Synnefo - Feature # 969

Status:	Closed	**Priority:**	Medium
Author:	Vangelis Koukis	**Category:**	Cyclades Images
Created:	07/29/2011	**Assignee:**	Nikos Skalkotos
Updated:	10/11/2011	**Due date:**	
Subject:	Remove all-host based processing of (potentially user-provided) Images		

Description

Currently, the Image deployment process does host-based processing of Images.
In the future, these Images will be custom, user-provided files. This will have major security implications.
More specifically:

- The host mounts the target filesystem.
- The host traverses directories in the target filesystem using its kernel-based filesystem implementation
- The host runs image-provided binaries in chroot, essentially trusting the potentially user-provided image completely.

This ticket will track moving to an architecture where the image is completely **untrusted**:

- All accesses to the image should be done programmatically, e.g. using library-based filesystem implementations, from unprivileged processes, with direct access to the underlying block device.
- The host should never run any user-provided binaries in its own context, they can be run completely isolated, e.g. in a container (LXC) or VM context (libguestfs).

Related issues:

related to Synnefo - Feature # 967: Monitor the number of blocks actually syn...	**Resolved**	**07/29/2011**
related to Synnefo - Feature # 1007: Use dd for deployment of Linux images	**Closed**	**08/04/2011**
blocks Synnefo - Feature # 991: Extend Synnefo mechanism to support custom Im...	**Assigned**	**08/03/2011**
blocks Synnefo - Feature # 491: Χειρισμός του συστήματος αρχείων νέων εικονικ...	**Closed**	**05/10/2011**

History

#1 - 10/11/2011 01:10 pm - Vangelis Koukis

- Status changed from Assigned to Closed

This has been implemented in the snf-image OS provider, https://code.grnet.gr/projects/snf-image.

After the initial host-based deployment of an Image, all customization happens inside a helper VM.
This ticket may close.