# Policy Trusted Virtual Machines

### From JSPGwiki

***Draft policy document - not yet approved or adopted.***

This is Draft Version 1.2 (21 April 2010) - for discussion at the HEPiX Virtualisation working group meeting on 22/23 April 2010.

**Table of contents**



# 1 Policy on the Generation of Trusted Virtual Machine Images for Use on the Grid

This document describes the security-related policy requirements for the generation of trusted virtual machine (VM) images for use on the Grid.

The aim is to enable Grid Sites to trust and instantiate VM images that have been generated elsewhere.

This policy does not limit the rights of a Site to decide to instantiate a VM image generated by any other non-compliant procedures, should they so desire. The Site is still bound by all applicable Grid security policies and is required to consider the security implications of such an action on other Grid participants.

# 2 Definitions and Scope

The following terms are defined.

- **VM base image**: A VM image, including a complete operating system and all required general libraries, compilers, programmes and utilities. All kernel and root-level configurations, including any that may be VO-specific, are included here.
- **VO configuration**: The Virtual Organisation specific application software, libraries, utilities, data and configuration which may be added to a VM base image necessary to provide the appropriate environment for use by members of the VO. No kernel modifications or root-level configurations are included here.
- **VM combined image**: The VM image resulting from the combination of the VM base image and the VO configuration (if any). If there is no VO configuration, the VM combined image is identical to the VM base image.
- **Tag**: A name uniquely identifying a VM combined image.

The following roles are defined. A particular individual may be authorised to carry out more than one role.

- **Image producer**: An individual generating VM base images.
- **VO producer**: An individual generating VO configurations.
- **Image combiner**: An individual combining VM base images and VO environment configurations to produce a VM combined image.
- **Endorser**: An individual who confirms that a particular VM base image or VO configuration or VO combined image has been produced according to the requirements of this policy and states that the

image can be trusted.

This policy addresses the following model of generation:

- A VM base image is generated by one of a limited number of authorised and trusted image producers. The authorisation is granted by a Site.
- A VO configuration is generated by one of a limited number of authorised and trusted VO producers acting on behalf of the VO. The authorisation is granted by the VO.
- A VM combined image is generated by one of a limited number of authorised and trusted image combiners. The authorisation is usually granted by a Site.
- A tag is assigned to each VM combined image.

# 3 Policy Requirements

By acting as an **Endorser** of a trusted virtual machine image and/or VO configuration for use on the Grid, you agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time.

1. You are held responsible by the Grid and by the Sites for checking and confirming that an image or configuration has been produced according to currently accepted best practices, that the image meets the requirements of this policy and that there is no reason, security-related or otherwise, why it should not be trusted for use on the Grid.
2. You must disclose to the Grid or to any Site on request the procedures and practices you use for checking and endorsing images.
3. You must provide and maintain an upto date digitally signed list of currently endorsed images (i.e. their hashes). This list must have an issue timestamp and an expiration timestamp so that sites can be sure that older versions are not used.
4. You must keep an auditable history of every image or configuration endorsed including the name, date/time of generation and full list of OS/packages/versions. This must be made available to sites on demand.
5. You must remove images and configurations from the approved list if/when a problem is found, e.g. a new security update is now required. This removal must also be recorded locally in your auditable history.
6. You are responsible for handling all problems related to the inclusion of any licensed software in a VM image. You shall ensure that any software included in a VM image which is used for its intended purposes, complies with applicable license conditions and you shall hold the Site running the image free and harmless from any liability with respect thereto.
7. You recognise that VM base images, VO configurations and VM combined images, must be generated according to current best practice. These include but are not limited to:
    1. any image generation tool used must be fully patched and up to date.
    2. all operating system security patches must be applied to all images and be up to date.
    3. appropriate system audit logging must be configured.
    4. Images should not be pre-configured to obtain a workload. How the running instance of an image obtains a workload is a contextualization option left to the site at which the image is instantiated.
    5. Instantiated images should not be any more constrained, notably in terms of network access, than a normal worker node at the site at which the image is instantiated.
    6. There should be no installed accounts or user credentials of any form in an image.
    7. There should be no root access by users or VO's to any instantiated image.
    8. Images must be configured to meet fine-grained monitoring and control requirements defined in the Grid Security Traceability and Logging policy to allow for security incident response.
    9. The VM must request and respect the result of any local authorisation and/or policy decisions, e.g. blocking the running of Grid work for a particular user.
8. You must assist the Grid in security incident response and must have a vulnerability assessment process in place.
9. You recognise that the Grid and/or the Sites reserve the right to block any image or terminate any instance of a virtual machine and associated user workload that appear to be operating beyond their

authorisation and/or are not in compliance with this policy and/or other polices.
10. You recognise that if a Site runs an image which no longer appears on your list of endorsed images no longer endorsed, that you are no longer responsible for any consequences of this.

# 4 Discussion points

Still working on these instructions from the meeting of 12th April 2010: (currently the policy is open to one or more Endorsers)

The first version of the clause(s) should require a single endorser of the image (assumed, or explicitly stated, to be a worker node manager at the generating site who is considered to be responsible for the security of the base operating system portion of the image) with a requirement for the endorser to identify providers of additional software (notably VO software libraries).

The second version of the clause(s) should require explicit endorsement by contributor(s) of all additional software in addition to endorsement from the person responsible for the base operating system portion of the image. The second version of the relevant clause(s) must allow for the possibility that a single person could endorse multiple components of the overall image.

Other points to be discussed:

1. Do we need to assign any explicit liability to the Endorser?
2. Can we find an Endorser from the hash of an image or its tag? e.g. is there a Grid central image database?
3. Does there need to be a list of trusted Endorsers (maintained centrally)? Or does each site maintain this?
4. Each image must be uniquely identifiable and revocable (via a serial number? or just its tag?) and not replayable (therefore need monotonically increasing serial number)?
5. Must the image be signed and registered in a repository of images provided by the Grid? Or are we just creating hashes and signed lists of current good hashes?
6. Do we document current best practice elsewhere?

Retrieved from "http://www.jspg.org/wiki/Policy_Trusted_Virtual_Machines"

- This page was last modified 22:20, 21 Apr 2010.