interface 0002	🔍	[ILO/mgmt], (up), MAC: 4C:AE:A3:EE:72:1D, Speed: 1 Gb/s, In: 0.00 B/s (0%), Out: 75.3 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	0.00 b/s / 602 b/s
OK	Interface 0003	🔍	[ILO/mgmt], (up), MAC: 4C:AE:A3:EE:72:20, Speed: 1 Gb/s, In: 7.13 kB/s (<0.01%), Out: 377 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	57.0 kb/s / 3.02 kb/s
OK	Interface 0004	🔍	[Heartbeat], (up), MAC: 4C:AE:A3:EE:72:1F, Speed: 1 Gb/s, In: 22.3 kB/s (0.02%), Out: 4.33 kB/s (<0.01%)	2021-09-20 19:07:29	35.2 s	178 kb/s / 94.7 kb/s
OK	Interface 0005	🔍	[Heartbeat], (up), MAC: 4C:AE:A3:EE:72:22, Speed: 1 Gb/s, In: 4.30 B/s (<0.01%), Out: 77.0 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	34.4 b/s / 616 b/s
OK	Interface 0006	🔍	[Heartbeat], (up), MAC: 4C:AE:A3:EE:72:21, Speed: 1 Gb/s, In: 4.30 B/s (<0.01%), Out: 77.0 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	34.4 b/s / 616 b/s
OK	Interface 0007	🔍	[LINK-TO-UPS], (up), MAC: 4C:AE:A3:EE:72:24, Speed: 1 Gb/s, In: 5.78 B/s (<0.01%), Out: 75.4 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	46.3 b/s / 603 b/s
OK	Interface 0009	🔍	[Server MGMT], (up), MAC: 4C:AE:A3:EE:72:26, Speed: 1 Gb/s, In: 489 B/s (<0.01%), Out: 926 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	3.91 kb/s / 7.41 kb/s
OK	Interface 0010	🔍	[Server MGMT], (up), MAC: 4C:AE:A3:EE:72:25, Speed: 1 Gb/s, In: 4.30 B/s (<0.01%), Out: 470 B/s (<0.01%)	2021-09-20 19:07:29	35.2 s	34.4 b/s / 676 kb/s
OK	Interface 0011	🔍	[Virtual Machine VLAN], (up), MAC: 4C:AE:A3:EE:72:28, Speed: 10 Gb/s, In: 14.9 kB/s (<0.01%), Out: 20.0 kB/s (<0.01%)	2021-09-20 19:07:29	35.2 s	119 kb/s / 160 kb/s
OK	Interface 0185	🔍	[P2P to Core], (up), MAC: 4C:AE:A3:EE:76:6B, Speed: 10 Gb/s, In: 187 B/s (<0.01%), Out: 87.6 B/s (<0.01%)	2021-11-22 11:18:31	4.93 s	1.50 kb/s / 701 kb/s
OK	Interface 0196	🔍	[IRF-Port 2/2], (up), MAC: 4C:AE:A3:EE:76:75, Speed: 40 Gb/s, In: 17.4 kB/s (<0.01%), Out: 17.9 kB/s (<0.01%)	2021-09-20 19:07:29	4.94 s	139 kb/s / 143 kb/s
OK	Interface 0201	🔍	[IRF-Port 2/1], (up), MAC: 4C:AE:A3:EE:76:79, Speed: 40 Gb/s, In: 51.4 kB/s (<0.01%), Out: 25.6 kB/s (<0.01%)	2021-09-20 19:07:29	4.94 s	411 kb/s / 205 kb/s
OK	Memory MODULE LEVEL1 192	🔍	Usage: 31.0% - 1.21 GB of 3.92 GB	2021-11-10 15:06:31	4.94 s	
OK	Memory MODULE LEVEL1 210	🔍	Usage: 31.0% - 1.21 GB of 3.92 GB	2021-11-10 15:06:31	4.94 s	
OK	SNMP Info	🔍	CORE, Roma, Calmi-Claudio	2021-09-20 19:07:29	4.94 s	
OK	Temperature MODULE LEVEL1 192	🔍	42 °C	2021-11-10 14:54:31	4.95 s	42 °C
OK	Temperature MODULE LEVEL1 210	🔍	42 °C	2021-11-10 14:54:31	4.95 s	42 °C
OK	Uptime	🔍	Up since May 19 2021 12:49:42, Uptime: 263 days 8 hours	2021-09-20 19:07:29	4.95 s	263 d

### 2.1.3.5 IDS & Anti-malware

We are internally prototyping the deployment of an Intrusion Detection System (IDS) at network level, based on open source software. The IDS will detect suspicious patterns and alert the Log Management solution (see Section 2.1.3.2) for further actions. We will start deploying first the IDS system and later we will evaluate to turn into Intrusion Prevention System (IPS), which will block malicious software payloads automatically. The prototyping solution is based on **Suricata** [35], a well-known IDS and IPS threat detection engine. It is a signature-based solution that works by using regularly updates patterns to spot security threats. The result of this activity will feed the Log Management system, where it will be analysed and reported.

Another technical security measure we are prototyping is the deployment of an anti-malware/anti-virus solution, which will run on all the HPE GATEKEEPER hosts. We are using **ClamAV** [36], a well-known “*open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats*”. It works by employing always updated signature to detect viruses and other malicious content. It can be periodically run (e.g., daily or weekly) to scan the whole server filesystem for detection. The scan result will be sent to the Log Management, where it will be analysed and reported.

## 2.2 Continuous Integration and Continuous Delivery

In D4.1 we outlined the CI/CD strategy and architecture, including the concepts of SecDevOps and CI/CD tools identified in the previous phase of the project.

The aim of the following section is to describe the implementation of the CI/CD architecture focusing on the interaction between components, how the solution guarantees security requirements and what is the output for the final user.

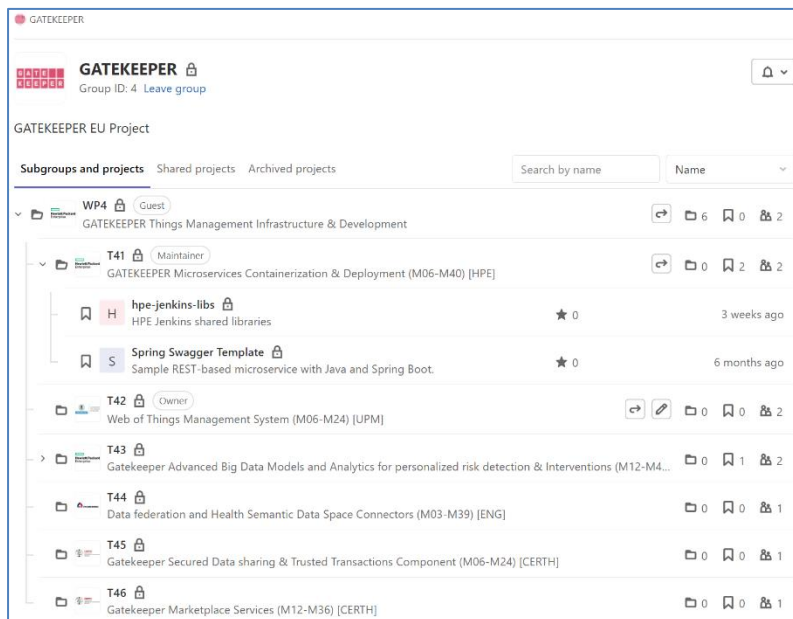
### 2.2.1 CI/CD Implementation

In this section we describe the tools used to implement the CI/CD pipeline starting from the code versioning system, through the software repository, the ci/cd server until the tools for security testing and reporting. The idea of creating the pipeline is to make automatic the software development process instead of doing each step manually. Also, our solution introduces security at every level of the process.

As said in D4.1, the tool selected for managing code versioning is **GitLab**.



All partners have to push code in GitLab and for convention all projects are organized following the division of work packages (WP) and tasks (T).



To automate the access to GitLab to authorized users only, a custom user provisioning tool creates on GitLab only those users and assign them the guest role.

Every WP has a Task Leader Maintainer (TLM) which is a developer that will get the maintainer role of the corresponding GitLab Task Group. TLM will appoint users to work in projects under the Task Group with the developer or maintainer role. GitLab roles are

explained in [33].

**Nexus** has been chosen as software repository for components such as packages, libraries, binary and Docker images available to end users such as the Figure 20 below shows. For uploading the images we followed the same structure of GitLab, with the division into WPs and Tasks. This convention is also followed in the **Jenkins** pipeline to call the respective images.

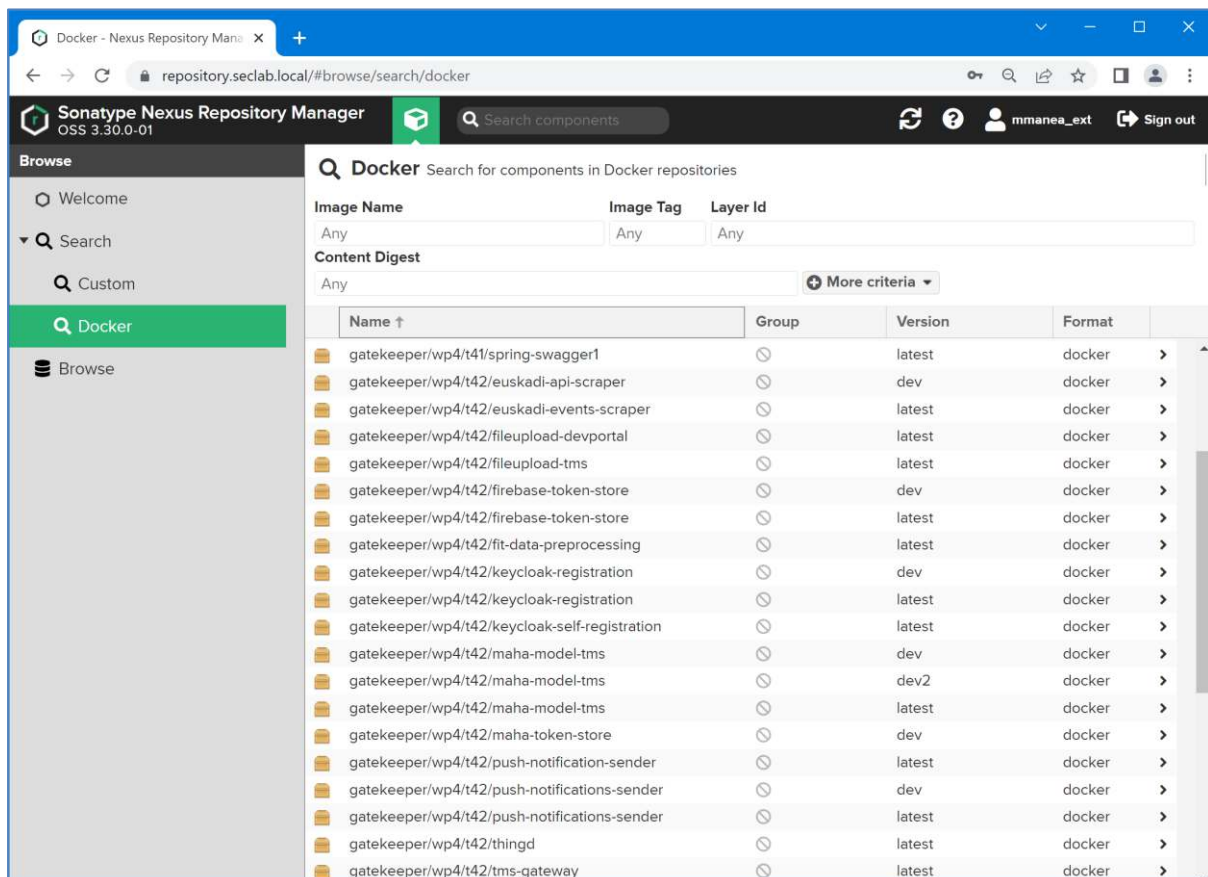


Figure 20 - Nexus Repository.

As a CI/CD orchestrator tool to monitor source repositories, build software, run tests and deploy software it has been chosen the open source tool **Jenkins**.

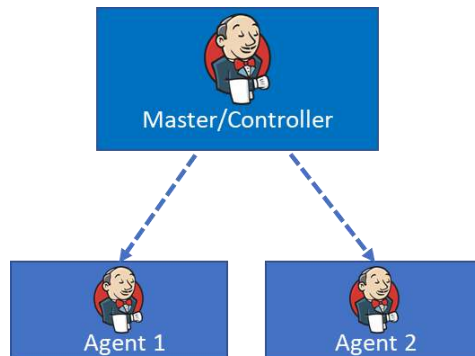


Figure 21 - Jenkins Infrastructure.

For Jenkins we realized a multi node infrastructure made up of one Master node and two Agent nodes: the Master node is designed to coordinate and provide the Web Access and the API endpoints while the Agent nodes are designed to perform and balance the work.

In particular, Agent 1 builds the software artefacts in a container, such in a way that the tools needed to build are part of the container instantiation and not directly installed on the Agent.

Agent 2 is identified as the security node that analyses the code of the software artefacts and it performs different levels of security analyses.

According to the CI/CD pipeline concept described in the D4.1, in order to automate the deployment process three pipelines are implemented.

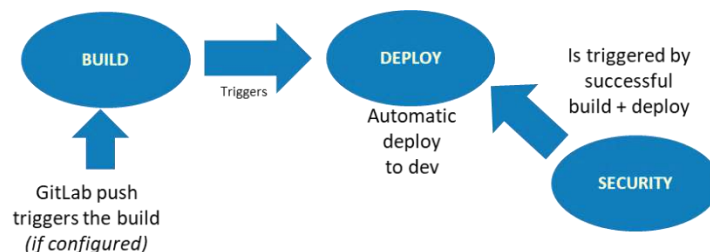


Figure 22 - GATEKEEPER CI/CD pipelines diagram

As shown in the Figure 22 the Build pipeline is triggered automatically at every push of the project in GitLab and it automatizes the build of the project, the creation of the Docker image and its push on the Nexus Docker Registry. Then, if the previous pipeline succeeded, the second Deploy pipeline is triggered and automatically deploys the component to the development environment. Finally, the Security pipeline is triggered if the Build and the Deploy pipelines are succeeded.

For automating the creation of the three pipelines we use the Jenkins plugin *Seed Jobs*. This utility has been configured to permit to fill out a form by entering parameters such as:

- Work Packages/Task folder where the Jenkins Jobs will be created;
- Job basename, that typically is the component name;
- GitLab URL, retrieved from the GitLab web interface;
- Build template, chosen from a preconfigured template or customize it manually;
- Dockerfile, the name of the dockerfile to build the container image;
- Image, the name of the container image pushed to the private Nexus Docker registry;
- Yaml files, used for deployment onto OKD (one or more).

Once these details are provided, the *Seed Job* automatically creates the three standardized pipelines for build, deploy and security.

## Build pipeline

In the Build pipeline there are different phases where first the code is checked out from GitLab and the container used to build is setup. It follows compile, testing and package stages where it is possible to customize the build process depending of the used tools. The next three stages are referred to the container images managing, building and pushing to the images to the Nexus Docker repository. There is an optional phase to tag the image before the push if it is not used the latest tag. When no errors occur the Deploy Job is automatically called.

Stage View													
	Checkout Code	Setup Build Container	Compile	Testing	Package	Manage Container	Build Container Image	Push Container Latest Image	Optional Tag and Push Container	Clean-up Built Container Image	Call Deploy Job	Archive Artifacts	Declarative: Post Actions
Average stage times: (Average <i>git</i> run time: ~1min 7s)	2s	2s	4s	12s	3s	1s	2s	6s	0ms	1s	22s	2s	384ms
Nov 10 19:29	846ms	897ms	3s	11s	3s	130ms	1s	6s		310ms	16s	2s	823ms

Figure 23 - Stages of the build pipeline

## Deploy pipeline

In the deploy pipeline the attention is focused on the release of the components in the development environment. To make it possible, we need credentials to access to the OKD container orchestrator. In the next steps are applied the YAML deployment files to OKD where the configuration of the multiple Kubernetes resources are defined. The security pipeline is automatically triggered upon a successful build and deploy.

Stage View						
	Validate Settings	Checkout Code	OKD Login	Apply YAML files to OKD	OKD Logout	Declarative: Post Actions
Average stage times:	0ms	1s	3s	4s	2s	978ms
Nov 11 08:49		1s	2s	4s	1s	1s

Figure 24 – Stages of the deploy pipeline.

## Security pipeline

The security pipeline performs different types of security analysis of the software artefacts.

The first security control is performed by Semgrep [1] which is used to scan static source code to spot code vulnerabilities. The second security control is the container scanning by the Gype [2] tool to spot well-known vulnerabilities in container packages. The last control is Software Composition Analysis (SCA) done by OWASP Dependency Check [3] to spot security issues in third party libraries.

Every security tool creates a specific report. We added in the pipeline a step that make use of DefectDojo [4], an open source vulnerability report aggregator, where all security analysis results obtained by the previous scans are merged. These results are displayed in dashboards and diagrams that give an overall view on vulnerabilities to the developer.

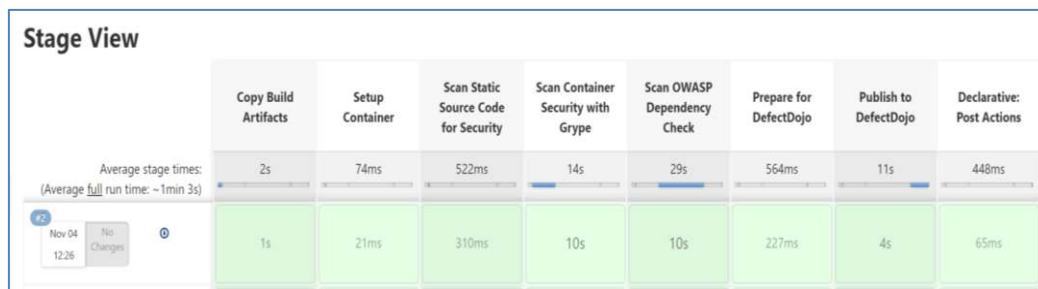


Figure 25 – Stages of the security pipeline.

## 2.3 Containerization Implementation

As described in the containerization techniques overview presented in D4.1 (Section 1.3), we finally select OKD [4] as the container orchestration engine to host and run the GATEKEEPER Platform services developed by the partners as part of the other WP4 tasks.

OKD leverages on the de-facto standard Kubernetes engine [7], but adds many features including a stricter security environments (by default containers cannot run with administrative privileges) and a sophisticated but user-friendly graphical interface that let users interact with it without the need to go through the command line.

OKD has been configured to segregate with separated tenants all the GATEKEEPER Pilots. This makes use of the project and namespace concepts that allow to isolate the deployed components. Components are packages as containers and run in so called *Pods* (the Kubernetes resource to host one or more containers). Pods in different projects cannot talk to each other because we defined specific virtual network level policies for isolation.

The following Figure 26 illustrates the isolation between Project Pilots and their running components in the Pods<sup>3</sup>:

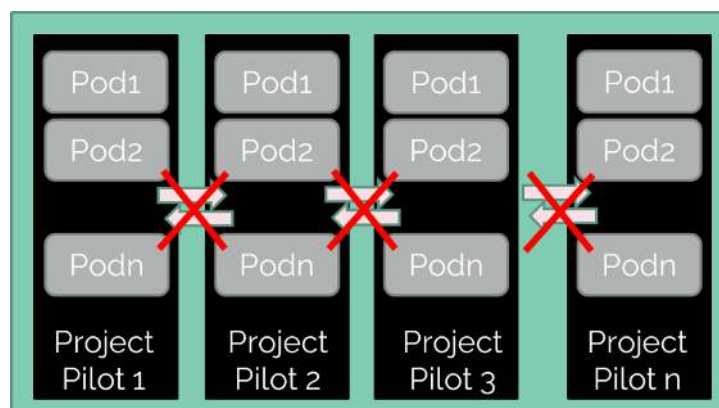


Figure 26 – Segregation for GATEKEEPER Pilots

<sup>3</sup> The running components of the GATEKEEPER Platform services can be considered a set of Pods.



Project Pilots can be accessed only to authorized Pilot users and administrators. Accounts are defined on the centralized Data Centre Identity Management service and follows the authorization process defined in Section 2.1.2.3. Also access to Pilots tenants is granted via Multi-Factor Authentication to authorized people only.

Similar to the Pods, also the Pilots' data is segregated in different volumes (Kubernetes calls them Persistent Volume Claims - PVC). These volumes are maintained in the HPE Nimble storage solution, which guarantees a high-level of availability and also has been configured to use data encryption at rest as a technical security measure.

Figure 27 shows the list of OKD Projects defined to support the project Pilots execution:

### Projects

Name	gatekeeper	
Name	gatekeeper	Clear all filters
Name ↑	Display name ↑	Status ↑
PR gatekeeper-dev	Dev	✓ Active
PR gatekeeper-pilot1	PUGLIA	✓ Active
PR gatekeeper-pilot2	ARAGON	✓ Active
PR gatekeeper-pilot3	SAXONY	✓ Active
PR gatekeeper-pilot4	BASQUE_COUNTRY	✓ Active
PR gatekeeper-pilot5a	Greece_UC_#a	✓ Active
PR gatekeeper-pilot5b	Greece_UC_#b	✓ Active
PR gatekeeper-pilot6a	Cyprus_UC_#a	✓ Active
PR gatekeeper-pilot6b	Cyprus_UC_#b	✓ Active
PR gatekeeper-pilot7	Milton_Keynes	✓ Active
PR gatekeeper-pilot8	Poland	✓ Active
PR gatekeeper-pilot9	Covid-19	✓ Active
PR gatekeeper-pilot10	Bangor	✓ Active
PR gatekeeper-pilot11	SINGAPORE	✓ Active
PR gatekeeper-pilot12	TAIWAN	✓ Active
PR gatekeeper-pilot13	HONG KONG	✓ Active
PR gatekeeper-production	Prod	✓ Active
PR gatekeeper-test	Test	✓ Active

Figure 27 – List of GATEKEEPER Pilots projects (tenants)

In addition to the Pilots, we have three special projects:

- **gatekeeper-dev:** it contains always the latest version of the GATEKEEPER Platform services that is under active development (this is also automatically populated when the CI/CD executes, see 2.2);
- **gatekeeper-test:** it is used to perform integration testing for the Pilots, before moving to their specific project;
- **gatekeeper-prod:** it is used to host some common components that are shared among all the pilots, like the GATEKEEPER Marketplace (T4.6).

The following Figure 28 shows a specific Pilot project (tenant) with all its required running components of the GATEKEEPER Platform:

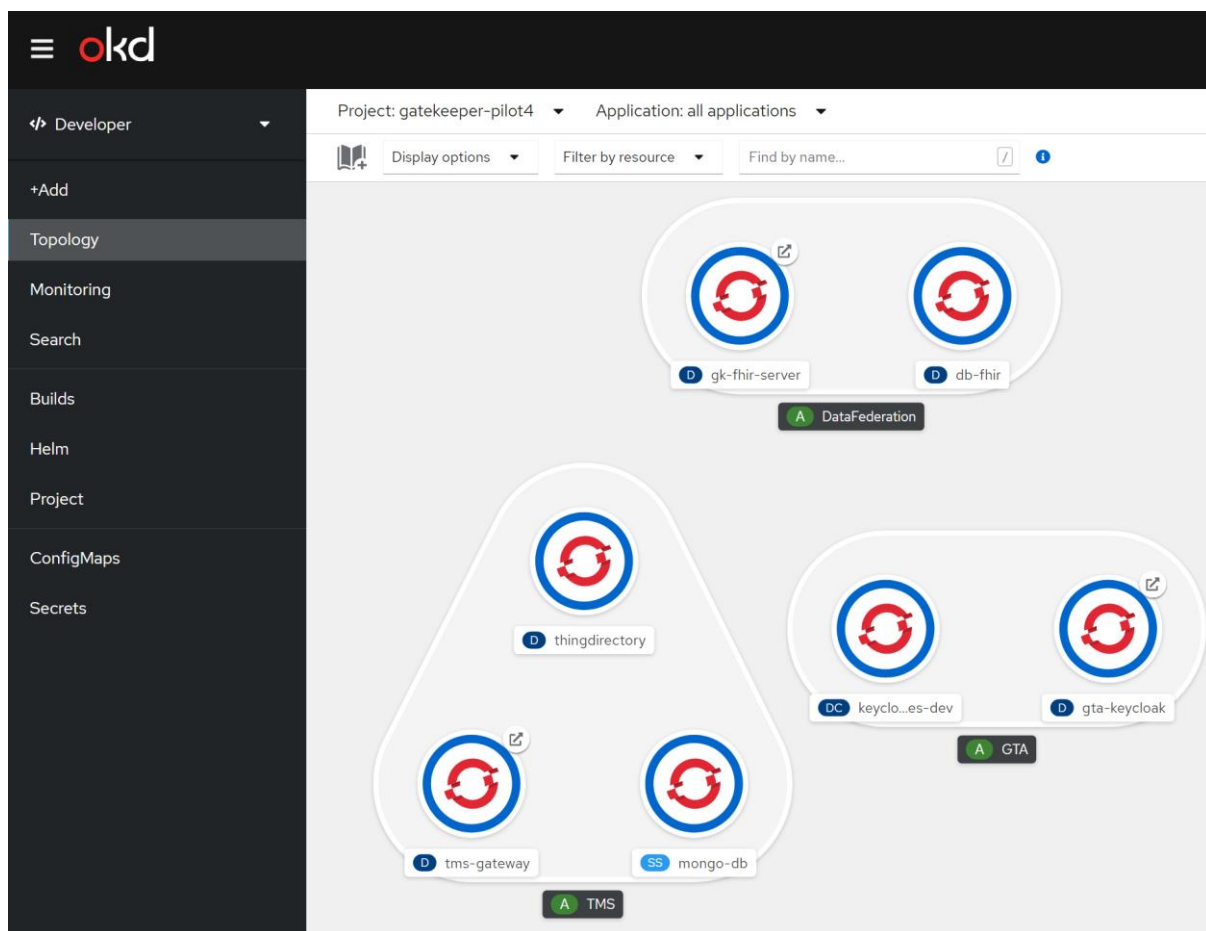


Figure 28 – Sample project with available components

The figure shows the Pods grouped by component, like TMS (Thing Management Systems, part of T4.2), Data Federation (part of T4.4), and the GTA (GATEKEEPER Trusted Authority, part of T4.5).

## 2.4 Support and Ticketing System

The Support and Ticketing System in GATEKEEPER responds to the need to implement a system to handle infrastructure problems across the entire Data Centre services and to collect new feature requests in a structured and reportable way.

To address this purpose we utilized the GitLab Issue functionality, by creating a specific project under a GitLab which is accessible to all GATEKEEPER users that want to report a problem or a feature request.

This is useful both for the users that keep trace in a single place of their issues and both for the person assigned to resolve it that can check easily the status of the issue.

It has been created a Wiki landing page for the GATEKEEPER users with instructions about how to report issues, the provided functionalities and some guidelines to follow to standardize the process.

The issue reporting makes use of custom labels (shown in the Figure) to permit a better identification of the issue lifecycle status and to classified them by type.

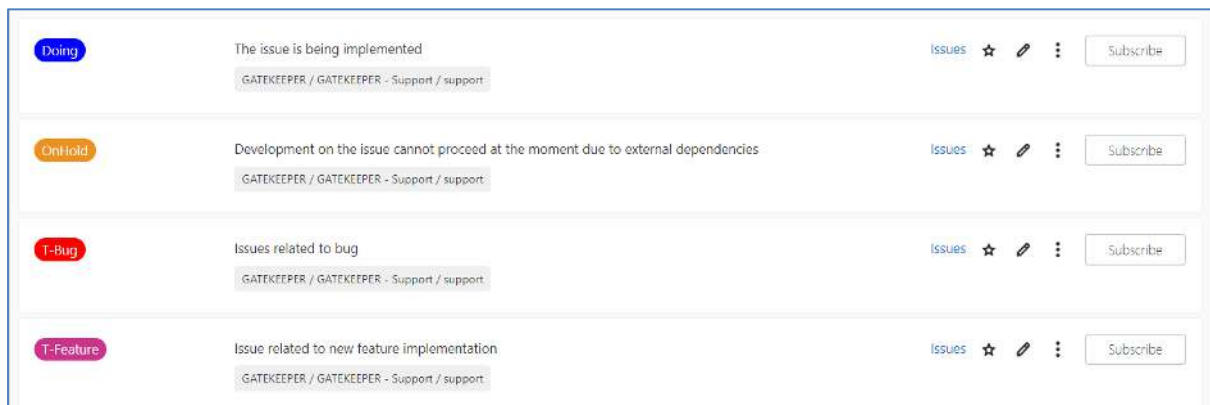


Figure 29 – Support projects' labels.

For example, we identify two type of issues, depending it concerns a **Bug** or a new **Feature** and we created the respective labels:

- **T-Bug**: this label is assigned to an issue that reports an incorrect behaviours in a Data Centre component.
- **T-Feature**: this label is assigned to an issue that is a new or change request to develop new functionalities or enhance existing ones.

Regarding the status, in addition to the Open/Closed label given by default, we decided to create other labels for handling the issue lifecycle by adding two new states:

- **Doing**: a label for an issue that is in progress;
- **OnHold**: a label for an issue that is temporary stopped for external dependencies, which can be an action asked to the user.

Based on these labels it is possible to create multiple boards on the Issue tab with a different custom view that follows our criteria to process the issue.

For example, we created two boards: one by Type and one by Status.

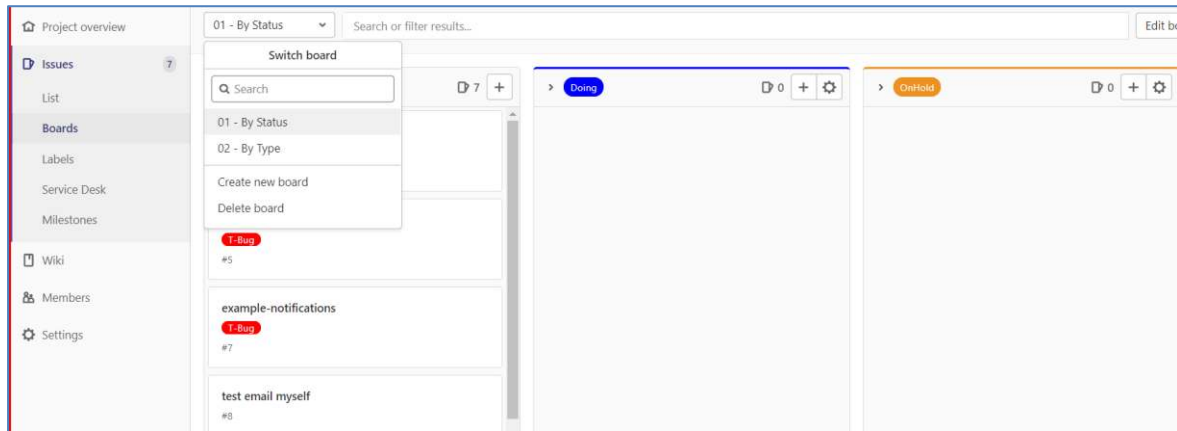


Figure 30 – Issue boards.

When a user creates an issue, following the instructions on the Wiki page, s/he has to select in the picklist the proper template that is created for each type of issue (bug or feature, as mentioned before). To simplify and best fitting the problem, it has been created **BugTemplate** and **FeatureTemplate** with a suggested form to fill.

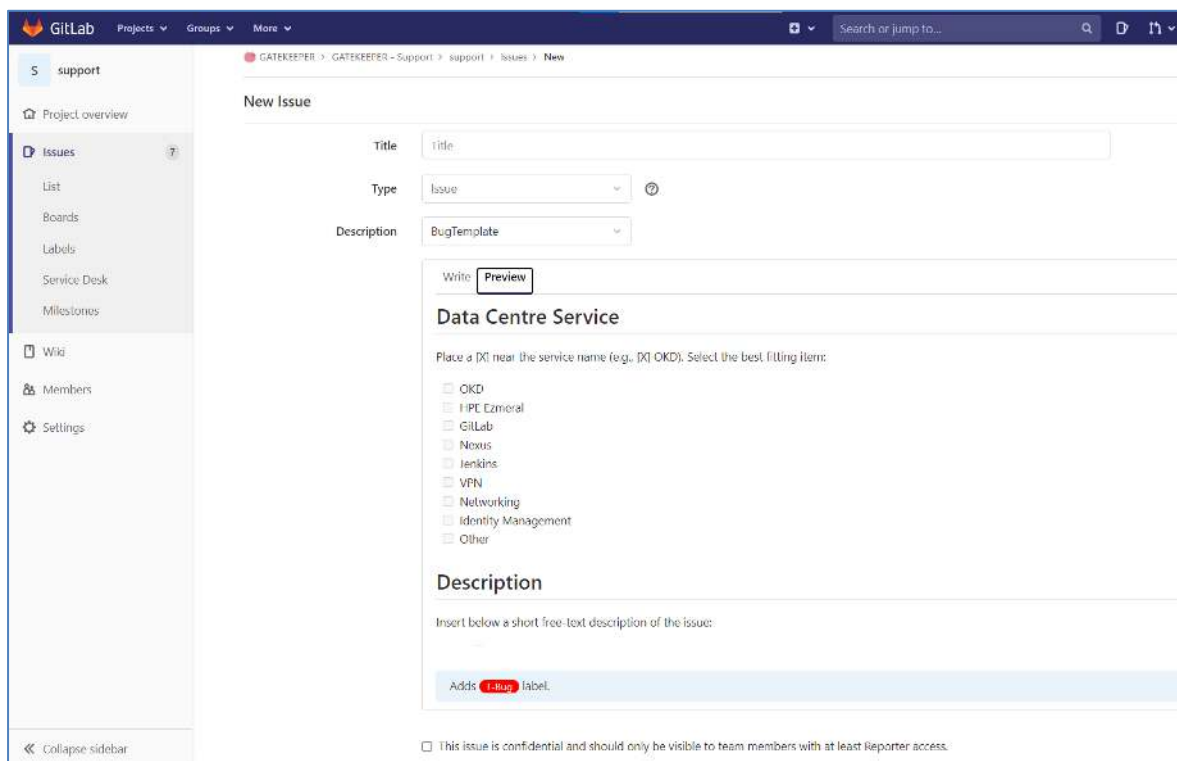


Figure 31 - Issue Template prototype.

There is also the possibility to keep an issue confidential (visible only to the issue creator and to HPE staff).

Currently the Support and Ticketing System has just been released and it is expected it will be enhance in the future period with the feedbacks coming from the users.

## 3 GATEKEEPER User Manuals

### 3.1 GATEKEEPER Data Centre Infrastructure

#### 3.1.1 Data Centre Access User Manual

In D4.1 we delivered the Access Manual for partners' access via VPN (road warrior VPN). We now also release the manual for site-to-site VPN connections used for project pilots and open callers.

As part of this deliverable, we release as an Annex the **confidential document** that describes in detail the operating procedure GATEKEEPER partners must follow to use the S2S VPN. We report in Figure 32 the index of the document.

T4.1 Site-to-Site VPN to HPE GK Data Centre		G A T E K E E P E R
<b>Table of contents</b>		
<b>TABLE OF CONTENTS .....</b>		<b>5</b>
<b>INTRODUCTION.....</b>		<b>6</b>
<b>1 SITE-TO-SITE VPN CONNECTION.....</b>		<b>7</b>
1.1 OPENVPN INSTALLATION AND CONFIGURATION.....		7
1.1.1 Ubuntu 20.04 LTS.....		7
1.1.2 CentOS / RedHat 7.....		9
1.1.3 Amazon Linux 2.....		11
<b>CONCLUSIONS .....</b>		<b>14</b>
<b>REFERENCES.....</b>		<b>15</b>
<b>APPENDIX A REQUIRED INTERNET COMMUNICATION .....</b>		<b>16</b>
<b>APPENDIX B SAMPLE CONNECTION LOG.....</b>		<b>17</b>

Figure 32 – GATEKEEPER-WP4-GK\_Data\_Centre\_Access\_Site\_To\_Site\_HPE document ToC

The document guides the GATEKEEPER partner users through the steps of getting the necessary software to setup the S2S VPN connection to the Data Centre for various operating systems. Part of this information has already been discussed in Section 2.1.3.1.

**This document is marked as confidential because it contains Data Centre details that must not be made public.**

### 3.2 Continuous Integration and Continuous Delivery

Since the implementation activities related to the CI/CD task have been delivered we released a manual for CI/CD attached in Appendix A.

In the manual we describe a high-level workflow for developers and present a demo to get started with a sample micro-service. We go deep in the use of the versioning tool, the CI/CD tool and the Seed Job to create automatically the build, deploy and security pipelines. Below we report the agenda of the webinar that HPE delivered to the GATEKEEPER partners (developers):

### SECURE CI/CD PLATFORM

#### DEVOPS FOR GATEKEEPER PLATFORM – WEBINAR AGENDA



- **Pre-requisites**
- **Quick hands-on**
  - CI/CD for GATEKEEPER
  - High-level workflow for developers
  - Demo: how to get started with your own micro-service
- **All the details**
  - Versioning Tool: GitLab
  - CI/CD Tool: Jenkins
  - Security analysis
  - Tuning the seed job output
    - Build Pipeline
    - Deploy Pipeline
    - Security Pipeline

Figure 33 – Agenda HPE CI/CD webinar

To use this platform for CI/CD this webinar explains the whole steps that a user have to follow:

- Log in to the Web applications;
- Create a project into GitLab;
- How initialize pipelines with Seed Job in Jenkins;
- Run the generated CI/CD pipelines;
- Generate a security report.

## 4 Conclusions

This deliverable provided the description of the result of the activities spent for the setup and operation of the GATEKEEPER Data Centre by HPE to support the project consortium. It described the current data centre layout, the organizational and technical security measures in place, and the supporting services, including CI/CD tools, container orchestration engine for running the GATEKEEPER Platform, and the Support and Ticketing System.

For the upcoming period, we plan to continue operating the Data Centre and provide support to partners. We will also put effort in maintaining and improving the overall security posture of the data centre, by patching and updating already in place tools and evaluating new countermeasures to lower the chances of successful cyberattacks.



## 5 References

- [1] Flex Fabric Virtual Technology Configuration, [https://support.hpe.com/hpesc/public/docDisplay?docId=a00050312en\\_us](https://support.hpe.com/hpesc/public/docDisplay?docId=a00050312en_us)
- [2] HPE Synergy - composable bladed infrastructure, [https://www.hpe.com/emea\\_europe/en/integrated-systems/synergy.html](https://www.hpe.com/emea_europe/en/integrated-systems/synergy.html)
- [3] oVirt - free open-source virtualization solution for enterprise, <https://www.ovirt.org>
- [4] OKD - community distribution of Kubernetes, <https://www.okd.io>
- [5] Red Hat OpenShift - hybrid cloud platform, <https://www.openshift.com>
- [6] CentOS, Community Enterprise Operating System, <https://www.centos.org>
- [7] Kubernetes - production-grade container orchestration, <https://kubernetes.io>
- [8] HPE Ezmeral, Run, manage, control and secure the apps, data and IT that run your business—from edge to cloud, <https://www.hpe.com/ezmeral>
- [9] Docker, Open Source containers, <https://www.docker.com/community/open-source>
- [10] HPE Nimble, storage solution, <https://www.hpe.com/us/en/storage/nimble.html>
- [11] HPE StoreOnce, backup solution, <https://www.hpe.com/us/en/storage/storeonce.html>
- [12] HPE Networking Switches, network solution, [https://www.hpe.com/emea\\_europe/en/networking/switches.html](https://www.hpe.com/emea_europe/en/networking/switches.html)
- [13] IEEE 802.1Q, Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks, [https://standards.ieee.org/standard/802\\_1Q-2018.html](https://standards.ieee.org/standard/802_1Q-2018.html)
- [14] IEEE 802.3, Standard for Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications-Aggregation of Multiple Link Segments, [https://standards.ieee.org/standard/802\\_3ad-2000.html](https://standards.ieee.org/standard/802_3ad-2000.html)
- [15] HPE Proliant DL Servers, rack-optimized secure industry-standard servers, <https://www.hpe.com/us/en/servers/proliant-dl-servers.html>
- [16] Bareos, Open Source Data Protection, <https://www.bareos.org>
- [17] Synopsis Black Duck Open Hub, <https://www.openhub.net>
- [18] Git, distributed version control, <https://git-scm.com>
- [19] Linux KVM, Kernel-based Virtual Machine, <https://www.linux-kvm.org>
- [20] VMware ESXi, Bare Metal Hypervisor, <https://www.vmware.com>
- [21] Xen, Type-1 Virtual Machine, <https://xenproject.org>
- [22] FreeBSD Chroot Jails, [https://docs.freebsd.org/en\\_US.ISO8859-1/books/handbook/jails.html](https://docs.freebsd.org/en_US.ISO8859-1/books/handbook/jails.html)
- [23] Solaris Zones, Oracle Solaris Zones Introduction, [https://docs.oracle.com/cd/E36784\\_01/html/E36848/zones.intro-1.html](https://docs.oracle.com/cd/E36784_01/html/E36848/zones.intro-1.html)
- [24] Virtuozzo Containers, product retired, <https://www.virtuozzo.com/support/all-products/virtuozzo-containers.html>
- [25] OpenVZ, Open source container-based virtualization for Linux, <https://openvz.org/>
- [26] Cgroups (previously process containers), <https://lwn.net/Articles/236038/>
- [27] Linux Containers (LXC) project, Infrastructure for container projects, <https://linuxcontainers.org>
- [28] Docker Swarm, Swarm mode key concepts, <https://docs.docker.com/engine/swarm/key-concepts>
- [29] Etcd, a distributed, reliable key-value store for the most critical data of a distributed system, <https://etcd.io/>
- [30] Jenkins, free and open source automation server, <https://www.jenkins.io/>
- [31] Source-To-Image (S2I), toolkit and workflow for building reproducible container images from source code, <https://github.com/openshift/source-to-image>
- [32] Checkmk Raw Edition, <https://checkmk.com/product/raw-edition>

- [33] GitLab roles, <https://docs.gitlab.com/ee/user/permissions.html>
- [34] GDPR, regulation 2016/679, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [35] Suricata, opensource threat detection engine, <https://suricata.io/>
- [36] ClamAV, open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats, <https://www.clamav.net/>

## Appendix A Annexes

The following documents are released as confidential documents restricted only for members of the consortium (including the Commission Services):

- Slideset of the CI/CD Webinar held : GATEKEEPER-WP4-GK\_CI-CD\_Webinar\_HPE.pptx
- Document about how to setup a S2S VPN: GATEKEEPER-WP4-GK\_Data\_Centre\_Access\_Site\_To\_Site\_HPE\_v1.05.pdf

## Appendix B User Registration Form Text for S2S VPNs

For the sake of readability and accessibility, we report the full text of the User Registration Form shown in Figure 3 – Preface of the S2S User Registration Form.

GATEKEEPER

HPE Data Centre Site-To-Site

Remote Access Request

*Please complete the following form. Your data will be collected by HPE as GATEKEEPER partner for the sole purposes of account management and user access provisioning to HPE Data Centre infrastructure hosting the GATEKEEPER project services. You must give your consent to HPE for processing your data according to the HPE Privacy policy available using the link located at the bottom of the form. The HPE responsibilities are described in the link.*

*This computer network is provided for authorised use only. Users have no explicit or implicit expectation of privacy. Any or all uses of systems of this computer network and all data in this Data Centre may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised sites and law enforcement personnel, as well as authorised officials of other agencies. By accessing to this computer network, the user consent to such disclosure at the discretion of authorised site personnel. Unauthorised or improper use of this network may result in administrative disciplinary action, civil and criminal penalties. By accessing to this computer network, you indicate your awareness of and consent to these terms and conditions of use. Users are responsible for ensuring that they act in accordance with this policy and other policies and legislation applicable to the HPE network.*

*Please note that by submitting this form you also agree to have your activities on HPE Data Centre monitored for compliance and security purposes. You must not disable (or attempt to) or change any security control, as well as respect the assigned privileges and not escape the perimeter of your role.*

*Should you have any inquiry please contact HPE project partner for further information.*

*Technical details about how to access HPE Data Centre services are published on Alfresco project document management system. You will receive an email as soon as your access will be granted with more information.*

*Notice: it is strictly forbidden to share this registration link outside involved GATEKEEPER project partners.*

HPE GATEKEEPER Team

---

<https://www.gatekeeper-project.eu/>

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 857223*

## Appendix C User Registration Form Fields for S2S VPNs

For the sake of readability and accessibility, we report the fields of the Partner Registration Form for S2S VPNs shown in Figure 4 – Fields of the S2S User Registration Form.

\* Required

1. Partner Single Point of Contact - First Name \*  
*Please insert your name and optional middle name*
2. Partner Single Point of Contact – Surname \*  
*Please insert your surname*
3. Partner Single Point of Contact - E-Mail Address  
Please specify the contact e-mail address (e.g., [user@example.org](mailto:user@example.org)). This e-mail address will be used only for communications about HPE data centre and site-to-site connection. Only valid GATEKEEPER partner e-mail address will be accepted.
4. Organisation Name \*  
*Please specify your organisation: **here we show a drop down list of consortium partners' acronyms***
5. I have read and I accept the HPE Privacy policy for personal data collection available at the URL:  
[https://www.hpe.com/emea\\_europe/en/legal/privacy.html](https://www.hpe.com/emea_europe/en/legal/privacy.html) \*

## Appendix D Internal HPE Portal home page

For the sake of readability and accessibility, we report the text of the Internal HPE Portal home page shown in Figure 6 – Internal HPE Portal (in **green** the additions with respect to D4.1).

HPE SECLAB	
This page provides helpful links for HPE SECLAB made for GATEKEEPER.	
<b>Identity Management</b> Go here to manage your user account. Access Password Change: <i>[internal link]</i> You can change your password or reset it if it expires. <b>SECLAB Internal Certification Authority</b> Import the HPE SECLAB into your browser or other services. Download the SECLAB Internal CA to trust the provided services: <i>[internal link]</i>	<b>For Developers</b> Tools provided for authorised developers only.  Access OKD Console: <i>[internal link]</i> OKD is a distribution of Kubernetes optimized for continuous application development and multi-tenant deployment.  <b>Access HPE Ezmeral Console for Big Data/AI/ML: <i>[internal link]</i></b> <b>HPE Software platform designed to run both cloud-native and non-cloud native applications in containers. More info.</b>  <b>Access CI/CD Tools</b> <b>GitLab: <i>[internal link]</i> - source code repository</b> <b>Nexus: <i>[internal link]</i> - container registry</b> <b>Jenkins: <i>[internal link]</i> - build and deploy automation server</b> <b>Tools to enable project software development.</b>



<b>Important notice</b> <p>This computer network is provided for authorised use only. Users have no explicit or implicit expectation of privacy. Any or all uses of systems of this computer network and all data in this Data Centre may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised sites and law enforcement personnel, as well as authorised officials of other agencies. By accessing to this computer network, the user consent to such disclosure at the discretion of authorised site personnel. Unauthorised or improper use of this network may result in administrative disciplinary action, civil and criminal penalties. By accessing to this computer network, you indicate your awareness of and consent to these terms and conditions of use. Users are responsible for ensuring that they act in accordance with this policy and other policies and legislation applicable to the HPE network.</p>	<b>About this Project</b> <p>This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857223</p> <p>[ GATEKEEPER ]      [ Hewlett Packard Enterprise - HPE ]</p> <p>(c) Copyright 2021 Hewlett Packard Enterprise Development Company, L.P. Valid agreement required.</p>
--	--