EGI-InSPIRE

VO Operations Portal plan (version 3)

Document identifier:	VO Operations Portal_V3.doc
Date:	**13/10/2011**
Document Link:	

Abstract

This document describes a proposal for the development plan of the VO Operations Portal.



Copyright notice

Document Log

Issue	Date	Comment	Author/Partner
0.1	03/08/2011	Initial document version	G. Borges
1.0	30/08/2011	Include development table; UCST review	G. Borges, C. Lorphelin, G. Sypos
2.0	30/09/2011	Include feedback from F. Michel (LeSC)	G. Borges, F. Michel, C. Lorphelin
3.0	13/10/2011	Include final remarks from F. Michel (LeSC)	F. Michel

TABLE OF CONTENTS

1 INTRODUCTION

NGI/EGI operational teams are responsible for the monitoring of EGI infrastructure so that it is always available for the end users with reliability defined in EGI Resource Centre OLA [R1]. However, Virtual Organisations build their own frameworks on top of the basic grid functionalities, expanding its use for the benefit of their communities. Taking into consideration that there are more than 200 VOs registered in EGI, coming from a wide spectrum of areas, it is virtually impossible that operation teams will be able to detect specific VO problems. Therefore, the testing and monitoring of services from VO-specific perspective has to be delegated for the VOs themselves.

Currently VO/VRC managers do not have a simple and easy way to detect and alert the VO infrastructure providers about operational problems interfering with VO work flows. Some of the communities have deployed a VO Service Availability Monitoring (SAM) instance [R2] and implement monitoring shifts based on its results. The VO SAM is a specific configuration of the EGI Operations SAM service to monitor the VO production infrastructure, and periodically triggers the execution of probes in grid sites along the day. The present list of probes includes:

- Job submission testing via CE probe/metrics: full job submission chain is exercised - job submission, states monitoring, output sand-box retrieval, ...
- Data managements testing via SRM probe/metrics: get full SRM endpoint(s) and storage areas from BDII, copy a local file to the SRM into default space area(s), ...
- WN testing via WN probe/metrics: replica management tests (WN<->SE communication), ...
- WMS testing via WMS probe/metrics using submissions to predefined CEs.
- LFC testing via LFC probe/metrics: read and update catalogue entries, ...

At running time, the different probes return a specific exit code to reflect the success or the failure of the test execution, and translated to different probe status (OK, WARNING, CRITICAL and UNKNOWN) displayed in the VO SAM NAGIOS web interface. The shift process consists in looking to the (not so friendly) VO SAM NAGIOS interface, and open operational problems to the failing sites. However such process is very time consuming delaying the identification and mitigation of problems.

This document presents a draft plan for the development of a VO Operations Portal as module of the EGI Operations Portal. It will be based on the functionalities already available in the Operations Dashboard presently in use for the monitoring and control of the infrastructure. A VO using a VO SAM instance may use the VO Operations Portal for a fast identification of problems, and trigger the request for their mitigation on demand.

This document is organised in the following sections:

- Chapter 1: Introduction.
- Chapter 2: Overview of the requirements and functionalities.
- Chapter 3: Architecture overview of the main building blocks.
- Chapter 4 : Tasks and effort for the development and testing of the tool.
- Chapter 5: Conclusions.

2 REQUIREMENTS AND FUNCTIONALITIES

Several communities representatives (GISELA, BIOMED, We-NMR) have requested the possibility for the project ***to provide a tool allowing a quick and easy identification of resources failing automatic VO SAM tests. VO experts could then access to this tool to validate results and alert infrastructure providers about how to mitigate the issues.*** The benefit of the such tool is straightforward since ***it optimizes the work of VO experts allowing them to pro-actively supervise the infrastructure, easily identify problems and push for their resolution before those issues are experienced by the end users***. The requirements are collected in RT ticket #1800 [R3].

The document refers to this new tool as the "VO Operations Portal".

2.1 Basic functions

According to the different discussions held at the EGI User Forum 2011 and at EGI Technical Forum 2011, the communities already have a clear definition of the basic functionalities that the VO Operations Portal should provide:

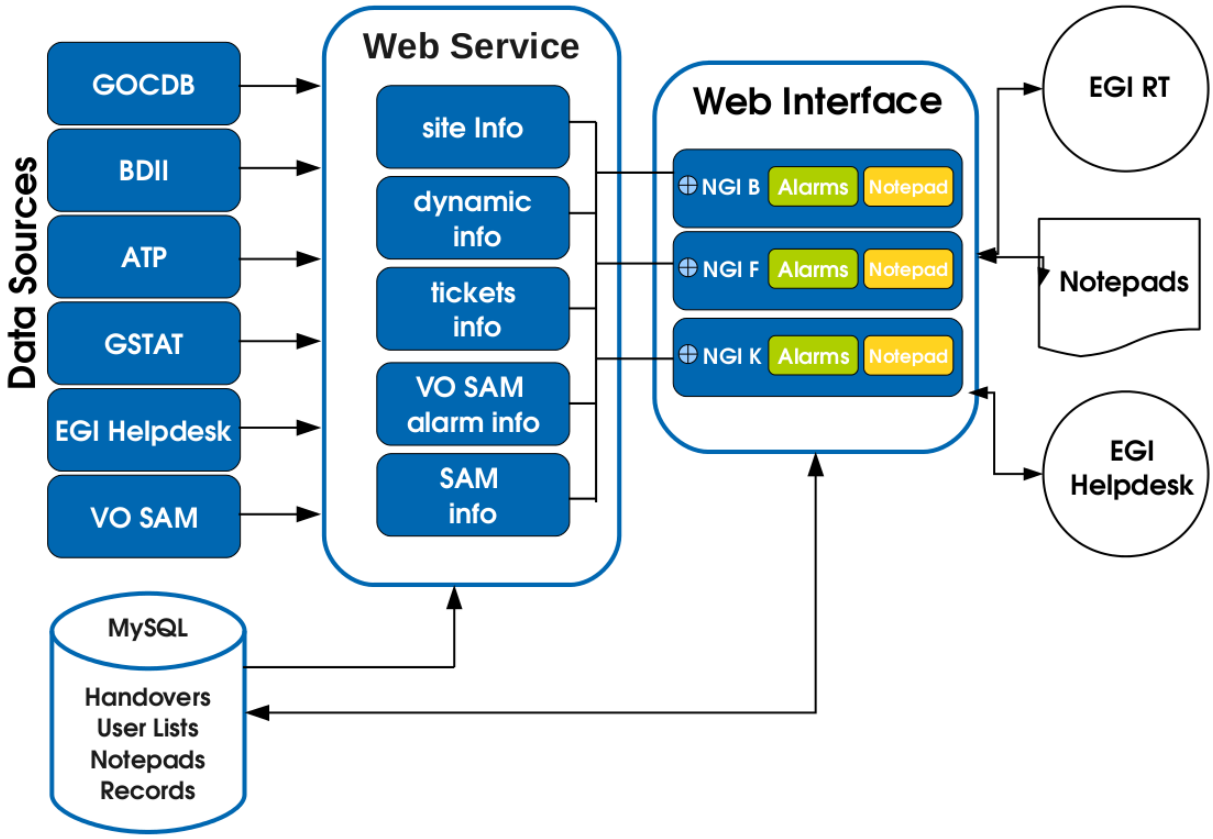
- Provide a dashboard whose basic entities are sites, tickets and alarms.
  - An alarm reports changes in the status of a given site service, based on automatically generated notifications created by the VO SAM (operated by / for the VO). An alarm should be generated once the dashboard processes notifications from the VO SAM reporting transitions from status=OK to any other status. Transitions from any other status to status=OK should automatically close an on-going alarm.
  - A ticket is a notification (triggered by VO staff) sent to site administrators via EGI helpdesk reporting one or more on-going alarms affecting a site service. The dashboard should provide a mechanism to link several on-going alarms under a ticket template which is then opened and assigned to the proper site via EGI helpdesk.
- The dashboard should report the present number of on-going alarms per site for all sites supporting the VO, and the present number of open tickets per site, for all sites supporting the VO.
- Flapping alarms (which change from status=OK to any other state, and then back to status=OK, several times during a reasonable short time period) should be identified and reported as on-going alarms.
- The information displayed by an on-going alarm should include details from the failing VO SAM test, and historical data regarding for how long is the alarm active (representing how long a site component is failing).
- The dashboard should offer the possibility to declare a list of VO SAM tests to take into account while processing service failure notifications coming from the VO SAM.
- The dashboard should present information about downtimes for the site and site services, and do not raise alarms for resources in downtime and/or declared as "not in production" or "not monitored" in GOCDB.
- Tickets should report the last known status of the VO SAM test for the alarms which were initially linked to the ticket.
- VOs wishing to use TEAM tickets should be able to use that EGI helpdesk property for the tickets submitted via the VO Operations Portal.

- In order to avoid the duplication of tickets, the dashboard should provide a mechanism to alert VO staff that a given alarm is not VO specific, and that a ticket was already opened in EGI helpdesk by the regular operations teams.
- The access to the dashboard should be controlled. Only allowed staff will be able to interact with the tool based on specific VO roles, or on a declaration on the VO ID card.
- The dashboard should present information about the site service topology (node services at the site according to GOCDB) and direct operations links to site details in GOCDB and GSTAT.
- The dashboard should allow sending notifications directly to the sites and to other VO Operators.
- The dashboard should offer the possibility to compute different kinds of metrics (for example through a well defined Builder), and to export the raw data under a defined format. The export should not only be performed manually from the user interface (export button), but also through an http get url containing all parameters, allowing for another application to request metrics reports without the need to fill in a form.
- Examples of important metrics are:
  - Cumulated time (hours, days, months) each site service (SRM node, CreamCE, ...) spent in CRITICAL status (or in WARNING status) over a period of time. Ex: node.my.domain spent 96 hours in CRITICAL state during September 2011.
  - Average time per period of time A (hours, days, months) each site service (SRM node, CreamCE, ...) spent in critical status (or in warning status) over period B. Ex: node.my.domain spent an average 0.13 hours in CRITICAL state per day during September 2011.
  - Total number of alarms cumulated over a period of time per site and per service (SRM node, CreamCE, ...). Ex: There were 60 SRM failures for the VO during September 2011; my.site had 10 failures during September 2011; my.site had 2 SRM failures from 10th of September 2011 to 20th of September 2011.
  - Average number of alarms per period of time A (hours, days, months) over period of time B per site and per service. Ex: average number of SRM critical alarms per day during September 2011.
  - Possibility to apply thresholds, and show only those elements that had more than x alarms per period of time A, during period of time B. Ex: all SRMs that had more than 5 alarms per day during the last two weeks.

3 ARCHITECTURE

Such tool must provide similar features for general VOs as the Operation Dashboard [R4] does for the EGI ops VO. The **proposed** architecture is depicted in the following figure, and it relies on a three-tier model originally developed for the Central / Regional Operations Dashboard:

- A Web Interface.
- A Data Aggregation and Unification (Web) Service named Lavoisier [R5].
- A MySQL DataBase.

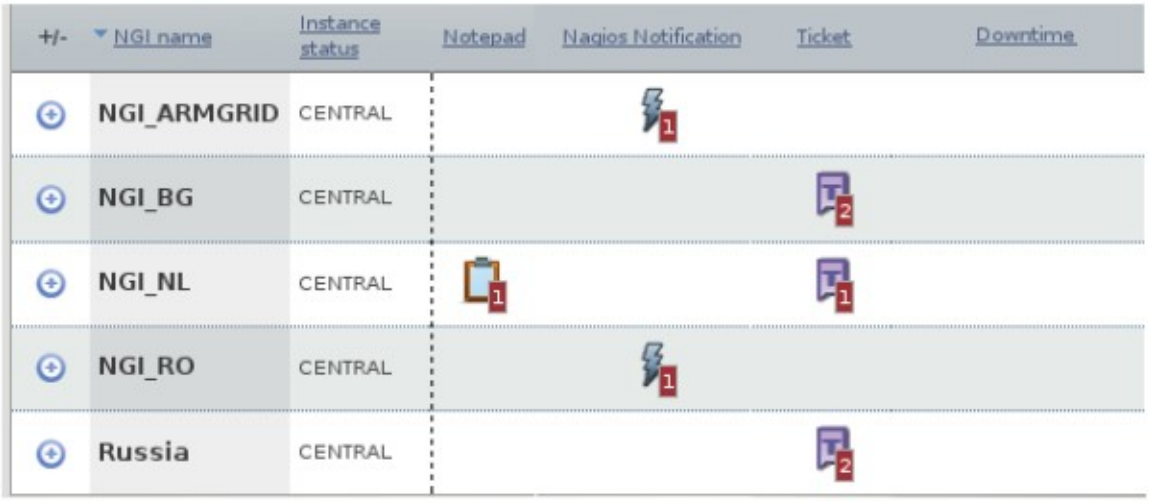


3.1 Data aggregation and unification service

The Web Service Lavoiser has been developed at CC-IN2P3, and it is heavily used in EGI Operations in the Central and Regional Operational Portals. It is the component used to store, consolidate and 'feed' data into the web interface. It provides information from various sources, which protects the application from intermittent failures of information sources. The application was developed to enable easy and efficient cross-data sources queries, independently of technologies used. Data views are represented as XML documents and the query language is XSL. Through dedicated adapters (plug-ins which interact with data sources and produce a XML document as their output) Lavoiser is able to get information from different EGI tools using their specific APIs like GOCDB, GSTAT, Aggregated Topology Provider service (ATP), EGI Helpdesk (GGUS), GIIS (BDII), VO SAM and others.

3.2 Web Interface

The proposed VO Operations Portal will have a central instance with one entry point per VO (http://operations-portal.egi.eu/VoDashboard/<Voname>). The web interface is written within a PHP Framework (Symfony) and represents the user interface. Whenever authorisation is needed, authentication is done using X509 certificates. The proposed Web Interface view will be based on the current COD Operations Dashboard view, presented in the next figure:



The figure represents a synoptic view per NGI with a summary of all VO SAM notification/alarms, all tickets in EGI Helpdesk opened through the dashboard, all messages exchanged withing VO operations (handovers), all messages sent to sites (notepads) and all downtimes for resources supporting the VO. The details for all events under each NGI can be obtained clicking on the "plus signs" on the left. A drop-down box appears reporting information for sites and resources for which VO SAM tests have failed.

Through this web interface, an authenticated user with the correct VO role will be able to:

- Access all site's alarms and tickets.
- Send a notepad (message) to given site.
- Exchange messages with other VO Operators (handovers).
- Access all messages exchanged with the site's operator.
- Open a ticket via EGI Helpdesk to a given site linking on-going alarms.
- Access and update EGI Helpdesk tickets opened via the dashboard.
- Generate metrics within a given time period.

3.3 Database

The last component of the architecture is a MySQL DB. The Symphony Framework allows to automatically build a DB given a specific schema. The DB keeps important information like exchanged Notepads and Handovers, ACL and other relevant records about user actions.

4 WORK-PLAN

The work-plan consists of the following major activities: **Development, Test and certification and Operation and Support**. The activities and tasks to be accomplished under each phase are presented in the following sections.

4.1 Development

The development work consist of two phases, both to be executed by CNRS under TJRA1.5:

1. Development I, representing the initial development effort, planned to start at the beginning of October 2011, and expected to end at the beginning of January 2012. The effort estimation for this initial development and incorporation of the VO Operations Portal is 2.0 PM (approximately 8 personsweek).
2. Development II: A second round of development after the primary certification, UCST testing and users feedback. Presently, it is not possible to estimate the effort for this second development phase without knowing in advance the bugs and problems observed during the tests. This second phase is expected to start at the beginning of February 2012 , and concluded at the end of February 2012.

Development I assumes that the proposed VO Operations Portal will be deployed as a module of the Operations Portal. The main advantage is that the basic components technology is already available (Lavoiser adapters already exist), and the data sources and their APIs are provided within the framework of the project and operated by different EGI-InSpire partners. The major effort will be distributed according to the tasks presented in the following table, and estimated to be delivered on:

- extending the Lavoiser web service for the retrieving data from the sources and treating it properly;
- development of a new Web interface for the dashboard itself, the Metrics parts and the Handover part;
- Implementation of authentication and controlled access to the tool.

Tasks for phase Development I	Estimated required effort (personweek)
Data connection and treatment	**1**
Interface developments	**4**
Overview part (dashboard)	2
Metrics part	1
Handover Part	1
Authentication and control access	**1**
Notepad and tickets creation	**2**
TOTAL EFFORT	**8**

4.2 Test and certification

The testing and certification work for the VO Operations Portal will be carried out in two sequential phases, after Development I:

1. Testing I, an intensive testing phase in order to check if the functionalities of the tool are in agreement with the delivered requirements. The main tests will focus on how the VO Operations Portal will be able to deliver the proposed end-user functionalities and monitor the overall performance. This phase will follow a dedicated test plan (depicted in the following table) executed by the VO Services Team @ LIP under TNA3.4. It is expected to take 2 personsweek, starting with the release of the first version (January 2012) and is ending two weeks later.
2. Testing II, representing the testing and reviewing that UCST will be doing under TNA3.2. It will start after Testing I finishes and should end at the beginning of February 2012 (this deadline should be sufficiently flexible to allow to collect feedback from different user communities).

#	Type	Test Description
1	Authentication & Authorisation	Test access and check error messages generated in different scenarios: • access without a valid user certificate. • access with a valid user certificate.
2	Authentication & Authorisation	Test access and check error messages generated in different scenarios: • access without proper VO role. • access with proper VO role.
3	Functional	Evaluate the Web interface functionalities and the synoptic view. • Check how functional it is is terms of end-user usability. • Browse through the information displayed for all alarms, notepads, handovers, downtimes, etc.. and confirm the accuracy of the displayed information. • Check that the information gathered for the sites (downtimes, nodes, services, downtimes etc...) is correct comparing it directly from various different sources • Provide feedback to the developers
4	Functional	Check the validity of the VO Dashboard alarms. • Are the alarms displayed in the VO Operations Portal coherent with real failures tests in the VO SAM? • Are there notifications in the VO SAM that are not displayed in the VO Operations Portal?
5	Functional	Configure the VO Operations Portal to show a subset of VO SAM notifications (alarms). Confirm that the functionality is working checking that generated alarms correspond to the set of selected VO SAM tests.
6	Functional	Send a notepad to a given site. • Check that the notepad is received • Check if it becomes available in the notepad history.
7	Functional	Send an handover to another VO staff. • Check that the handover is received

		• Check if it becomes available in the handover history.
8	Functional	Open a trouble ticket to a site in EGI Helpdesk via the VO Operations Portal for a site with an open alarm. • Check if the provided templates are adequate to the foreseen action. • Update/Close the ticket opened via the Dashboard.
9	Functional	Generate metrics on demand. • Check the validity of the information gathered and the quality of the produced information. • Provide feedback to the developers about new metrics.

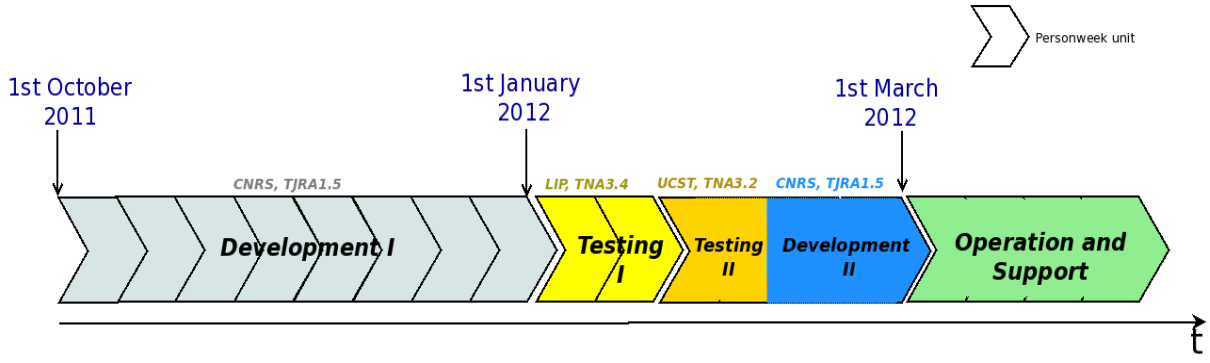
4.3 Operation and support

The proposed VO dashboard will be a module of the Operations Portal with a central entry point per VO (http://operations-portal.egi.eu/VoDashboard/Voname). All the 3 architecture components are already deployed and in production, and the versions supporting the new VO Operations Portal instance will be introduced through an EGI Operations Portal release once the development, test and certification activities are completed.

Support will be provided by the VO Services and EGI Operations Portal Teams via EGI Helpdesk, and in coherence with the EGI Operations Portal work-plan.

4.4 Timeline

The following diagram presents the expected work-plan timeline.



5 CONCLUSION

The VO Operations Portal is a tool foreseen to empower VOs with a service necessary to deliver the best possible availability for end users. The proposal is to make it accessible as a module of the EGI Operations Portal, with a central instance with an entry point per VO (http://operations-portal.egi.eu/VoDashboard/Voname). All VOs with a VO SAM Nagios Box will be able to have immediate access to such dashboard. Since the architecture of the tool is strongly based on the Operations Dashboard components already used in operations, the effort on its development is based on extending the current components according to the delivered requirements. The development and testing phase is expected to take 8personsweek in total.

6 REFERENCES

R 1	https://documents.egi.eu/document/31
R 2	https://wiki.egi.eu/wiki/VO_Service_Availability_Monitoring
R 3	https://rt.egi.eu/guest/Ticket/Display.html?id=1800
R 4	H. Cordier et al, "From EGEE Operations Portal towards EGI Operations Portal", Proceedings of ISGC 2010. Also available at http://cic.egi.eu/common/all/documents/Portal_documentation/2010_03_10_CLO_OPERATIONS.pdf
R 5	S. Reynaud et al,"Lavoiser: A Data Agregation and Unification Service", Proceedings of CHEP06. Also available at http://cic.egi.eu/common/all/documents/Portal_documentation/Lavoisier_CHEP06_paper.pdf