

Accounting Portal Availability and Continuity Plan

Main	EGI.eu operations services	Support	Documentation	Tools	Activities	Performance	Technology	Catch-all Services	Resource Allocation	Security
------	----------------------------	---------	---------------	-------	------------	-------------	------------	--------------------	---------------------	----------

Documentation menu:	Home •	Manuals •	Procedures •	Training •	Other •	Contact ►	For:	VO managers •	Administrators
----------------------------	--------	-----------	--------------	------------	---------	-----------	------	---------------	----------------

Back to main page: [Services Availability Continuity Plans](#)

Introduction

This page reports on the Availability and Continuity Plan for the **Accounting Portal** and it is the result of the risks assessment conducted for this service: a series of risks and treats has been identified and analysed, along with the correspondent countermeasures currently in place. Whenever a countermeasure is not considered satisfactory for either avoiding or reducing the likelihood of the occurrence of a risk, or its impact, it is agreed with the service provider a new treatment for improving the availability and continuity of the service. The process is concluded with an availability and continuity test.

	Last	Next
Risks assessment	2018-05-03	2019 May
Av/Co plan and test	2018-05-28	2019 May

Hardware HA Configuration

- The Accounting Portal service is available in a dedicated virtual machine running in the CESGA cloud framework based on OpenNebula software, which offers high availability thanks to its resources:
 - A pool of physical servers where the virtual machine can run. Over 50 servers with 24 cores and 32GB per server are available. These servers are configured with redundant power supply and two disks in RAID-1 configuration.
 - Storage is provided in a NetApp HA storage solution, providing redundant configuration for data movers (servers) and RAID-TEC (triple parity) protection for the disks; the backup of this storage is performed on a daily basis

Performances

The performances reports in terms of Availability and Reliability are produced by ARGO ^[1] on an almost real time basis and they are also periodically collected into the Documentation Database ^[2].

In the OLA it was agreed the following performances targets, on a monthly basis:

- Availability: 99%
- Reliability 99%

Over the past years, the Accounting Portal hadn't particular Av/Co issues highlighted by the performances that need to be further investigated.

Risks assessment and management

For more details, please look at the google spreadsheet ^[3]. We will report here a summary of the assessment.

Risks analysis

Risk id	Risk description	Affected components	Established measures	Risk level	Expected duration of downtime / time for recovery	Comment
1	Service unavailable / loss of data due to hardware failure	All	All services are running on virtual machines. In case of hardware failure of the host machine the virtual machine can be re-instantiated in another hypervisor in the private cloud. Daily backups of the service including database data.	Low	In case an instance must be instantiated from backups can take up to two-three working hours. In case latest backups are not available some data must be re-generate from the central accounting repositories and this may take up to two hours.	the measures already in place are considered satisfactory and risk level is acceptable
2	Service unavailable / loss of data due to software failure	All	Restoring of the codebase via git repository	Low	One to two working hours	the measures already in place are considered satisfactory and risk level is acceptable
3	service unavailable / loss of data due to human error	All	Restoring of the codebase via git repository, restore of backup of virtual machine, restoring of data from SSM services.	Low	Two to Three working hours.	the measures already in place are considered satisfactory and risk level is acceptable
4	service unavailable for network failure (Network outage with causes external of the site)	Web frontend	CESGA has redundant network connectivity to the NREN	Low	Close to zero, less than one hour.	the measures already in place are considered satisfactory and risk level is acceptable
5	Unavailability of key technical and support staff (holidays period, sickness, ...)	All	More personnel have been involved in the operation of the Accounting portal, this ensures actions taken within the OLA goals every working day. There is also internal documentation with management procedures and portal architecture.	Low	Within the OLA targets for operational actions Longer periods in case of bugs or maintenance (one week) because not all the personnel can develop patches to the code.	the measures already in place are considered satisfactory and risk level is acceptable

6	Major disruption in the data centre. Fire, flood or electric failure for example	All	The computing centre has electric backup system and fire control devices. In case of an occurrence despite the controls, the virtual machine can be instantiated elsewhere.	Low	1-2 weeks, the time to deploy recover operational status at CESGA or the service to another resource centre partner of the NGI	the measures already in place are considered satisfactory and risk level is acceptable
7	Major security incident. The system is compromised by external attackers and needs to be reinstalled and restored.	Frontend and DB	Daily backup are executed. Backup is stored in a separate system and can be restored in another VM	Low	1-2 work hours. In case new host certificates are required, up to 2 days.	the measures already in place are considered satisfactory and risk level is acceptable
8	(D)DOS attack. The service is unavailable because of a coordinated DDOS.	Web interface	NREN provides protection for DOS attacks, firewall can limit impact of the DDOS	Low	Depending on the attack, few hours maximum	the measures already in place are considered satisfactory and risk level is acceptable

Outcome

The level of all the identified risks is acceptable and the countermeasures already adopted are considered satisfactory

Availability and Continuity test

The proposed A/C test will focus on a recovery scenario: the service is supposed to have been disrupted and needs to be reinstalled from scratch. Typically this covers the risks 1,2, and 7. The last backup of the data will be used for restoring the service, verifying how much information will be lost, and the time spent will be measured.

Performing this test will be useful to spot any issue in the recovery procedures of the service.

Test details

references in the RT ticket 14308 ^[4]

```
10:45 CEST -> poweroff of the original machine (accounting-devel-next)
11:05 CEST -> Power on for the template (minimal) machine for recovery
12:00 CEST -> Data recovery completed
12:10 CEST -> Boot restoration and miscelaneous comprobations.
12:15 CEST -> Recovered machine rebooted and services on line
```

The recovery took about **70 minutes**.

Test outcome

The test can be considered successful: the service can be restored in few time and there are no loss of data. Even if the service is not available for few hours or a day, this can be considered acceptable: the portal is used for displaying and collecting accounting information, the other infrastructure services are not depending on it. Only infrastructure/operations centres/resource centres/VOs managers would suffer of a temporary disruption of the service.

Revision History

Version	Authors	Date	Comments
	Alessandro Paolini	2018-05-03	first draft, discussing with the provider
	Ivan Diaz, Alessandro Paolini	2018-05-28	added a paragraph about HA configuration; added information about the test
	Alessandro Paolini	2018-08-15	added the paragraph Test Outcome, plan finalised

References

- [1] <http://egi.ui.argo.grnet.gr/egi/OPS-MONITOR-Critical>
- [2] <https://documents.egi.eu/public/ShowDocument?docid=2324>
- [3] <https://docs.google.com/spreadsheets/d/1rB6JSywfXVZ9GIIHWo1askSRz8oRMC9DzkW9LLVJ898/edit#gid=1681174663>
- [4] <https://rt.egi.eu/rt/Ticket/Display.html?id=14308>

Article Sources and Contributors

Accounting Portal Availability and Continuity Plan *Source:* <https://wiki.egi.eu/w/index.php?oldid=102129> *Contributors:* Apaolini, Ivandiaz