**EOSC Monitoring - integration factsheet**

**What is it**

Monitoring is the key service needed to gain insights into an infrastructure. It is continuous and on-demand to quickly detect, correlate, and analyze data for a fast reaction to anomalous behavior.

The key functional requirements are:

- Monitoring of services
- Reporting availability and reliability,
- Visualization of the services' status,
- Provide dashboard interfaces,
- Sending real-time alerts.

The dashboard design enables easy access and visualization of data for end-users. System supports a rest-like http API that allows third parties to gather monitoring data programmatically.

**Why to use it**

Monitoring is used to identify and correlate problems before they negatively affect end-user experience and ultimately the productivity of the organisation. Management teams can monitor the availability and reliability of the services from a high level view down to individual system metrics and monitor the conformance of multiple SLAs.

The Monitoring service checks the availability and proper functioning of a service. It can warn of problems as they arise, allowing to resolve the issue immediately and minimize the time the service may be down.

Just because everything is working doesn’t mean that it’s all working as well as it could be. The Monitoring Service helps the Service Providers understand the ins and outs of the service, so that the owner can focus on areas that might be putting it at risk. Targeting problematic areas or functionalities, and resolving them before incidents occur could help the performance and usage of the service.

The Monitoring Service helps the Service Owners to be proactive. The Monitoring Service supports alerts which is an advantage and informs the Service Owners about possible problems before they impact the users. The Service Providers will be able to fix the problem before they cause any trouble. Detecting and fixing issues before they cause problems has multiple benefits like preventing system downtime and avoiding unhappy users.

**How to integrate with it**

Details of these different options are described in the different use cases part of the Monitoring Documentation: [https://argoeu.github.io/argo-monitoring/docs/guides/intro](https://argoeu.github.io/argo-monitoring/docs/guides/intro)

**Integration Option 1: Monitor an Onboarded Service**

This use case covers the scenario to monitor a service Onboarded to EOSC via the Providers Portal. The results of this process will become available via the EOSC Exchange Monitoring WebUI ([https://argo.eosc-portal.eu](https://argo.eosc-portal.eu)). In order to start monitoring an onboarded service, several requirements should be met. In addition to the basic information provided during the onboarding process, the service provider needs to provide some extra information needed by the ARGO monitoring service.

**Integration Option 2: Monitor an Infrastructure**
Use case 2 covers the scenario when infrastructure monitoring requirements cannot be met by EOSC-Exchange Monitoring. For example, one the following are required:

- defining custom topology and aggregation of monitored endpoints
- selecting from existing range of probes and adding custom ones
- managing profiles and metrics for different services

**Integration Option 3: Integrate External Monitoring service**

In order to be able to scale-out and take advantage of existing Monitoring systems, the EOSC Monitoring service is capable of accepting data from external sources. When referring to external sources we mean other monitoring engines that want to connect with the EOSC Monitoring Service. This use case is split in two different sections as follows:

1. Case 3.1: Supported Monitoring Engine and Operating System (Nagios on Centos 7 or Debian 8).
2. Case 3.2 Other Monitoring Engine and Operating System

**Integration Option 4: Combine Results of existing ARGO Tenants**

This use case covers the scenarios where the topology and the results of multiple tenants need to be combined in a number of reports.

**Integration Option 5: Third-party services exploiting EOSC Monitoring data**

This use case covers the scenario according to which the customer needs to use the results of the EOSC Monitoring Service in an external service/dashboard.

The customer can access the following information via an API:

- A/R information about the service and its service components
- Status information about the service and its service components
- The topology and grouping of the service

**Dependencies & Prerequisites**

EOSC Monitoring service requires following topology information in order to monitor services:

- the services and service endpoints they are running,
- the way they are organised (e.g. groups of sites, groups of services),
- the service actors (owners, admins, contact points).

Topology can be further extended with attributes needed for individual probes (e.g. service port or URL, path to be used in case of storage services, e.g.).

**Where to ask assistance**

If you just want to ask a question please email at argo@grnet.gr