Technical Annexes

CINECA

CINECA, November 2025

Sommario

1 Annesso I: HPC service model description

CINECA

CINECA HPC infrastructure: the national HPC infrastructure for research

Service description

Ver 1.0

CINECA, November 2025

Changelog

Version	Data	Author(s)	Change Descripttion
1.0	2025-10-25	HPC Production Team	First complete draft

Definitions and glossary

Term/Acronym	Definition
HPC project	A pool of HPC resources associated to a set specific tasks under the responsibility of a Principal Investigator
Requestor	An individual or entity that initiates a request for services, resources, or information.
Principal Investigator	The person nominated by the Requestor, administrating the HPC Project, contact point for any communication related to the HPC resources, and responsible for assigning any additional collaborator to the project.
Collaborator	Any person given access to the resources of the HPC project and resources by the Principal Investigator via UserDB.
Users	Principal investigators and Collaborators, or, more in general, any person able to access the HPC infrastructure
UserDB	CINECA HPC User Portal for the registration and management of HPC users and projects (https://userdb.hpc.Cineca.it).

Acronyms

Term/Acronym	Definition
AP	Access Policies
CLI	Command Line Interface. A text-based interface used to interact with software and operating systems
DPO	Data Protection Officer
GPU	Graphics Processing Unit. A specialized processor designed to accelerate graphics rendering.
GUI	Graphical User Interface
HPC	High Performance Computing
IaaS	Infrastructure as a Service
PI	Principal Investigator
PII	Personal Identifiable Information
SLA	Service Level Agreement
SLO	Service Level Objective

SLI Service Level Indicator

VM Virtual Machine

Objectives

This document describes the Cineca HPC Infrastructure, and its related services.

By requesting the service, this document becomes part of the formal contract between Cineca and the Requestor. This binds both parties to comply with what is reported below according to their mutual roles and responsibilities.

Service description

Main characteristics and functionalities

Cineca HPC resources are made available to authorized users in a shared environment. Access is provided through a pool of dedicated service nodes, referred to as front-end nodes. The primary access methods are via the SSH protocol or through a graphical interface using a VNC server (RCM service). Large-scale data transfers are managed through dedicated servers, known as data mover nodes, which are equipped with specialized and optimized tools for this purpose.

Access to resources is typically granted through a two-factor authentication (2FA) mechanism and only after the user has registered on the Cineca User Portal (UserDB). Before accessing the HPC systems, the registered user must accept Cineca's access policies, which are available at the following address: https://www.hpc.Cineca.it/access-policy-to-Cineca-supercomputing-facilities/

The personal data collected during registration on the UserDB portal are managed in accordance with ISO 27001 standards. The information notice regarding data processing methods is available at the following link: https://www.hpc.Cineca.it/privacy-notice-for-processing-of-user-data-on-Cineca-userdb-service/

Both aforementioned documents may be amended by Cineca to comply with new laws or ISO standards that may be enacted, as well as to address changes in the security conditions of Cineca's systems. In such cases, written notice will be provided to the Requestor at least two weeks in advance, during which the previous documents will remain in effect. Within this period, the Requestor may request termination of the contract without penalty, or may agree with Cineca on new, customized terms.

Parallel filesystems hosted on Cineca HPC machines share the same logical structure and file system definition. The available storage areas can have multiple definitions/purposes:

- **temporary**: data are accessible for a defined time window, after the data are not used for a predetermined time, they are automatically canceled;
- **permanent**: data are accessible for a certain amount of time after the end of the project or the expiration of the username.

Storage areas can be also:

- **user specific**: each user has exclusive data area;
- **shared**: area accessible by all collaborators belonging the same project;
- **open**: area accessible by all users of an HPC system.

In general, Cineca filesystem can host Users' data on these partitions:

Name	Availability	Read	Write	Quota	Backup	Note
$HOME	permanent	user specific	user specific	50 GB	Daily	More capacity is possible under request
$WORK	permanent	shared	shared	1 TB	No	More capacity is possible under request
$FAST	permanent	shared	shared	1 TB	No	Only on specific systems; based on SSD disks; more capacity is possible under request
$SCRATCH	Temporary	user specific	user specific	No quota	No	Files older than 40 days are automatically deleted
$TMPDIR	temporary	shared	shared	Depending on the machine	No	directory removed at job completion
$PUBLIC	permanent	open	user specific	50 GB	No	
$DRES	permanent	shared	shared	Defined by project	No	

Daily backups guarantee the $HOME filesystem. In particular, the daily backup procedure preserves a maximum of three different copies of the same file. Older versions of files are kept for 1 month. The last version of deleted files is kept for 2 months, then definitely removed from the backup archive.

WORK, FAST and DRES are usually kept up to six months after the expiration of the related project. HOME and PUBLIC are maintained for six months after the expiration of the username that happens one year after the removal of the WORK/FAST/DRES area of the last project.

Roles and responsibilities

Each allocation on the machine is under the responsibility of:

- one Principal Investigator (PI): lead person in the team to whom the HPC resources are assigned, responsible for managing collaborators and contact point for any request related to the usage of the resources or the HPC services.
- Collaborators: any other person in the team, nominated by the PI, who can access the HPC resources.

The UserDB web portal contains all the active and expired projects and their related PI and collaborators

Mutual Responsibilities of the Users and Provider (Shared Responsibility Model)

Users Responsibilities and Limitations:

- **Credential Management:** The User is responsible for safeguarding access credentials to the HPC machines and any related services.
- **Backup**: The User has the responsibility to backup the data hosted in any partition other than $HOME since they are not automatically backed up. Although Cineca undertakes to keep user data secure, it shall not be held liable for any loss of data.
- **Communication**: The User is responsible for subscribing to and following the "HPC News",

where communications on the HPC services are sent from CINECA staff.

Provider Responsibilities and Limitations:

- **Security and Resilience:** The Provider is responsible for managing the security and resilience of the HPC systems and the underlying hardware and software infrastructure.

- **Service Levels and Indicators:** The Provider is responsible for collecting service levels (SLAs) and service quality indicators (SLIs).

- **Data Breach Notification:** The Provider must notify the Operator of any relevant PII data breaches (and provide the contact information for such notifications).

- **Contract Termination:** The Provider must notify the Requestor and Operators of the contract termination process, including the timing for providing information for data and configuration export in the required open format. The Provider must also specify the timeline for the permanent removal of the Requestor and Operators data post-termination.

- **Maintenance Communication:** The Provider must communicate any maintenance interventions for scheduled maintenances, the communication is given with one week notice.

Software Licenses - Reciprocal Responsibilities

CINECA is responsible for all licenses related to the software installed on the physical platform used for delivering the HPC services, including virtualization systems, storage, networking, and management, monitoring, and logging portals.

Conversely, the Users are responsible for all necessary licenses for the software installed on the HPC systems by them. It is the User's responsibility to verify that the licensing of the products used complies with the rules imposed by the software manufacturer and to ensure compliance, directly addressing any potential anomalies and security issues.

Service Location

The primary sites of the HPC service are located at:

- CINECA data centers in Tecnopolo DaMa (Bologna, Italy)
- CINECA data centers in Tecnopolo Napoli (Napoli, Italy)
- CINECA data centers in Casalecchio di Reno (Bologna, Italy)

CINECA is committed to notifying the Requestor with adequate advance notice of any changes to the location of the site.

Event Logging

By default, the logging of components managed by CINECA is configured to be sent to and retained on the log management platform for a minimum of six months or as otherwise required by applicable Italian law. The Log Management platform is not directly accessible to the user.

Backup

Daily backups guarantee only the $HOME filesystem unless otherwise specified. In particular, the daily backup procedure preserves a maximum of three different copies of the same file. Older versions of files are kept for 1 month. The last version of deleted files is kept for 2 months, then definitely removed from the backup archive.

Although Cineca undertakes to keep user data secure, it shall not be held liable for any loss of data.

Service Monitoring

CINECA performs monitoring of the service components under its responsibility through its monitoring platform, which utilizes active probes to verify the availability of the components it manages. Upon request, if possible, notifications of significant service events can be sent to the Requestor via email or other agreed-upon methods.

Scheduled and Unscheduled System Maintenance

CINECA reserves a window to perform scheduled manual or automatic updates related to its server systems (management systems). CINECA commits to keeping the service interruptions to the minimum possible. Generally, interventions that do not impact on the functionality of the HPC systems are not notified in advance.

Any maintenance of infrastructural components that may impact production will be communicated via HPC News with one week's notice prior to the planned date, unless urgent security-related interventions are required. In such cases, maintenance may be conducted without prior notice if deemed critically necessary, with notification provided post-event.

Incident Management and Data Breach

CINECA handles incidents on the HPC infrastructure reported via email (at superc@Cineca.it) and recorded through the ticketing system portal, available 24/7, 365 days a year.

All incoming requests are automatically forwarded to the first level queue; within the Next Business Day the requests are either resolved or moved to the Second Level Queue. Requests in the Second Level Queue will have a first exhaustive reply within one Business week.

Incidents may also be detected through CINECA's monitoring systems. Communication with the Requestor regarding incidents is managed through the issue tracker if the incident was reported by the Requestor. Upon request, CINECA can provide a summary of the Incident Report once it is officially closed.

Reporting and Mutual Responsibilities

For the HPC services referenced in this document, Provider responsibilities cover the incidents related to infrastructure and management interfaces, as well as logging services. This includes any reports of credential theft that require prompt action from the provider (e.g., blocking or resetting credentials).

If an infrastructure incident affects information security (threatening or causing loss of confidentiality, integrity, or availability within the provider's scope), CINECA will initiate a second level of escalation managed by its CERT*. This team will analyze the incident to identify the attack vector, provide workarounds, and implement permanent security measures or additional improvements as part of Problem Management (Lessons Learned).

A particular case of security incidents is the handling of Data Breaches, where personal or sensitive data is affected. These incidents follow a dedicated reporting channel (Infrastructure Services - SD Data Breach on customerportal.Cineca.it), managed by CINECA's DPO, and may also involve relevant authorities.

* Computer Emergency Response Team

Key performance Indicators (KPI), Service Level Agreements and Target Values

KPI, SLI, SLA, and SLO for the HPC Infrastructure

CINECA will apply this Service Level Agreements to all its supercomputers:

No	SLI	Description	SLA	SLO	Period for computing of figure
1a	Availability of the supercomputer	Fraction of time the system is usable (able to support production runs) and available to users excluding planned maintenances Includes: files systems, home directories, login nodes, access network.	> 95% (monthly basis) for the first 3 months of operation >97% (monthly basis) for the remaining of the operational period	>98% (monthly basis	Monthly
1b	Availability per system partition	Average capacity (percentage of nodes) available per partition, excluding planned maintenances	> 75% (monthly basis) for the first 3 months of operation >85% (monthly basis) for the remaining of the operational period	>95% (monthly basis)	Monthly
2.	Unscheduled outages and maintenance.	Measured in days per year. Maintenance is considered as scheduled if users are warned at least 1 week in advance, otherwise it is considered unscheduled outage or maintenance. Maintenance actions targeting high severity security incidents are not taken into consideration.	Not more than 7 calendar days per year	Not more than 2 calendar days per year	Yearly
3.	Availability of the critical auxiliary IT equipment	IT equipment necessary for the usage of the supercomputer (example: external network access, storage, fabric, management network, …)	> 95% (yearly basis) for the first year of operation >97% (yearly basis) for the remaining of the operational period	>98% (yearly basis)	Yearly
4	Availability of external connectivity	External backbone connectivity to GÉANT.	> 99 % on a yearly basis No more than 5 days of	> 99 % on a yearly basis No more than 1 days of	Yearly

			maintenance per year	maintenance per year	

Furthermore Cineca will try to maintain the following Service Level Objectives:

No	SLI	Description	SLO	Period for computing of figure
3.	Stability of performances of the supercomputer	Regular execution of a standard set of benchmarks selected by Cineca.	> 90% of the performances measured after the installation of the supercomputer	Yearly
5.	Usage of the Supercomputer	(excluding unavailability and scheduled maintenance periods) Percentage of compute hours consumed per partition for the complete system.	> 75% on a monthly basis	Monthly
6.	Availability of the facility	Refers to availability of key facility equipment including: Cooling, power supply, fire security.	> 99 % on a yearly basis No more than 5 days of maintenance per year	Yearly
8.	User Satisfaction	Measure of user satisfaction via user survey. The survey should include Handling of Tickets and overall quality of responses to user requests.	Overall user satisfaction must be over 3 in a scale 0-5. Value 3 indicates an acceptable degree of satisfaction; users are reasonably happy with the environment and services, and no changes are required although there might still be room for improvement. Values below 3 indicate dissatisfaction; improvements or other actions are desirable. Values above 3 indicate level of exceptional appreciation and satisfaction.	Yearly

The supercomputer services provided to users must be available 24 hours, 7 days per week, except when there is maintenance. A service can be requested during support hours.

Availability is determined by the percentage of fully usable time (able to operate in normal performance) and available to users. It must include at least the compute nodes, login nodes, network access, file systems and access to home directories.

Cineca will seek 100% availability, and meet the availability defined in the SLOs but clearly only SLA are considered for the purposes of this agreement.

Cineca will calculate “Service Unavailability” in a calendar month. “Service Unavailability” consists of the number of minutes that the service was not available to Users, and includes unavailability associated with any maintenance at the hosting site other than Scheduled or Security Maintenance. Outages will be counted as Service Unavailability even if users do not open an incident with support during or after the outage. Service unavailability will not include Scheduled or Security Maintenance, or any unavailability resulting from:

- acts or omissions of the Requestor or any use or user of the service authorized by the Requestor;
- deliberate acts or gross negligence of a User or an End User or reasons of Force Majeure.

In the case of a malfunction involving a total unavailability exceeding 24 hours of the supercomputer or its IT environment, Cineca must inform via HPC News the Users no later than 48 hours (2 working days) after the commence of the incident and a crisis unit would be set up to solve the issue.

SLA applicability limits

The service levels (SLA and SLO) mentioned above do not apply in cases of service interruptions caused by:

- Unavailability due to actions not directly attributable to CINECA (force majeure, e.g., strikes, demonstrations blocking transportation routes; road accidents; wars and acts of terrorism; malicious cyber-attacks; natural disasters such as floods, storms, hurricanes, etc.). Disaster conditions.
- Unavailability of network connections not directly attributable to CINECA.
- Unavailability of the Requestor's network connections.
- Hardware/software issues on the Requestor's workstations or servers.
- Non-compliance with the AP (Access Policies) by the Requestor, affecting shared services.

Extraordinary downtimes are the result of interventions that CINECA deems urgently necessary, at its sole discretion, to mitigate threats to the security and/or stability and/or confidentiality and/or integrity of the infrastructure and/or servers and/or data and/or information.

Application or system support for malfunctions of hardware or software not provided or not directly managed by CINECA is explicitly excluded.

CINECA assumes no contractual or extra-contractual liability concerning hardware or software products made by third parties. The responsibilities related to third-party products used by CINECA to deliver the service remain entirely and exclusively governed by the warranties provided by the manufacturers.

SLA Measurement and Reporting to the Requestor

As part of its service management system, CINECA continuously measures the KPIs, evaluates them, and uses the data to guide any necessary corrective actions.

Support SLA

CINECA provides technical support for the service. The Principal Investigator designated by the Requestor independently determines the list of their personnel authorized to access the Support service.

Support can be engaged for:

- Reporting incidents or malfunctions (anomalies)
- Requests for configuration changes or other standard requests

Support is provided by sending an email at superc@Cineca.it which will automatically create an issue in the CINECA HPC Trouble Ticketing System (more details on the management of requests are reported in section 3.1.12).

Support service levels

The following indicators, thresholds, and applicable penalties are identified (applicable only to Production environments):

Definitions for Support SLAs	
Observation Period	The observation period for measuring the SLAs is set at 1 consecutive calendar month, starting from January.
Measurement Window	7x24x365
Incident or Support Request Classification	Incident reports or support requests are classified according to a Priority level, determined based on Severity and Urgency
Reaction Time	This is the time elapsed between the first documented attempt by the Requestor to report the issue and the issuance of the Trouble Ticket, along with the corresponding notification.
Support SLA for Incident or Anomaly Reports	**Incidents:** • First Level Queue: within the Next Business Day the requests are either resolved or moved to the Second Level Queue • Second Level Queue: a first exhaustive reply within one Business week.
Support SLA for Support Requests	**Requests:** • First Level Queue: within the Next Business Day the requests are either resolved or moved to the Second Level Queue • Second Level Queue: a first exhaustive reply within one Business week.

Service Availability Hours

The service is available 24 hours a day (24/7). Support must be available from 8:30 AM to 6:30 PM (CET/CEST), Monday through Friday, except when the facilities are closed due to holidays, strikes, administrative closings, or inclement weather. A service can be requested or an Incident reported by Mail at any time. Incidents reported or services requested outside the working hours will be served at the next scheduled working day.

Contact Points for Issue Reporting

Via e-mail at: superc@Cineca.it interfaced with a ticketing system available 7x24x365.

Personal Data Management Policies

Common personal data are requested for the administrative registration of contracts and service delivery. Data is collected through the UserDB activation form. Data are stored on UserDB portal solely for the purpose of service provision and will not be shared with third parties.

Further Information

None

Annesso II: HPC cloud model description

CINECA

Cineca HPC cloud:
the national cloud for research

Service description

Ver 1.4

By HPC Cloud Support Team

Cineca, October 2025

Changelog

Version	Data	Author(s)	Change Description
1.0 - Final	2024-10-07	HPC Cloud Team	First complete draft
1.1 - Updated	2025-02-13	HPC Cloud Team	Updated backup section Updated links to HPC User Guide
1.2 - Updated	2025-05-30	D. Testi	Updated links to the HPC User Guide
1.3 - Updated	2025-09-04	G. Muscianisi	Updated links to the HPC User Guide in the footnotes
1.4 - Updated	2025-10-23	D. Testi	Added as Annex the definition of Tenant Availability

Definitions and glossary

Term/Acronym	Definition
Cloud project	Virtual infrastructure, also known as "tenant", associated to a pool of cloud resources (vCPUs, storage, floating IPs).
Tenant	Synonym of Cloud project.
Requestor	An individual or entity that initiates a request for services, resources, or information.
Principal Investigator	The person nominated by the Requestor, administrating the Cloud project (tenant), contact point for any communication related to the Cloud resources, and responsible for assigning any additional collaborator to the project.
Collaborator	Any person given access to the administration of Tenant and resources by the Principal Investigator via UserDB.
Operator	Any person (Principal Investigator, Collaborator) with access to the Tenant administration and related resources.
UserDB	Cineca HPC User Portal for the registration and management of HPC users and projects (https://userdb.hpc.Cineca.it).

Acronyms

Term/Acronym	Definition
AP	Access Policies
CLI	Command Line Interface. A text-based interface used to interact with software and operating systems
DPO	Data Protection Officer
GPU	Graphics Processing Unit. A specialized processor designed to accelerate graphics rendering.
GUI	Graphical User Interface
HPC	High Performance Computing
IaaS	Infrastructure as a Service
LB	Load Balancer

PaaS	Platform as a Service
PI	Principal Investigator
PII	Personal Identifiable Information
SLA	Service Level Agreement
SLO	Service Level Objective
SLI	Service Level Indicator
vCPU	Virtual Central Processing Unit. A virtualized CPU that is allocated within a cloud or virtualized environment
VM	Virtual Machine

Objectives

This document describes the HPC Cloud Infrastructure as a Service, through which the Operator can define its own virtual infrastructures (in a shared environment), in cloud IaaS mode, and manage it in total autonomy, as if it was his/her own (virtual) infrastructure.

By requesting the service, this document becomes part of the formal contract between Cineca and the Requestor. This binds both parties to comply with what is reported below according to their mutual roles and responsibilities.

Service description

Main characteristics and functionalities

The service operates under the IaaS model, organized through tenants, which are logically isolated environments within a multi-tenant cloud architecture. Each tenant, representing a cloud project, is provided with a budget of virtualized resources within Cineca's HPC Cloud infrastructures. Tenants, and associated resources, are allocated based on contracts or agreements with Cineca (e.g., participation in European or ISCRA projects). Each tenant's configuration within the virtual infrastructure is fully segregated from other tenants.

Cineca's HPC Cloud is powered by OpenStack*, an open-source cloud software that provides the underlying infrastructure for this IaaS service. OpenStack offers a range of services to manage and utilize virtual resources within the cloud.

Users can interact with the infrastructure through any OpenStack client, enabling efficient resource management and customization according to user needs.

For a full description of Cineca's HPC Cloud Infrastructures, the IaaS features and list of the OpenStack services currently available, we refer the reader to the official HPC User Guide.

Roles and responsibilities

Each tenant does not have a designated administrator; instead, it is assigned a pool of Operators, which includes:

- one Principal Investigator (PI): lead person in the team to whom the cloud resources are assigned, responsible for managing collaborators, with administration access to the allocated tenant, and contact point for any request related to the usage of the resources or the cloud services.

* https://www.openstack.org/

- Collaborators: any other person in the team, nominated by the PI, who can access the tenant administration and the associated cloud resources.

PI and collaborators are specified in the corresponding entries on the UserDB portal (Cineca HPC User Portal, where users and cloud projects are registered).

PI and collaborators share the same roles within the OpenStack tenant (both tenant administrators), and they authenticate in the OpenStack dashboard via Cineca HPC Identity Provider (IdP), specifically the KeyCloak instance at sso.hpc.Cineca.it.

Mutual Responsibilities of the Operators and Provider (Shared Responsibility Model)

Operators' Responsibilities and Limitations:

- **Credential Management:** The Operator is responsible for safeguarding access credentials to the management system and for managing permissions within his/her tenant, including lifecycle management, revocation, and authorizations.
- **Logical Security:** The Operator is responsible for managing the logical security (access controls and firewalls) of the virtual infrastructure defined within their tenant, including logging and monitoring access.
- **Software security:** The Operator is responsible for maintaining the software security (Operative System update, security patch, fix, etc.) within his/her tenant.
- **Backup**: The Operator has the responsibility to perform snapshots of virtual machines and data volumes and save them in separate storage according to the appropriate needs.
- **Communication**: The Operator is responsible for subscribing to and following the "HPC News", where communications on the HPC services are sent from Cineca staff.

Provider Responsibilities and Limitations:

- **Security and Resilience:** The Provider is responsible for managing the security and resilience of cloud administration systems and the underlying physical infrastructure.
- **Service Levels and Indicators:** The Provider is responsible for collecting service levels (SLAs) and service quality indicators (SLIs).
- **Sub-Contractor Notification:** The Provider must notify the Operator of any sub-contractors who may access personal data (PII) and any countries from which these sub-contractors might process data. The Provider should formalize the appointment of another data processor for these sub-contractors, including minimum technical measures for data access.
- **Data Breach Notification:** The Provider must notify the Operator of any relevant PII data breaches (and provide the contact information for such notifications).
- **Contract Termination:** The Provider must notify the Requestor and Operators of the contract termination process, including the timing for providing information for data and configuration export in the required open format. The Provider must also specify the timeline for the permanent removal of the Requestor and Operators data post-termination.
- **Maintenance Communication:** The Provider must communicate any maintenance interventions for scheduled maintenances; the communication is given with one week notice.

Service usage

The HPC Cloud service enables the Operator to independently create and manage one or more Cloud projects (tenants) acting as proper virtual infrastructures. Each tenant is composed of virtual resources such as vCPUs, GPUs, storage areas, networks. The Operator is assigned a pool of resources defined in terms of:

- Number of vCPUs
- GB of RAM
- GB of storage
- Number of public IP addresses (floating IPs)

On request, the Operator can be also granted

- Number of GPUs
- Additional storage where to store snapshots

Upon accessing the Cloud portal (OpenStack Horizon dashboard) with HPC credentials, within the assigned tenants, the PI and collaborators can autonomously create and manage all components of their virtual infrastructure (VMs, Virtual Networks, Security Policies, Load Balancer Policies, and so on) by means of the GUI or CLI, in compliance with the Access Policies (AP) accepted at the time of registration on UserDB (see Appendix A).

For complete technical documentation, please refer to the User Guide documentation (HPC Cloud UserGuide).

Security guidelines for service usage

The security guidelines for the services or applications deployed on the tenant, which are the Operators' responsibility, are beyond the scope of this document. Regarding the use of the service, we recommend following the security guidelines described in the HPC Cloud Security Guidelines section of the User Guide.

Software Licenses - Reciprocal Responsibilities

Cineca is responsible for all licenses related to the software installed on the physical platform used for delivering the HPC Cloud services, including virtualization systems, storage, networking, and management, monitoring, and logging portals.

Conversely, the Operator is responsible for all necessary licenses for the software installed on the virtual machines managed by them. It is the Operator's responsibility to verify that the licensing of the products used complies with the rules imposed by the manufacturer for virtual environments and to ensure compliance, directly addressing any potential anomalies and security issues. The Operator is not allowed to instantiate virtual machines with Microsoft Windows Operating System.

Service Location

The primary site of the service is located at the Cineca headquarters in Casalecchio di Reno (Bologna, Italy). Cineca is committed to notifying the Requestor with adequate advance notice of any changes to the location of the site.

Event Logging

By default, the logging of components managed by Cineca is configured to be sent to and retained on the log management platform for a minimum of six months. The Log Management platform is not directly accessible to the user.

The Cloud portal (OpenStack Horizon dashboard) provides the ability for the tenant administrators to view relevant events, such as configuration operations, powering on, powering off, and other activities related to virtual machines.

The Operator is responsible for managing logs produced by software systems installed on the VMs.

Backup

Cineca provides a centralized and automated backup system for the virtualization layer and its configuration. Backup of virtual machines, data volumes/shares are not performed by Cineca and are under the responsibility of the Operators based on their needs. The functionality to create backups and snapshots is available both via the OpenStack Horizon dashboard and CLI, but Operators should be aware that such snapshots and backups are currently stored on the same HPC Cloud infrastructure.

Service Monitoring

Cineca performs monitoring of the service components under its responsibility through its monitoring platform, which utilizes active probes to verify the availability of the components it manages. Upon request, if possible, notifications of significant service events can be sent to the Requestor via email or other agreed-upon methods.

Regarding the usage statistics of VM resources (vCPUs, storage, floating IPs), the PI and collaborators of a tenant can overview the usage of the virtual resources through the OpenStack Horizon Dashboard.

Scalability and Sustainable Load

The scalability of the service is manual and is requested by the Requestor or the Principal Investigator based on their service needs (in the framework of the signed contract/agreement). Scalability can be achieved through increasing the resources of existing VMs or adding new Virtual Machines.

Requests for resource increases (vCPUs, storage and number of floating IPs) can be made by sending a request to the Support Team (email at superc@Cineca.it). Cineca will assess the request (in the framework of the signed contract/agreement) with respect to the current capacity of the HPC Cloud Infrastructure.

Scheduled and Unscheduled System Maintenance

Cineca reserves a window to perform scheduled manual or automatic updates related to its server systems (management systems). Cineca commits to keeping the service interruptions to the minimum possible. Generally, interventions that do not impact the functionality of the tenant's VMs but only affect management systems (e.g., access portals, monitoring systems, metric collection, etc.) are not notified in advance.

Any maintenance of infrastructural components that may impact production will be communicated via HPC News (or via ticketing system) with one week's notice prior to the planned date, unless urgent security-related interventions are required. In such cases, maintenance may be conducted without prior notice if deemed critically necessary, with notification provided post-event.

Information Security and Regulatory Compliance

For the HPC Cloud services it provides, Cineca is certified in accordance with ISO/IEC 27001:2022[*], as Cloud Service Provider for projects in the Life Science domain. The certification is reaffirmed annually through audits conducted by the Certifying Authority.

In compliance with these standards, Cineca implements a range of technical and organizational measures to ensure information security, GDPR compliance, adherence to Minimum Security Measures for Public Administrations, and AGID requirements for Public Administration Cloud Service Providers.

[*]https://www.CINECA.it/sites/default/files/2024-06/ISO-27001-IT319237-ITA.pdf

The certification does not cover projects in IaaS model, but many of the security measures in place are valid for all Cloud projects hosted on the Cineca HPC Cloud infrastructure:

- **24x7x365 Security**: Comprehensive physical security is maintained at the datacenters and offices where employees are located across all sites.
- **Datacenter Architecture and Evolution**: The design of the datacenter and its evolution ensure operational continuity for all essential layers of service delivery, including facility infrastructure, cooling systems, electrical continuity, network, and farm RAID storage.
- **Protection Systems**: Implementation of sensors and protection systems (e.g., fire detection, flood prevention, temperature control), along with redundant electrical continuity and cooling systems.
- **Asset Management**: Centralized management of physical and software components, managed by Cineca through a Configuration Management Database.
- **Continuous Monitoring**: Ongoing monitoring of resources and services to detect critical issues (capacity) and incidents, or to prevent incidents, integrated with alarm systems and trouble ticketing.
- **Access Management**: Control of system and database access, management of utility program access, and governance of system administrators, including password policies and individual accounts.
- **System Hardening**: Implementation of hardening measures for provider systems.
- **Incident Management**: Includes handling security incidents and data breaches, managed by Cineca's CERT and Cybersecurity Team.
- **Segregation**: Strict separation of tenant environments, including logging and management interfaces.
- **System and Software Updates**: Regular updates to systems and software under Cineca's responsibility.
- **Clock Synchronization**: Centralized redundant clock synchronization from authoritative sources (e.g., Istituto Galileo Ferraris). Clock synchronization is ensured by the NTP server (ntp.Cineca.it), which can also be used by Requestor systems.
- **Training and Updates**: Ongoing training and updates for administrative and general staff on skills and operational procedures.

Encryption of data at rest is not implemented at the infrastructural level (storage, database, backup) due to high costs and performance impacts. It is delegated to the application level, where necessary, or to implementation at the virtual layer by the tenant. To encrypt data, the Operator can make use of the OpenStack hypervisor's layer ability to encrypt volumes during creation, on demand (OpenStack Barbican service[*]).

In relation to information security and overall virtual infrastructure management, the Operator's role is emphasized. The Operator is responsible for managing and responding to his/her assets (defined via the OpenStack Horizon Dashboard) and for correctly implementing security through policy definitions. The Operator must adopt measures deemed appropriate to ensure functionality, reliability, integrity, and confidentiality, and implement controls, logging, system updates, and access management as prescribed by current regulations and the Access Policies set by the hosting provider.

Incident Management and Data Breach

Cineca handles incidents on the HPC Cloud infrastructure reported via email (at superc@Cineca.it) and recorded through the ticketing system portal, available 24/7, 365 days a year.

[*] https://docs.hpc.Cineca.it/cloud/tenant_adm/store_sens_data.html

All incoming requests are automatically forwarded to the first level queue; within the Next Business Day the requests are either resolved or moved to the Second Level Queue. Requests in the Second Level Queue will have a first exhaustive reply within one Business week. Specific Cloud related issues are forwarded to the HPC Cloud support Queue.

Incidents may also be detected through Cineca's monitoring systems. Communication with the Requestor regarding incidents is managed through the issue tracker if the incident was reported by the Requestor. Upon request, Cineca can provide a summary of the Incident Report once it is officially closed.

Reporting and Mutual Responsibilities

For the HPC Cloud IaaS service referenced in this document, Provider responsibilities cover the incidents related to infrastructure and management interfaces, as well as logging services. This includes any reports of credential theft that require prompt action from the provider (e.g., blocking or resetting credentials). Incidents occurring within the Operator's machines or related to the Operator's authentication system are excluded from the Provider's responsibility. However, if there is an attack on the Operator's infrastructure (VMs), it can still be reported to Cineca for support in containment or evidence collection (e.g., logs, backups, or forensic clones).

If an infrastructure incident affects information security (threatening or causing loss of confidentiality, integrity, or availability within the provider's scope), Cineca will initiate a second level of escalation managed by its CERT. This team will analyze the incident to identify the attack vector, provide workarounds, and implement permanent security measures or additional improvements as part of Problem Management (Lessons Learned).

If the Provider detects or is informed by third parties of abnormal behaviors from IPs associated with the Operator, Cineca will promptly notify the target Operator by opening a specific issue. Cineca reserves the right to suspend connectivity for the involved IPs if the infrastructure component is at risk or to mitigate adverse effects.

A particular case of security incidents is the handling of Data Breaches, where personal or sensitive data is affected. These incidents follow a dedicated reporting channel (Infrastructure Services - SD Data Breach on customerportal.Cineca.it), managed by Cineca's DPO, and may also involve relevant authorities. The Requestor can open Data Breach issues only if the data loss pertains to data processing for which Cineca is the data controller (e.g., user contact details for the service), given the nature of the IaaS service, which involves only the provision of infrastructure and not the processing of Requestor-owned data.

Activation procedures

The IaaS service provided by Cineca can be accessed following the establishment of a contract between the parties, to which this document serves as an annex.

The service allows the Operators to create their own computing infrastructure within an allocated pool of virtual resources (Cloud IaaS service model). Cineca provides and manages the physical infrastructure that enables the Operators to establish their own virtual infrastructure, which is isolated from that of other Requestors and from Cineca itself.

The Requestor also designates a "Principal Investigator" to whom the personal account for accessing the Cloud management system will be assigned via UserDB. The Principal Investigator is authorized to define authentication and authorization methods for delegating aspects of the management of the Requestor's infrastructure, such as configuring their own Identity Provider, assigning other collaborators to the project, or defining local accounts. In any case, the Principal Investigator assumes

full responsibility for all matters related to these access accounts, including credential expiration and lifecycle management.

Service Activation - Activation Agreement

According to the agreed virtualized resource pool, Cineca will allocate the requested resources on the Cloud infrastructure during the service setup phase, within 15 working days from the duly formalized request (i.e., contract registration), unless otherwise agreed upon by the parties. Following the registration procedure on UserDB*, the Principal Investigator will receive HPC credentials for accessing the service, along with links to the usage and management guides and instructions for changing passwords.

Service Level Agreement (SLA)

Service Class	**Cineca HPC Cloud - IaaS**
Feature / Sub-Feature	• Create and manage VMs within the assigned resources • Complete Operator autonomy through GUI and CLI • Ability to use available virtual networks according to the predefined service topology, with options to implement Load Balancing, or apply firewall rules using security policy groups • Ability to perform Operator-managed VM snapshots independently • Capability to monitor VM status and key usage metrics • Ability to create VMs from standard templates or images provided by Cineca or available to the Operator
Indicator/Measure	Tenant Availability – DIS1 (definition is available in Appendix B)

Measurement Management System	• The service delivery window is 24/7, 365 days a year.
	• Tenant availability will be calculated excluding:
	  ○ Scheduled and extraordinary downtimes requested by Cineca
	  ○ Scheduled and extraordinary downtimes requested by the Requestor
	  ○ Downtimes due to malfunctions not attributable to Cineca
	• Availability is calculated based on measurements taken by Cineca's monitoring infrastructure.
	• Monthly reports on availability will include information on downtimes of the monitoring infrastructure.

Unit of Measure	Percentage
Elementary Data to Record	• Date and time of downtime (to the minute) • Date and time of reactivation (to the minute)
Reference Period	3 months
Measurement Frequency	4 times per year
Sampling Rules	Considered downtimes: • Downtimes that occurred and were resolved within the current observation period

* https://docs.hpc.Cineca.it/general/users_account.html#userdb

	• Downtimes that began in the previous observation period and were resolved in the current period.
Calculation Formula	Necessary Data: • Duration of the downtime • Tenant Availability
Rounding Rules	The percentage should be rounded to the nearest decimal point based on the second decimal: • Round down if the decimal is 0.05 • Round up if the decimal is > 0.05
Targeted SLA availability (threshold value)	DIS1 ≥ 99%
Targeted SLO availability (threshold value)	DIS1 ≥ 99.5%
Contractual Actions	For every 0.1% of availability below the target SLA, an additional service extension will be provided, corresponding to 1% of the due service.

SLA applicability limits

The service levels (SLA and SLO) mentioned above do not apply in cases of service interruptions caused by:

- Unavailability due to actions not directly attributable to Cineca (force majeure, e.g., strikes, demonstrations blocking transportation routes; road accidents; wars and acts of terrorism; malicious cyber-attacks; natural disasters such as floods, storms, hurricanes, etc.). Disaster conditions.
- Unavailability of network connections not directly attributable to Cineca.
- Unavailability of the Requestor's network connections.
- Hardware/software issues on the Requestor's workstations or servers.
- Non-compliance with the AP (Access Policies) by the Requestor, affecting shared services.

Extraordinary downtimes are the result of interventions that Cineca deems urgently necessary, at its sole discretion, to mitigate threats to the security and/or stability and/or confidentiality and/or integrity of the infrastructure and/or servers and/or data and/or information.

Application or system support for malfunctions of hardware or software not provided or not directly managed by CINECA is explicitly excluded.

Cineca assumes no contractual or extra-contractual liability concerning hardware or software products made by third parties. The responsibilities related to third-party products used by Cineca to deliver the service remain entirely and exclusively governed by the warranties provided by the manufacturers.

SLA Measurement and Reporting to the Requestor

As part of its service management system, Cineca continuously measures the service levels, evaluates them, and uses the data to guide any necessary corrective actions.

Support SLA

Cineca provides technical support for the service. The Principal Investigator designated by the Requestor independently determines the list of their personnel authorized to access the Support service.

Support can be engaged for:

- Reporting incidents or malfunctions (anomalies)
- Requests for configuration changes or other standard requests

Support is provided by sending an email at superc@Cineca.it which will automatically create an issue in the Cineca HPC Trouble Ticketing System (more details on the management of requests are reported in section 3.1.12).

Support service levels

The following indicators, thresholds, and applicable penalties are identified (applicable only to Production environments):

Definitions for Support SLAs	
Observation Period	The observation period for measuring the SLAs is set at 1 consecutive calendar month, starting from January.
Measurement Window	7x24x365
Incident or Support Request Classification	Incident reports or support requests are classified according to a Priority level, determined based on Severity and Urgency
Reaction Time	This is the time elapsed between the first documented attempt by the Requestor to report the issue and the issuance of the Trouble Ticket, along with the corresponding notification.
Support SLA for Incident or Anomaly Reports	**Incidents:** • First Level Queue: within the Next Business Day the requests are either resolved or moved to the Second Level Queue • Second Level Queue: a first exhaustive reply within one Business week.
Support SLA for Support Requests	**Requests:** • First Level Queue: within the Next Business Day the requests are either resolved or moved to the Second Level Queue • Second Level Queue: a first exhaustive reply within one Business week.

Service Availability Hours

The service is available 24 hours a day (24/7).

Contact Points for Issue Reporting

Via e-mail at: superc@Cineca.it interfaced with a ticketing system available 7x24x365.

Personal Data Management Policies

Common personal data are requested for the administrative registration of contracts and service delivery. Data is collected through the service activation form. Data are stored on Cineca's information systems solely for the purpose of service provision and will not be shared with third parties.

Further Information

Quality of Service Indicators:

Code	SLI	Description	Value
SLI1	Tenant Availability	The percentage of time in each reference period during which the Tenant is accessible and usable, excluding scheduled service downtimes.	99% monthly, excluding downtimes listed in section 3.1. Measurement Window: 7x24x365
SLI2	Support Hours	The hours during which technical support is operational.	From Monday to Friday between 9 and 17.
SLI3	Maximum First Support Response Time	The maximum time elapsed between the Requestor's report of an issue and the initial response from the Provider.	Response times depend on request type and priority as defined in the Support SLAs.
SLI14	Data Retention Period	The duration for which Requestor data is retained by the Provider after service termination notification.	30 days

Pricing

Service billing is based on the maximum resources allocated in the HPC Cloud Infrastructure, as defined at the time of contract signing and subject to modifications as specified later.

In the case of software licenses provided by Cineca, the billing will be based on the usage declared at the time of contract. Adjustments may be necessary following compliance checks or changes requested by the Requestor/Operator.

Service Modification and Termination

Modification of Resources: Requests for changes to the resources allocated to a tenant can be made to the Support Team (email at: superc@Cineca.it) by the PI, as defined during contract activation.

Termination of Service: Service termination can be requested at any time and will take effect from the month following the request. The procedure requires the request to be formally submitted, signed by the Requestor, and sent via PEC or registered mail (A/R) to Cineca reference person. Cineca will initiate the closure process within 30 days from the formal request, informing the Operator of the commencement of termination and specifying the agreed-upon closure date in the issue request.

- **Data Retrieval**:
  - The User will generally have the tools needed to recover and transfer all data and configurations from the Tenant in standard OVF and XML formats by requesting the export of virtual machine images.
  - In special cases (e.g., large volumes of data), technical support from Cineca can be requested for data export, potentially involving a consultancy service according to the established rates for Cineca professional profiles. Time frame for technical support will be agreed with Cineca depending on the requirements.
- **Post-Termination Procedures**:
  - **Tenant Deactivation**: After one month from the termination date, Cineca will deactivate the Tenant (the Operator will no longer be able to access the resources both via GUI and CLI).
  - **Data Export**: Within one month from the termination date, the Operators must complete the export of their data.
  - **Resource De-Allocation**: After one month from the termination date, Cineca will de-allocate the assigned resources and remove any remaining objects (e.g., VMs), including data.
  - **Log Data**: Log data will be retained for the defined retention period.

Annex III: Access Policies

User Responsibilities (new: update on May 2024)

Cineca supercomputing facilities Access Policy

Introduction:

This Access Policy (AP) applies to all users of the Cineca supercomputing facilities. Cineca may make any reasonable change to this AP at any time. If the user does not accept these changes, it may cease to use the Cineca Supercomputing facilities at any time.
User means the individual who has been authorised to access and use the Cineca HPC Resources. For the purposes of this AP, the following terms will have the defined meanings:

- Cineca System means the high performance computing facilities installed in Cineca;
- Resources means the high performance computing service made available by Cineca;
- Username means the identification name assigned to each individual User who has been authorized to access and use the Resources.
- Account means any right to have access to Resources as previously defined. The conditions under which an Account is activated may refer to, but are not limited to, formal contracts, awards, tests and development, training and education. Resources access is defined through a Project with an authorized budget.
- Period of Availability means the time period allocated by Cineca to the User for accessing and using the Cineca Resources;
- Malicious Software means computer virus, Trojan, worm, logic bomb or other material which is malicious or technologically harmful;
- Intellectual Property Rights (IPR) means:
    a. Patents, inventions, designs, domain names, trade marks and related goodwill and trade names (whether registered or unregistered) and all rights to apply for registration of the same;
    b. Copyright and related rights, database rights, know-how and confidential information;
    c. All other intellectual property rights and similar or equivalent rights anywhere in the world which currently exist or are recognized in the future; and
    d. All applications, extensions and renewals in relation to any such rights.
- GDPR means the General Data Protection Regulation that becomes enforceable on 25 May 2018 and aims at the protection of personal data for all individuals within the EU

General Use:

- The User agrees to the enrolment, processing and transmission of the personal data asked for by Cineca;
- The User will inform Cineca of any changes to his/her personal enrolment information;
- The User will use the Resources only in conjunction with the purposes for which the Account is activated, the overriding objectives of Cineca and this AP;
- The User must inform Cineca in case his activity requires the loading and processing of data that may fall under the GDPR (personal data), to identify the appropriate security level; in any case the User confirms that sensitive or personal data will not be loaded and processed to Cineca resources without Cineca written authorisation;
- The Username is strictly personal and may not be transferred to any other third party. The rights to use Cineca Resources will terminate when the Account is exhausted or expired.

- The User recognizes that policies laid down by Cineca may restrict the access to Cineca Resources by citizens of certain countries.
- The User will respect all IPR belonging to Cineca, including any copyright and license.
- The User agrees to not remove from the Cineca System any data without the explicit or implied permission of its owner.
- Use of the Cineca Resources is at the risk of the User. Cineca does not make any guarantee as to their availability or their suitability for purpose.
- Cineca excludes all liability for representations, statements, conditions or warranties to that or any other effect except to the extent that such liability may not be lawfully excluded.
- The User will exercise all reasonable care when accessing Cineca Resources.
- The username will survive for a limited period after the end of all the related Accounts. The User will be allowed to manage and download the data in this period. One month before the expiration of the username, the User will be notified of the imminent expiration. After the expiration of the username, all data stored in the User's personal workspace will be deleted.
- The right to use Cineca Services ends when the original purpose is no longer valid or in specific circumstances the User has parted from the User's affiliated organization. In the latter case, the Principal Investigator (PI) of the Project decides whether the User can continue using Services even if affiliated to a new organization. If the User is the PI of the Project, the User must contact the party who has made the Project allocation to verify its eligibility. In any case, the PIs have the right to associate and remove third users (collaborators) from their account. The User Account and associated content will be handled according to the corresponding service descriptions and their terms of use.

Unacceptable Use:

The User will not use Cineca Resources for any unacceptable purposes. Unacceptable purposes include but are not limited to:

- Any activity which is illegal under local, national or international law.
- Any attempt to breach or circumvent any administrative or security controls.
- Any creation, storage, use or transmission of data which is in breach of any copyright or licence;
- Any usage not allowed by the EU AI act (https://artificialintelligenceact.eu/);
- Any activity which causes material or moral damage to Cineca, or which causes loss of operational efficiency, or loss or corruption of the Cineca System.
- Any activity which interferes with the use of the Cineca Resources by other users.
- Any activity which compromises the privacy of other users.

Security:

- Cineca will provide the User with a username and a link to a portal where User can set the password and activate two-factors authentication (2FA) access. The link has a time validity. It is the responsibility of the User to protect the details of his/her username, password and 2FA token; The User will not divulge its credentials to any third parties, unless expressly authorised to do so by Cineca. The User will not use any other user's username to access the Cineca Resources.
- At login time, if needed, User will be requested to authenticate itself. Once the authentication has taken place, the server will issue a time-limited certificate needed by the User to connect to Cineca systems.
- Passwords should be changed as often as needed in order to guarantee a reasonable security to Cineca's system access;
- The User will take all steps necessary to protect the security of personal computers, laptops and workstations against unauthorised access. Recommended security measures include the use of password-protected screensavers and locking and/or shutting down terminals when left unattended or not in use;

- The User will not knowingly introduce onto the Cineca System any Malicious Software and will not misuse the Internet in any way;
- The User will use the latest versions of anti-virus software available from an industry accepted anti-virus software vendor on all of its access systems to check for and prevent the introduction of Malicious Software onto the Cineca System;
- The User will act immediately to remove any Malicious Software from Cineca System. The User will not interfere with any anti-virus application software run by Cineca;
- Software that is required for the access of the Cineca Resources should be installed on the personal workstations in a protected partition or in a secure mode. That software will be maintained by the User and regularly updated for ensuring security updates;
- The User will not use any computer applications that jeopardise the functioning of the Cineca System. Cineca will notify the User, who will take all steps necessary to detect the cause and prevent re-occurrence. Cineca has the right to suspend the User's access to the Cineca System if necessary and to prohibit any computer application that, in its reasonable opinion, poses a security threat;
- Cineca will endeavour to protect the confidentiality of information stored on the Cineca System. Any information stored on the Cineca System will be used by Cineca, or any third party authorised by Cineca, for administrative, operational, monitoring and security purposes only;
- The User with administration privileges on IaaS cloud resources (VMs) will be responsible to maintaining the security (security patch, fix) on those resources. The User will also have the responsibility to backup both VMs and volume data.
- The User agrees to comply with any special conditions that may apply to specific software installed on the Cineca System;
- The User will report to Cineca if he/she becomes aware of any malfunction of the Cineca System or any problem in accessing the Cineca Resources.
- The User will report immediately to Cineca if he/she becomes aware of any unauthorised use of its username, or if he/she knows or suspects that there has been a breach of security or misuse of the Cineca Resources;
- The User must take suitable precautions to take care of his/her data once the Service comes to an end. Data are property of the User and are connected to the username;

Liabilities and Sanctions:

The User will be liable for any damages resulting from the infringement of this AP or any other policies or conditions imposed by Cineca with the exception of simple negligence. Any infringement or potential infringement will be notified by Cineca to the User in writing. If the infringement persists and/or further violations are detected and/or where the seriousness of the violation justifies it, Cineca may withdraw access rights to the Cineca System and/or initiate disciplinary proceedings and/or legal proceedings against the User. Cineca will not be held liable for any damage resulting from an interruption of the infrastructure access service from which injury to users and possible third parties results.

Annex IV: Privacy notice for processing personal data on Cineca UserDB service

(released on 27 May 2025)

Information and access to personal data pursuant to art. 13 of EU Regulation 2016/679 (General data protection regulation)

This privacy notice is provided to you, pursuant to art. 13 of EU Regulation 2016/679 - General Data Protection Regulation, and in relation to personal data that the Cineca Consorzio Interuniversitario (hereinafter Cineca) acquires as a result of the completion of the registration form at the platform https://userdb.hpc.Cineca.it, through which you have access as user to the services provided by the HPC Business Unit of Cineca in the technical and scientific computing context.

We therefore provide you with the following information:

1. Identity and contact details of the data controller

The "Data Controller" is the Cineca Consorzio Interuniversitario, based in Casalecchio di Reno (BO), via Magnanelli 6/3 – postal code 40033, represented by the Consortium Chairman. The General Manager has been granted implementing powers with regards to the protection of personal data by

a specific act dated 20/09/2023.

You may contact the Data Controller by writing to one of the following addresses: superc@Cineca.it,

dpo@Cineca.it, segreteria@Cineca.it, Cineca@pec.Cineca.it.

2. Contact details of data protection officer

In Cineca there is a Data Protection Officer, appointed pursuant to art. 37 of EU Regulation 2016/679. The Data Protection Officer can be contacted at the following email address: dpo@Cineca.it.

3. The purpose of processing and the legal basis for processing

The purpose of processing your personal data is to carry out all the activities necessary to allow you to register on the platform https://userdb.hpc.Cineca.it thanks to which you can:

- apply for an account on supercomputing systems;
- monitor active projects;
- access the ISCRA platform to submit project proposals which require the use of calculation resources on Cineca machines;
    - For the ISCRA application additional personal data will be requested
    - If the ISCRA project will be accepted the following personal data: Name, Surname, Project Title will be published on the ISCRA web site.

The legal basis for the processing of the personal data you provide to Cineca is the satisfaction of your request to access HPC computing resources.

4. Recipients and Categories of recipients of personal data

The recipients of the data you provide are the data Controller (CINECA Consorzio Interuniversitario) and any data Processors appointed by Cineca, as well as Cineca staff authorized to process the data for the above purposes (HPC user support staff). For the ISCRA evaluation process your data and application form will be disclosed to the scientific referees and to the members of the scientific panel.

Your personal data will not undergo dissemination.

5. data storage period

The determination of the storage period of your personal data is in accordance with the principle of processing requirements. Your personal data will therefore only be stored for the entire period of validity of your personal access to Cineca's computer systems, and for two years after the expiration of your username in respect to DPCM-14-apr-2021-n-81, Annex B; after this period, your personal data may be erased.

6. Rights of the data subject

Please note that with reference to your provided personal data, you have the following rights:

- to access your personal data;
- to obtain the rectification of your personal data or the limitation of the processing operations concerning you;
- To obtain the erasure of your personal data two years after the expiration of your username, in respect to DPCM-14-apr-2021-n-81, Annex B;
- to object to processing;
- to the portability of data (law applicable only to data in electronic form), as governed by art. 20 of EU Regulation 2016/679;
- to lodge a complaint with the supervisory authority.

Please note that to exercise the above rights (points 1 to 4) you may contact Cineca by sending an email to the following address: userdb@Cineca.it.

Cineca is required to provide a reply within one month of the request, extendable up to three months in case of particular complexity of the request. Please note that you can independently correct or erase personal data entered incorrectly at any time, by logging on to your personal page of the platform https://userdb.hpc.Cineca.it or by sending a request to HPC User Support (superc@Cineca.it)

7. Mandatory or optional nature of providing the data and the consequences of failure to provide the data

Providing data is mandatory in order to access the platform https://userdb.hpc.Cineca.it and consequently the HPC computing resources of Cineca.

Failure to provide the data will prevent you from obtaining the service access credentials.

Annex V: Tenant availability definition

(updated on 23 October 2025)

This document aims to provide a definition of tenant availability together with an overview of the critical and non-critical incidents with examples.

Definitions

First of all, we define the roles in the cloud tenant as:

- Operators: PI or collaborators, as in UserDB (Cineca User Portal), that have access to the Tenant via OpenStack (OS) and can manage the allocated resources;
- Users: anyone accessing or making use of the services hosted on the Virtual Machines (VMs) deployed by the operators.

Tenant availability generally refers to the ability of a specific tenant (or project) to access and use the cloud resources - such as compute, network, storage, and APIs - without disruption, in accordance with defined service-level objectives. From this perspective, availability means that the Operators can log in, manage virtual machines, access networks, store/retrieve data, and interact with OpenStack services within the project reliably and without delays or failures due to infrastructure or system issues.

Disruptions, due to due OpenStack services malfunctioning, may lead to delays or degraded performance in managing tenant resources, potentially affecting the quality of service experienced by Operators. However, from the Operator's point of view, the most critical requirement is that the services running on the VMs - such as web applications - remain operational and function as expected. This ensures that users can access and use these services without interruption.

Availability Levels

Based on the above, the tenant availability is defined in three levels (also depicted in Figure 1):

- **Available** when all the OpenStack services are running, Operators can perform all operation on cloud resources and services hosted within the tenant are reachable.
- **Degraded**: one or more OpenStack services are not running as expected. Some operations in the management of cloud resources are not possible or delayed. Services already hosted within the tenant are reachable.
- **Unavailable**: one or more OpenStack services are not running as expected. Services already hosted within the tenant are not running or reachable due to the OpenStack services malfunctioning.

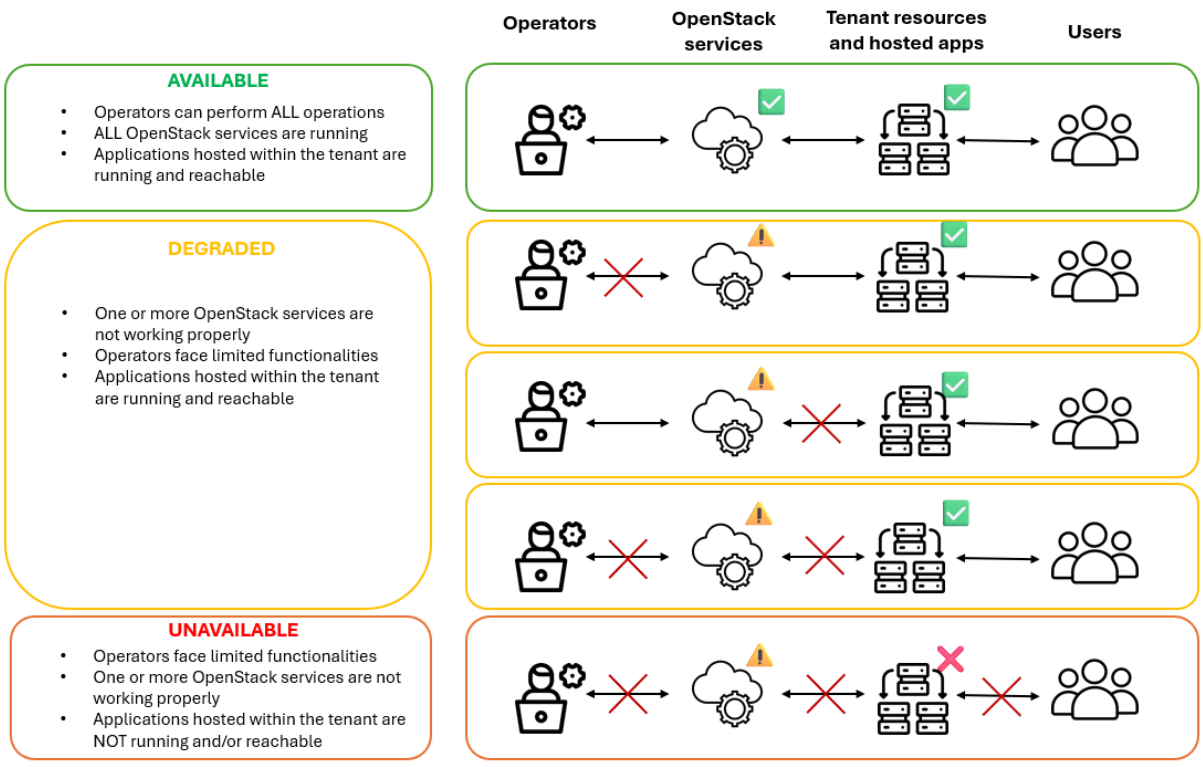

Figure 1 – Availability levels

Incidents classification

Unavailability and/or degradation starts from an incident to one or more OpenStack services and can be mapped to functionalities from the Operators' perspective as in Table 1. The table does not aim to be exhaustive, but to provide an understanding on the approach for the classification of incidents. The classification will be enriched/updated with further experience.

Table 1 – Impact of un-availabilities with respect to functionalities

Category	Functionality	Impact of unavailability	Level of impact

Access OS	Access via Horizon Dashboard	• Operators can't interact via GUI and manage the cloud resources
		  ○ No new resources can be added
		  ○ Existing resources cannot be updated
		• Management of resources can still be done via CLI
		• Services already hosted within the tenant are reachable
			Degraded

Access OS	Access via CLI	• Operators can't interact via the CLI and manage the cloud resources
		  ○ No new resources can be added
		  ○ Existing resources cannot be updated
		• Management of resources can still be done via dashboard
		• Services already hosted within the tenant are reachable
			Degraded

Category	Functionality	Impact of unavailability	Level of impact
		• Automatic workflows which need authentication via CLI can be impacted	

Access OS	Access via dashboard and CLI	• Operators can't interact via the CLI and GUI thus access and manage the resources
		  ○ No new resources can be added
		  ○ Existing resources cannot be updated
		• Services already hosted within the tenant are reachable
		• Automatic workflows which need authentication via CLI can be impacted
			Degraded

Access VMs and related services	Access to the VMs via SSH	• For issues with the OS networking service, the operators cannot access the VMs • VMs are still up, and services already hosted within the tenant are reachable	Degraded

Access VMs and related services	Access to the services hosted on the VM	• Users cannot reach the services hosted within the tenant and/or services deployed on the VMs might not be accessible
		• This can be caused for example by
		  ○ Internal network issues (the VMs are up but not reachable)
		  ○ The VMs are down because the hosts are not working (down hypervisors)
			Unavailable

Tenant management	Create/delete VMs	• Operators cannot create/delete new instances within the tenant • Other VMs are still up, and services hosted within the tenant are reachable	Degraded
Tenant management	Update/modify already created VMs	• Operators cannot update instances already created • VMs are still up, and services already hosted within the tenant are reachable	Degraded
Tenant management	Create/mount volumes	• Mounting/creation of new volumes is not possible • Services already hosted within the tenant are reachable	Degraded
Tenant management	Access to volumes	• Already mounted volumes are not accessible from the VMs • The workflow implemented in the tenant might be compromised	Unavailable
Tenant management	Update/modify already created VMs	• Operators cannot manage volumes already created (i.e. resize) • Services already hosted within the tenant are reachable	Degraded
Tenant management	Create/mount shares	• Mounting/creation of new shares is not possible	Degraded

Category	Functionality	Impact of unavailability	Level of impact
		• Services already hosted within the tenant are reachable	
Tenant management	Access shares	• Already mounted shares are not accessible from the VM • This might compromise the workflow implemented in the tenant	Unavailable
On request features	Load Balancer create	• Operators cannot create a new LB • Services already hosted within the tenant are reachable	Degraded
On request features	Load Balancer update	• Operators cannot modify/update LB already created • Services already hosted within the tenant are reachable	Degraded
On request features	Load balancer functioning	• An already created LB is not functioning as expected • This might cause the services hosted within the tenant not to be reachable or working as planned	Unavailable

SLA and reporting

For reporting purposes, each incident on the OpenStack infrastructure and services is analyzed following the above classification approach and classified as:

- "**Critical down**" if it leads to unavailability; critical downs are accounted in the calculation of the monthly availability percentage.
- "**Noncritical down**" if it leads to degradation; these are described in the monthly reports, but they are not accounted in the calculation of the tenant availability part of the SLA.

The availability is calculated as uptime / (uptime + downtime). Availability is then expressed as % over a certain period (typically one month). The downtime is calculated based on the duration of the "critical downs".

The tenant availability SLA is then provided to Operators with a global target. This is calculated considering the duration of critical downs only over the availability period. By default, the calculated tenant availability is considered the same for all tenants. Exceptions apply in cases involving Load Balancers, which are only considered for tenants that have the respective service enabled. Additionally, if an issue is limited to a specific subset of hypervisors, the impact is assessed only for the affected tenants.