



## LCG Operations Workshop

# *LCG VOBox Operations Recommendations and Questionnaire*

<i>Date:</i>	<b>30 September 2005</b>
<i>EDMS Reference:</i>	EDMS authorization applied for.
<i>Internal Version:</i>	<b>0.1</b>
<i>Status:</i>	<b>Draft</b>
<i>Author:</i>	<b>Steve Traylen</b>

Document Log			
Issue	Date	Author	Comment
0.1	30-Sep-05	Steve Traylen	Initial version

## Table of Contents

LCG Operations Workshop.....	1
<i>LCG VOBox Operations Recommendations and Questionnaire</i> .....	1
1 Introduction.....	3
2 Definitions .....	3
3 Operational Security Concerns .....	3
4 Hardware Resources .....	3
5 Network Connectivity.....	3
6 Monitoring the Service .....	3
7 Business Impact of the Service.....	4
8 Service Interventions .....	4
An Operational assessment questionnaire for VOs .....	5

## References

- [1] LCG/EGEE Security Policy Documents' Adhoc-Service-Systems-Security-Policy  
<https://edms.cern.ch/document/639856/>

## 1 Introduction

The concept of the VO dedicated systems or VO Boxes has introduced new operation scenarios due to the split responsibility and knowledge about what may be a critical service at a particular site.

This document describes recommendations to Site Managers from an operational point of view to implement a VO Box at a particular site.

For Virtual Organisations proposing to use VO Boxes it lists recommendations and procedures that must be adhered to, as well as details of what information to make available to the Site Managers in order to assess the best method of operation for a VO Box.

## 2 Definitions

The term *VO Box (Ad-hoc Service System)* designates a system provided by a site for use by one or more designated Virtual Organisations (VOs) for interactive access and running persistent processes. The terms MUST, SHOULD, MAY and MAY NOT must be interpreted according to RFC 2119.

## 3 Operational Security Concerns

Before any VO Box enters operation at any site the recommendations of the Joint Security Policy Group for VO Boxes will be adhered to as they are described in [1].

## 4 Hardware Resources

A clear indication from the VO of the hardware resources MUST be given. In particular these should include the obvious requirements of memory and disk space. In the case of disk space should this space be on the local hardware or is some networked file system acceptable? Some indication as to the CPU saturation that the service may use when running normally should be supplied. Is spare CPU capacity required in order to ensure a low latency in any service response time?

The site may like to co-locate VO service boxes on a single piece of hardware in order to make better use of resources. This may be done using hardware vitalisation techniques, a secondary virtual IP interface or just a single VO Box enabled for and accepting VO services from multiple VOs. For each of these co-locating methods the VO must give technical reasons why any of these co-locating solutions could not satisfy their needs for a VO box. The sites should provide dedicated physical hardware where the load from any one VO is such that it degrades the performance of other VOs. However it is assumed by sites that any one VO will never require more than one dedicated VO box at site.

## 5 Network Connectivity

When deploying a VO Box sites should consider the most suitable location within their network topology for deploying such a service. While [1] will provide a complete set of network connections to and from any VO Box this will not provide any data rates for these connections. Consideration should be taken into account especially if any VO service is expected to transport large quantities of data where private routes are reserved solely for bulk data transfers. Special routes exist between some T1s and the T0 which require host level configuration to be added.

Sites are encouraged to use the network port lists provided by [1] to enforce the required level of access. Tools such as IPTables to restrict protocol/source and destination of network connections and SELinux can be used to restrict particular users and binaries to particular ports.

## 6 Monitoring the Service

Since the VO Box and the services running inside are managed distinctly by both the local site administrators and the VO service managers there must be a clear distinction between the responsibilities of the two groups. The site is responsible for the operating system and for all services that are provided by a VO Box before a VO accesses and installs any of its VO services on the VO box. The site will monitor a VO Box for common failures such as kernel crashes, disk i/o errors, disk space, etc. In certain cases the site may then believe that a full disk or other failure is caused by a particular VO service and so will notify the VO service manager who is

then responsible for correcting the situation. The working operation of the VO service must be monitored and maintained by the VO.

## 7 Business Impact of the Service

Sites should assign a level of service to VO boxes after considering the impact of a VO Box being unavailable. The VO is best placed to understand how any loss of a VO Box is likely to impact the VO as a whole. For instance, will the site be unable to run jobs? Will the site drop out a particular class of new job submissions such as analysis jobs? The VO should provide this information.

In the case where the service has been completely lost due to a complete hardware disk failure or similar then as a minimum the site is responsible for returning an empty VO box into production in a timely fashion. Individual sites expect prior agreement for any additional action such as a nightly backup. The VO should state in advance if anything other than a reinstallation of the VO Box is required when there has been a complete service loss.

## 8 Service Interventions

At certain times sites will have to intervene with any service for planned maintenance such as hardware failures or operating system upgrades. These would normally be planned and published in advance but may happen immediately where security implications are present. Clear agreed lines of contact with the VO must be put in place either by named individuals or standard routes such as GlueSchema flags or broadcasts to VOs. The method must be defined and agreed in advance.

## An Operational assessment questionnaire for VOs

The answers to this questionnaire must be available to the *Site Managers* at all times. The information provided here MAY be stored in an on-line repository, accessible to all *site managers*. Specific *Sites* MAY require the information below and (at their discretion any additional information) to be sent explicitly to them.

By submitting this questionnaire or by using any service provided by a VO box service system, the VO maintainer agree that their personal information will be shared with all *Sites* and shall be used for administrative and operational purposes only.

### Name of the Virtual Organisation:

### Name and contact details of the maintainer:

Name:

Email address:

Phone number(s):

1. **What are the hardware requirements for your VObox?** (*Example – A node comparable to your site's fastest batch workers is sufficient. Twenty GigaBytes of possible network attached disk space is required.*)
2. **Can the VO Box for your VO be co-located on the same physical hardware as another VOs VO Box?** (*Example – This is not possible since we require our services to bind to a particular port that cannot be altered or can not bind to a particular network interface.*)
3. **How should the VO box be recovered after a complete loss?** (*Examples – A reinstallation of a vanilla VO Box with no VO additions is acceptable. A recovery from a nightly backup is required.*)
4. **What are the expected network requirements of the VO box?** (*Examples – Only command and control operations will take place so just the standard production network is required. All data access will be channelled through the VO box. )*
5. **What is the business impact for the failure of VO Box?** (*Examples – All jobs at the site will be lost. We will be unable to submit new work to this particular site. We will be unable to access any existing data at this site. )*
6. **How should the VO be contacted for service interventions?** (*Examples – Via a mailing list. Via an EGEE broadcast. Via status tags in the GlueSchema.*)



