

EOSC Ireland Node – Questions for a Node + Answers from PaNOSC

Original 18/3/2026, updated 7/9/2026

PaNOSC's answers to the questions posed by the Ireland Node about building a Node.

1. Architecture

1. What are the architectural components of the core of your EOSC node

The PaNOSC Node is made up of data repositories + remote data processing services. See <https://www.panosc.eu/panosc-eosc-node/> for overview of 19 services registered so far.

2. What technologies did you use for those components and what other options did you consider.

For now we use the following technology stack:

- a. Website to host home page – <https://eosc.panosc.eu>
- b. Community AAI UmbrellaID – being ported to myAccessId
- c. Catalogue of Services – registered in mTessHub, cf. <https://services.tesshub.hzdr.de/materials?collections%5B%5D=PaNOSC%20Node%20Service%20Collection>
- d. Web service to serve Catalogue to EU Node – [url]
- e. Facility data repositories – ICAT+DRAC, SciCat or Invenio based
- f. Remote data analysis service – VISA, cf. <https://visa.readthedocs.io/en/latest/>
- g. PaN-Space for users to create their own projects – see <https://heliport.helmholtz.cloud/mypan> (under development)

3. What resources from providers (compute, storage etc) are part of the MVP for your node

The resources are provided by the facilities partners of PaNOSC. They consist mostly of data and some access to compute for processing data from the PaNSOC node. EOSC Users will share the resources with the facility users. These consist of a range of CPU, GPU and storage resources.

4. Are data repositories part of your MVP? What does "integrating a data repository" mean for you ?

PaNOSC has 9 data repositories registered. Integrating a data repository means (1) the data must be related to the photon and neutron domain, (2) they are registered in the PaNOSC service catalogue, (3) they are harvested by the PaN-Finder, and (4) they should support the myAccessId login as one of the possible authentication mechanisms.

5. Skills needed to run the MVP. How many operations staff

Data management + IT infrastructure + AAI + cybersecurity skills

6. What resources are needed from resource providers, what co-ordination mechanism do you have with them for day to day operations including cybersecurity

The PaN community has a cybersecurity interest group which all PaNOSC partners participate in. There is no official CIRT (yet) but it will be required in the future.

7. Can you share your architecture diagram(s) along with any documentation you have on what you have built?

We can share our Project Plan which contains some diagrams. The architecture is very simple and most connections are human.

8. Do you see your national node as more of a service for the EOSC.eu node to access sub-nodes within your country or more as a portal/destination in itself?

PaNOSC is a thematic node and sees the link to the EU Node as being optional. National Nodes could have a stronger link if they could host PaNOSC Users and data. So far this has not happened.

9. Is EOSC ultimate design to have users log in centrally (EOSC.eu) and navigate to everywhere from there or with access also be fragmented?

No. Users should be able to login in to any Node and then access to other Nodes the Federation using SSO i.e. without having to login again

10. What is the benefit of fragmented access if each national node is so different from the others and the EOSC.eu node?

Today many of the same national and EU Node resources exist and are fragmented. The goal of the Federation is to federate them to reduce the fragmentation.

11. If I log in in a national node (if that makes sense) there must be some communication with the federation containing the national node (EOSC.eu), correct?

Not necessarily. It might happen through monitoring.

12. **What accounting information are you gathering when equipment is instantiated at a EOSC client site. Are the commands users execute being collected - to discourage / prevent / see malicious activity?**

Monitoring and accounting are foreseen but not defined internally for PaNOSC nor by the EOSC Federation yet.

13. **A compiled container or virtual machine will capture operating systems, libraries, and code in a particular point in time, so that an experiment can be reproduced. Do you provide a container or virtual machine registry e.g., Docker Registry, to support experiment reproducibility?**

We provide VMs through the VISA analysis platform but not a Docker registry. Distributing software is handled as follows: Software is packaged using Apptainer and/or modules and distributed through CVFMS.

14. **How is your national EOSC node supporting/enabling researcher access from different countries? e.g., how can an Irish researcher access your infrastructure / repos?**

In the case of the European facilities they are open to all Europeans. In the case of national Nodes this problem has not been fully solved yet i.e. usually only national researchers or those with links to national researchers have access to national nodes. It would be a big step forward towards a European ecosystem if the EOSC Federation could solve this through the Rules of Participation which still need to be defined and agreed upon.

15. **If a researcher needs equipment and resources distributed across multiple EOSC sites, can this type of experiment be accommodated easily?**

This has been demonstrated by some of the use cases e.g. the REANA and/or Galaxy ones. These use cases have setup bilateral agreements between the partners. There is no ready to use framework for doing this (yet). If a node wants to do this then they should find other nodes who agree to accept to share resources across multiple EOSC Nodes.

PaNOSC has not been involved in such a use case but it could be useful for distributing the workload of gpu or cpu-intensive workloads. The main bottleneck will be moving the data if there are large volumes of data involved.

2. Technology trials

1. **All: EOSC Handbook refers to reference implementation of "Node Core Capabilities" on p22. Where is that to be found? It would be quite valuable.**

They are listed in Table 4.1. On page 28. The Core Capabilities which are designated as Federating Capabilities are described in more detail in Chapter. Some of them are considered internal to the Node and will be implemented by the Nodes if required. Refer to the documentation in EOSC Beyond for more technical descriptions and examples of implementations.

Node Core Capabilities	Description
Resource Catalogue and Registry services	Catalogue of resources that can be accessed through the EOSC Node with a search engine to discover, access and order them
AAI	AAI (AARC Blueprint compliant) enabling access to Node resources (Core and Exchange) via federated credentials (i.e. community AAI and Infrastructure Proxy)
Helpdesk	Support incident response and service requests for services and other integrated resources
Service Monitoring	Monitor the availability and quality of the Node services
Service and Research Product Accounting	Track and record usage of resources
Order Management	A framework for providers to define offers and a unique interface for end-users to request access to resources
Configuration Management System	Shared space to store information on Node capabilities and on how services are provided through the node to ensure consistent service delivery (only for internal use)
User space	Dynamic customisable dashboard, where the node user logs-in, offering easy access to the Node resources
Application Deployment Management	Automated deployment and execution of services on the underlying Node provisioned infrastructure
Resource provisioning	Support users in identifying all available resources for a project and then assign a subset of them to the project

Table 4.1: EOSC Node Core Capabilities

2. **All: Is your national/candidate node up and running today?**

The definition of “running” is not defined so it depends on what you mean. If you mean we have Users who login using the EOSC AAI then the answer is no. If you mean Users of the resources provided then the answer is yes. The new services being developed as EOSC services e.g. the User Space and the PaN-Finder are still under development. I think until we have the EOSC AAI in production we cannot say the Node is operational.

3. **All: If your national/candidate node is up or architected already, can you share all/most documentation with us (Architecture diagrams/documents, Design considerations etc...)?**

We can share our Project Plan which is our working document with you. All software is open source and can be shared.

4. **All: For you national/candidate node do you have use-case or user-flow documents that you can share?**

The PaNOSC use case is the PaN-Finder <https://eosc.eu/wp-content/uploads/2025/10/EOSC-Federation-scientific-use-case-PaN-Finder.pdf>

The OSCARS PaNOSC projects are all potential Use Cases of the EOSC Federation https://oscars-project.eu/projects?title=&field_unlimited_clusters_target_id%5B11%5D=11

5. **All: Do you see your national/candidate node as providing actual user-facing resources directly -- beyond AAI, helpdesk, order management and catalogue services (of/for regional nodes)?**

For sure – the main objective of the PaNOSC is to provide FAIR data and scientific services so that researchers can exploit the data. The EOSC Federation is a means to this end by providing a framework and common goal for RIs in Europe. The goal is not the Node Core Capabilities. I presume this is the case for all Thematic Nodes. It would be interesting to hear what the motivation for National Nodes is.

6. **All: How are you handling logins and federated ACLs up and down?**

The PaNOSC AAI (UmbrellaID) has been transitioned to myAccessID which allows researchers to login with the home facility identity. ACLs are implemented at the facility level. Each facility needs to map the Researcher's identity to a local identity recognised by the ACLs. At most (all?) sites this is done via a local LDAP which means researchers still need a local account which is created manually or automatically.

7. **All: Do you see your national node as more of a service for the eosc eu node to access sub-nodes within your country or more as a portal/destination in itself?**

I see the national nodes as a service on their own. Similar to the EU Node which is a standalone node which provides services. Today it provides some of the core Federating Capabilities for the Federation as long as it is funded.

8. **NL SURF: Is Research Cloud itself the EOSC NL node or is it a service that you have implemented on RC which you have then surrounded with other functionality?**

Not for PaNOSC to answer

9. **EOSC.FI: From what I see, you are presenting the EOSC FI node as an API service. Is this correct and if so, how do you get non-API "capable" users onto it?**

Not for PaNOSC to answer

10. **All: For eosc nodes in your country that need to manage ACLs etc, do they relay ACL changes to the EOSC EU node or are ACLs managed on those nodes?**

No. See answer about how ACLs are managed above.

11. **All: Where do I log in? Regional nodes? National nodes? EU Node? Any of these? I'm reading about EOSC AAI but do not yet understand if**

The idea is that you can login to any node and then use SSO to navigate to other nodes.

12. **Are your client EOSC sites expected to run OpenStack / Kubernetes / other software?**

No. We have recommended software stacks but sites providing PaNOSC services are free to choose amongst the recommendations or none of them. In the latter case there is less federation possible and at some point it might become a blocking issue.

13. **To encourage use of the equipment at client EOSC sites, do you provide training to perspective researchers of the EOSC equipment? Or do you encourage EOSC sites to produce and provide the training? Is there are central location for all this information?**

We do not have dedicated training yet but we have a common training platform (<https://pan-training.eu/about>). We plan to develop dedicated training in the future.

14. **What technologies are you using to provide the EOSC National Node? Are they in house developed? Are they opensource? What technologies are you using to index research and data repositories connected to this node? Are you relying any technologies provided / offered / developed by the EOSC EU node? If so, which ones?**

PaNOSC Node and its providers use a mixture of in-house and externally developed technologies e.g. VISA, CVFMS, Jupyter, H5Web, mTessX, ICAT, SciCat, Invenio, PaN-Finder, PaN-Space, Openstack, Kubernetes, Mattermost being the main ones. We do not use any technologies developed by the EU Node mainly because they are not many and those that have been released are not following Open Source best practices i.e. they provide snapshots only.

3. Governance and funding

1. **Models for legal entity - what are the options, why were certain models selected.**

PaNOSC is developing an internal MoU as governance document. The host institute (ESRF) has signed the EOSC Federation MoU with the EOSC-A

2. **Staffing - centralised V distributed, what is considered core, what is required at institution/resource holder & user level. Service provision model(s).**

PaNOSC Node is a consortium of 11 members and is by nature distributed.

3. **Core Services (centrally controlled) V remote onboarded services.**

PaNOSC has a few core services like the landing page, the service catalogue, the training platform, the finder and the user space. All others are distributed.

4. **Management of policy landscape re user access rights from distributed resource providers (also credit system, buying credits etc).**

This is not defined yet but we will define recommendations and then delegate their implementation to the members.

5. **Funding Structures - depts V funders. Membership models.**

No extra funding has been received. Our INFRA-EOSC-01-2025 proposal was not funded. All efforts are in-kind funded by the PaNOSC members. This severely limits the amount of effort that can be dedicated to the node especially seeing as the EOSC Federation has created multiple sub-groups which require investing time in them.

6. **Additional staffing related to integrating sensitive data services/more generally any considerations for additional and specialist resource onboarding and management**

None - PaNOSC does not deal with sensitive data. Any potentially sensitive data are anonymised by the team responsible for them e.g. <https://human-organ-atlas.esrf.fr/>

7. **Phased implementations of service types - advice and resourcing**

We are working towards having the PaNOSC node in production in 2026. Everything is phased to the lack of dedicated resources. We meet once a week to discuss progress of the Project Plan and issues.

4. Connecting to EOSC federation

1. **What service catalogue metadata will you use?**

mTessX provides one.

2. What service categories will you have? (software/data/training/+?)

These are defined in the Service Catalogue

<https://services.tesshub.hzdr.de/materials?keywords%5B%5D=data%20management&collections%5B%5D=PaNOSC%20Node%20Service%20Collection>

We have defined the following ones so far:

- a. Data management
- b. Metadata management
- c. Research data management (RDM)
- d. Data mining
- e. FAIR data
- f. Findable, accessible, interoperable, reusable data
- g. Pattern recognition

3. Which domains are you focusing to as a pilot? (or all initially?) --> avoid those covered by thematic Node? (vice versa for national)

Photon and Neutrons – what else?!

4. Do you plan to consolidate service delivery under one (national) entity/compute provider or institutional/regional distributed level provisions?

Not planned

5. What is your EOSC service onboarding criteria?

Must be related to photons and neutrons. We are developing an onboarding guidelines and requirements.

6. What is your EOSC service monitoring criteria?

Not defined yet.

7. What interoperability framework guidance are you using? Service specific? (e.g. training diff to data diff to software diff to database?)

Not sure what is meant here

8. How will you deal with competing interoperability reqs - EHDS/data spaces/EOSC interoperability framework?

Not an issue yet

9. How are you dealing with SLAs? Service uptime minimums?

Best effort for now, more is difficult without dedicated funding.

10. How are you dealing with accredited databases? Priority? CDR/EDD of ELIXIR or coretrust seal general?

We have a mixture but recommend CoreTrustSeal

11. What EOSC Project outputs are you dedicated to supporting and integrating? e..g EOSC Future/Beyond or TREs EOSC ENTRUST?

EOSC-FIDELIS, EOSC Beyond, ...

12. How are you dealing with existing service catalogues of domains? TeSS - life science training/bio.tools - life science tooling? vs set up of new one for your node?

We are using (and co-developing) the new version of TeSS

13. If operating service provisions - how many staff & redundant shared support are there? e..g 1 FTE = all services/etc. Scaled approach as limited resourcing?

Not well defined but we strive to have 3 FTEs working on the node

14. How will you deal with helpdesk? Offload to service provider or centralised?

Not available yet, we will follow the technical platform chosen by the EU Node. The entry point will be centralised.

15. EOSC Core service integration musts and needs? Experience to integrate - how heavy? e.g. federate one database took X FTE?

AAI is taking months if not years in elapsed time (effort is less). Integrating the service catalogue took weeks.

16. Who will give effort/upgrade and integrate services for the node? Or simple catalogue and guidance provided?

Up to each service provider

17. What are the service sustainability requirements? e.g. once database live and available - sufficient or dedicated staffing (0.5 FTE)? Curation/ongoing requirements? Security updates?

We ask services to be maintained for 5 years

- 18. Are you planning any key EOSC bids? How could we collaborate - show we are prepared and have dedicated capacity to be an appealing partner?**

We applied for INFRA-EOSC-2025-01 but were not successful. We have one project funded by Gravity.

- 19. EOSC has many groups & countless outputs - task forces/opportunity areas/node working groups - what will you adopt? How will you stream these?**

Doing everything with only in-kind resources makes it very difficult.

- 20. How are you dealing with legal service requirements for onboarding and provisioning in a multi node format - e.g. Galaxy - could be in all nodes? How to get co-contribution model to support?**

We are setting up an MoU with internal guidelines for onboarding. Legal responsibility will stay with service providers.

- 21. Service mapping and landscaping - we know life sciences and social sciences; how did you cover all key services? National or european relevant only? How did you reach stakeholders?**

PaNOSC is a thematic node

- 22. What government programmes/supports on service delivery (ESFRIs) side have you seen as effective to lobby for in Ireland?**

Not applicable

- 23. What is your ESFRI engagement strategy ? European EOSC Nodes vs national implementations and alignments?**

PaNOSC has a mixture of ESFRI and national members. We follow the ESFRI EOSC strategy.

5. Dealing with services for handling sensitive data

PaNOSC provides only non-sensitive data. It is up to the resource providers to ensure data are not sensitive.

1. How are you dealing with TREs/SPEs? You provision or vs existing offerings?

2. How much capacity and effort to operate at EOSC Level?
3. Plans for federated analytics?
4. Plans for GDI integrations?
5. Plans for EOSC ENTRUST federated TRE alignments and updating?
6. What are the core offerings/base services in place for sensitive data?
7. How do you deal with different domain needs - commercial/social sciences/health/+ and their needs? Do you agree to exclude some out of scope e.g. criminal data - and what safety provisions do you have if anything goes wrong with access?
8. How are you engaging with ELIXIR/GA4GH other key orgs for standards and services? Are you adopting any directly?
9. To support processing of sensitive data, what are you doing in terms of networking, data storage, etc. For example, are disks associated with VMs encrypted? Is the networking isolated - for example VXLANs, or VLANs are separated? Defining Firewall and Public Private key pair access via SSH only to instances and SSL used in data transfer. Destruction of encrypted disks/data after experiment is completed etc. What are the requirements of the client sites?
10. What are the certifications, compliances required by an EOSC node to offer such processing of sensitive data services?