EGI.eu

SECURITY POLICY FOR THE ENDORSEMENT AND OPERATION OF VIRTUAL MACHINE IMAGES

Document identifier	EGI-SPG-VMEndorsementOperation-771-V1
Document Link	https://documents.egi.eu/document/771
Last Modified	04/09/2011
Version	1
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	Romain Wartel/CERN, David Kelsey/STFC
Document Type	Policy
Document Status	REVIEW
Approved by	Body who approved the doc
Approved Date	DD/MM/YYYY



Policy Statement

This security policy describes the security-related policy requirements for the generation, distribution and operation of virtual machine images on the infrastructure.

I. AUTHORS LIST

	Name	Partner/Activity/ Organisation/Function	Date
From			

II. DELIVERY SLIP

	Body	Date
Reviewed by	TCB	DD/MM/YYYY
Reviewed by	OMB	DD/MM/YYYY
Reviewed by	UCB	DD/MM/YYYY
Approved by	EGI.eu Director	DD/MM/YYYY
Approved by	EGI.eu Executive Board	DD/MM/YYYY

III. DOCUMENT LOG

Version	Date	Comment	Author/Organization
1.0	04/09/2011	SPG Phase 2 version - External draft	Romain Wartel/CERN, David Kelsey/STFC
2.0			

3.0			
4.0			

IV. APPLICATION AREA

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI.eu "Policy Development Process" (https://documents.egi.eu/document/169).

VI. ORGANISATION SUMMARY

To support science and innovation, a lasting operational model for e-Infrastructure is needed – both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) in order to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

In its role of coordinating grid activities between European NGIs, EGI.eu will:

- Operate a secure integrated production grid infrastructure that seamlessly federates resources from providers around Europe
- Coordinate the support of the research communities using the European infrastructure coordinated by EGI.eu
- Work with software providers within Europe and worldwide to provide high-quality innovative software solutions that deliver the capability required by our user communities
- Ensure the development of EGI.eu through the coordination and participation in collaborative research projects that bring innovation to European Distributed Computing Infrastructures (DCIs)

The EGI.eu is supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI.eu will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

EGI will collect user requirements and provide support for the current and emerging user communities. Support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 SECURITY POLICY ON THE ENDORSEMENT AND OPERATION OF VIRTUAL MACHINE IMAGES

1.1 Introduction

This document describes the security-related policy requirements for the generation, distribution and operation of virtual machine (VM) images on the infrastructure.

The aim is to enable VM images to be generated according to best practices and to be both trusted and operated elsewhere.

This policy does not compel resource centres to instantiate images endorsed in accordance with this policy nor limit the rights of a resource centre to decide to instantiate a VM image generated by any other non-compliant procedures, should they so desire. The resource centre is still bound by all applicable security policies and is required to consider the security implications of such an action on other participants.

1.2 Definitions

The following terms are defined.

- **Endorser**: A role, held either by an individual or a team, who is responsible for confirming that a particular VM image has been produced according to the requirements of this policy and states that the image can be trusted. An Endorser should be one of a limited number of authorised and trusted individuals appointed either by the infrastructure, a VO or a resource centre. The appointing body must assume responsibility for the actions of the Endorser and must ensure that he/she is aware of the requirements of this policy.
- **VM operator**: A role, held either by an individual or a team, who is responsible for the security of the VM during its operation phase, from the time it is instantiated, until it is terminated. Typically this addresses individuals with root access on the VM.
- **Third party**: An external entity other than the resource centre where the VM is operated.

All other terms are defined in the Glossary [R1].

1.3 Use case classification

This policy document addresses the following use cases.

1.3.1 Endorser: resource centre, VM operator: resource centre

In this class, virtualisation is not directly accessible by users. It includes, for example, the use of virtual worker nodes that act in a similar way to real worker nodes.

The resource centre is both the Endorser and the VM operator and is responsible to ensure the compliance of the VM with existing security policies.

1.3.2 Endorser: Third party, VM operator: resource centre

In this class, the resource centre is the VM operator, and the trust relationship is established between the resource centre and the Endorser.

1.3.3 Endorser: Third party, VM operator: Third Party

In this class, the resource centre runs the VM but is not the VM operator, and the trust relationship is established between:

- the resource centre and the VM operator
- the VM operator and the Endorser (both roles can be combined)

The resource centre is responsible to ensure sufficient traceability in order to enable malicious network activity to be linked with any VM and its VM operator, as defined in the Security Traceability and Logging policy [R2].

The resource centre has no direct trust relationship with the Endorser and may decide to apply specific restrictions to control the access of the VM to other resources, including network services.

1.4 Policy Requirements on the VM Operator

By acting as a VM Operator you agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time:

- You are responsible to fulfil all the operational security and incident response requirements expressed in other policies [R3].
- You are responsible to ensure that any VM being run is currently endorsed and to ensure its compliance with existing security policies, including but not limited to security patching, vulnerability management, incident response, logging and traceability.
- You are responsible for handling all problems related to the execution of any licensed software in a VM image. You shall ensure that any software run in a VM, complies with

applicable license conditions and you shall hold the resource centre running the image free and harmless from any liability with respect thereto.

- You are responsible for contextualising any endorsed image, including credentials and certificates.

1.5 Policy Requirements on the Endorser

By acting as an Endorser you agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time:

- You are held responsible by the infrastructure and by the resource centres for checking and confirming that a VM image has been produced according to the requirements of this policy and that there is no known reason, security-related or otherwise, why it should not be trusted.
- You recognise that the VM must be generated according to current best practice, the details of which may be documented elsewhere by the infrastructure. These include but are not limited to:
    - any image generation tool used must be fully patched and up to date;
    - all operating system and other installed software security patches must be applied to all images and be up to date;
    - images are assumed to be world-readable and as such must not contain any confidential information;
    - there should be no installed accounts, host/service private keys, ssh private keys or user credentials of any form in an image;
    - images must be configured such that they do not prevent resource centres from meeting the finegrained monitoring and control requirements defined in the Security Traceability and Logging policy [R2] to allow for security incident response;
    - the image must not prevent resource centres from implementing local authorisation and/or policy decisions, e.g. blocking the running of work for a particular user.
- You must disclose to the infrastructure or to any resource centre on request the procedures and practices you use for checking and endorsing images.
- You must provide and maintain an up to date list of your currently endorsed images together with the metadata relating to each VM image.
- Either the list or each individual image's metadata must be digitally signed by the endorser.
- You must keep an auditable history of every image endorsed including the date/time of generation and full list, including exact versions, of installed software and operating system contained in the VM. This must be made available to resource centres on demand.
- You must implement a removal or revocation procedure to allow the VM operators to exclude those images which are no longer endorsed. This procedure must be implemented whenever a problem is found, e.g. a new security update is required. This removal must also be recorded locally in your auditable history.
- You are responsible for handling all problems related to the distribution of any licensed software in a VM image. You shall ensure that any software distributed in a VM image, complies with applicable license conditions and you shall hold the resource centre running the image free and harmless from any liability with respect thereto.

- You must assist the infrastructure in security incident response and must have a security vulnerability patching process in place.
- You recognise that the infrastructure, the resource centres, and/or the VOs reserve the right to block any endorsed image or terminate any instance of a virtual machine and associated user workload for administrative, operational or security reasons.
- You recognise that if a VM operator runs an image which is no longer endorsed, you are not responsible for any consequences of this beyond the time of your removal of the endorsement.

2 REFERENCES

R 1	EGI Glossary. https://wiki.egi.eu/wiki/Glossary_V1 SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71
R 2	Grid Security Traceability and Logging Policy. https://documents.egi.eu/document/81
R 3	Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents
R 4	
R 5	




e-infrastructure