Joint Security Policy Group

Ad-hoc Service Systems Security Recommendations and Questionnaire

Date:	**21 September 2005**
EDMS Reference:	https://edms.cern.ch/document/639856/
Internal Version:	**0.5**
Status:	**Draft**
Author:	**David Groep**

Document Log			
Issue	**Date**	**Author**	**Comment**
0.1	12-Sep-05	David Groep	Initial version
0.2	15-Sep-05	David Groep, MWSG	Improved
0.4	19-Sep-05	David Groep	Incorporated comments from IanN and from the GridPP slides by Steve Traylen
0.5	21-Sep-05		Incorporated comments by Joel Closier , Alessandra Forti

Table of Contents

References

[1] LCG/EGEE Security Policy Documents' Glossary of Terms, Ian Neilson et al.
https://edms.cern.ch/document/573613

[2] Audit Requirements, Ian Neilson et al.
https://edms.cern.ch/document/428037

1 Introduction

Since the concept of the VO dedicated systems or other temporary, ad-hoc service boxes introduces new threats and security incident scenarios, by virtue of allowing interactive login and the ability to run long-running service instances, specific security recommendations and policies for VO boxes are appropriate.

This document describes recommendations to Site Managers, from a security point of view, to implement with respect to the VO Dedicated Systems.

For Virtual Organisations proposing to use VO Boxes it lists recommendations and security policies that must be adhered to, as well as the information to make available to the Site Managers in order to assess the security and risks of the VO box.

2 Definitions

The italicized terms in this document refer to definitions in the *LCG/EGEE Security Policy Documents' Glossary of Terms* [1]. The term ***Ad-hoc Service System (VO Box)*** designates a system provided by the 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 Access to and services on the VO Box

The operating system on the VO Box will be installed and maintained by the Site Resource Administrators, according to their current best practice, as the VO Box is part of the trusted network fabric of the Site. The Site Manager is thus responsible for maintaining the integrity and functionality of the base operating system, and therefore privileged (root) access to the system MUST be limited to the Resource Administrators, notwithstanding any additional site policies that may be in effect.

The Site cannot assume liability for the VO's actions, and thus the VO administrators will not get access to a host certificate-key pair. There may be a host certificate-key pair available on the box, but any VO services will then need to be part of a site-provided apache or tomcat container or be able to work based on proxy certificates of the host credential, or use a dedicated service credential issued to the VO, e.g. based on host aliases in a domain assigned to the VO.

For manageability reasons, the base operating system on the VO dedicated system is expected to follow the OS profile of other systems provided by the Site, in particular the Worker Node profile. No other service level should be assumed unless additional prior agreements have been reached with the *Site*, e.g. sites MAY or MAY NOT offer backup facilities.

Interactive access to the VO box, and the capability to run services on the system, MUST be limited to a specific, named list of individuals within the VO. These individuals MUST have user-level access only. To ensure traceability, these accounts MAY be mapped to distinct accounts for each named individual, at the site's discretion.

The VO MUST designate security and operational responsible persons for their services. Typically, these two roles will be separate. The security responsible SHOULD be registered according to the Incident Handling and Response Guide.

4 Logging and traceability

Contrary to jobs run by VO users on worker nodes, the VO box provides the option to run *services*, to be contacted by remote clients, within the trusted site network. When such services are provided by the VO, these service implementations MUST comply with the same security recommendations and best practices like other grid middleware and base OS services. In particular

- All interactions of the service MUST be logged, and these logs MUST include time-stamped information regarding its client (peer IP protocol, address and port, specific client subject name)
- When multiple services are involved in handling/processing the request, a common request identifier MUST be used by all services, or appropriate "link" identifiers logged on inter-service hand-over.

- The logging SHOULD be redirect-able, at the site's discretion, to syslog(8) to make sure that it can be stored in a tamper-resistant way.
- Logging data in VO-managed files SHOULD be retained for the period specified in the *Audit Requirements*[2]
- In the processing of identity certificates, Certificate Revocation Lists and subject namespace constraints SHOULD be honoured.

Preferably, the service SHOULD implement a blacklisting capability for individual client subject names, to be configured by the site. If such a mechanism is absent, the site will be required to disable the entire VO box in case of incidents.

If the VO collects information regarding other *Services* or *Grid Services* at a *Site* that are not operated by the VO on the VO Box, the VO MUST provide details regarding

- what is being monitored at the *Site*
- what is being stored
- what is being published (and to whom, and secured via which mechanism)?

5 Network Connectivity

The network connectivity to and from the VO Box will be managed and contained according to site policies. In particular, inbound connectivity to privileged ports is prohibited.

- connectivity on the VO box will generally be managed and contained
- the VO must document specific connectivity requirements. In particular, they should answer the following questions (preferably via the questionnaire in appendix A):
    - do you need connectivity to the outside networks from this box? (and if so, to what destinations and to which ports)
    - do you need inbound connectivity from outside networks **to** the box? (and if so, from which destinations and to which ports)?
        - Are these connections secured and authenticated? If yes, via which protocols, if not, why not?
        - Are connections logged? And how & to where?
    - do you need connectivity to other systems inside the site (and if so, to what systems, and to which services/ports)?
    - will jobs running at the site try to contact this box? If so, at what ports/services? Does this also hold if the worker nodes have outbound IP allowed?
- The connectivity requirements must reflect actual current use by the VO's services. Each connectivity request must be accompanied by a service description (and a protocol description where available), as well as a description of the security level (plain-text, encrypted via a pre-shared secret, client or server authentication encrypted re-useable tokens, idem via client-authenticated TLS or GSI, one-time tokens).
- VOs may request a specific port, but this will not guarantee actual assignment of the specific port requested. For operational reasons, or in case the port has already been assigned to a different service, an alternate port may be assigned. VO software must be able to handle such alternate assignments.

6 Security Service Challenges

The VO box (and thereby the VO box maintainer and security responsible) will be subject to security service challenges. These security service challenges follow the model used for the security service challenges directed towards sites. They typically include (but are not limited to) exercise of the operational incident management procedures, probes to assess the accurateness of contact information (including contacting any out-of-office hours phone numbers), and challenges to trace incidents to specific end-entities.

A Security assessment questionnaire for VOs

The answers to this questionnaire must be available to the *Site Managers* and the *Site Security Officers* at all times. The information provided here MAY be stored in an on-line repository, accessible to all *site managers*. Specific *Site*s 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 an Ad-hoc Service System, the VO maintainer and the VO security responsible agree that their personal information will be shared with all *Sites* and shall be used for administrative, operational and security purposes only.

Name of the Virtual Organisation:

Name and contact details of the maintainer:

Name:

Email address:

Phone number(s):

Name and contact details of the VO security responsible

Name:

Email address:

Phone number(s):

Out-of-office hours phone number:

We, the VO maintainer and the VO security responsible, take responsibility for all services running on the VO box running under the VO's system credentials, and for all actions, events and incidents resulting directly or indirectly from the programmes running on the Ad-hoc Service System under the VO's user or group system identity.

This Questionnaire contains two additional tables:

- Network and Service Table
- Information Monitoring and Publication Table

Network and Services Table

(this is an example, please modify to reflect your actual current use)

Service	**Protocol and ports**	**Targets (choose):** • **specific range** • **local site** • **WNs only**	**Description**	**Logging location(s)**
gsissh	1975/tcp security: GSI	Inbound from 137.138.0.0/16 and 192.16.186.192/26	Interactive login service secured via GSI	Via syslog at level authpriv.notice
xrootd	5443/tcp security: TLS	Bidirectional from WNs and from 137.138.0.0/16	File transfer service for *xxx*, called from jobs running on the worker nodes. The protocol is described in *document.* The network access pattern is *yyy*.	$VO_SW_DIR/log/xrootd.log.*

Explanation of table entries:

- **Service** – short name of the service
- **Protocol and ports** – protocol (TCP/UDP) and the port number. A reference to the protocol description should be supplied if it's not a "standard" protocol (i.e. one that can be found in the an IETF RFC of GGF GWD).

  Indicate the "security level" of the protocol: plain-text, encrypted via a pre-shared secret, client or server authentication encrypted re-useable tokens, ibidem via client-authenticated TLS or GSI, one-time tokens, ...
- **Targets** – how will the port/protocol be accessed. Is it outbound *from* the VO box or inbound *into* the VO box? What network(s) will contact the box/be contacted by the box? Specify at least one (or more) of "world", "specific range" (and indicate the range. Standard CERN fixed networks are in 137.138.0.0/16), "local site" (i.e. all machines into the LCG-related network segments inside the site hosting the box), or "WNs only" (only worker node machines inside the site's network).
- **Description** – A short description of the service, including the foreseen network access pattern (so that anomalies can be detected by the site and local IDS systems tailored to monitor the traffic).
- **Logging destinations** – a description of the logging by the service (a *must* in case of a service providing a service to the world or specific network ranges), and the destination of the logging entries (syslog, file, …)

Information Monitoring and Publication Table

(this is an example)

Monitored Item	**Storage**	**Publication**	**Security**
Free disk space in $VO_SW_DIR, every 5 minutes	Not stored locally	Published via R-GMA in table *X*, to the authenticated world	R-GMA security: authenticated users only
VObox system load, every 15 minutes	$VO_SW_DIR/logs/load.log	Not published	File system, mode 0660