

# Some updates on FedCloud

V. Spinoso – E. Fernandez



- Checking the images with SECANT seems to be working but we need to be sure that the results are meaningful before bringing this to full production

The screenshot shows the Secant web interface at <https://appdb.egi.eu/store/vo/fedcloud.egi.eu/imagelist>. The interface displays a table of VAppliances with columns for Published, Available/Used VAppliances, VAppliance version updates, Messages, and Allowed Actions. A modal window is open over the 'EGI Centos 6' entry, showing a security report for version 2018.07.20. The report indicates that the current version failed to pass security checks. The failed checks are:

- NTP\_AMPLIFICATION\_TEST** (v1.0): Check failed to complete. test if image is vulnerable to network time protocol amplification attack.
- NMAP\_TEST** (v1.0): Check failed to complete. test open ports using nmap tool.

Other checks shown in the modal include:

- SSH\_AUTHENTICATION\_TEST** (v1.0): check if ssh authentication is allowed (passed).
- LYNIS\_TEST** (v1.0): Check skipped. run Lynis (Security auditing tool) inside the machine.
- PAKITI\_TEST** (v1.0): Check skipped. check installed packages with Pakiti3.

The security report was completed on 2018-07-20 17:51:01. The table also shows other VAppliances like EGI Centos 7, EGI Docker (Ubuntu 16.04), EGI FedCloud Clients, and EGI Small Ubuntu 16.04 for oring.

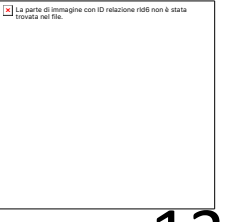
La parte di immagine con ID relazione r105 non è stata trovata nel file.

## Transition to Check-in

- How do we deal with user banning? Is ARGUS still the thing to use?
- How do sites know if a user is no longer in a VO and what to do with resources created by that user (i.e. how to do deprovisioning)?
- Do we have everything in place to trace the actual user from an incident happening at one site?

## Open issues

- Network has no unified policies: open-closed ports, public-private networks
  - A trend to move to OpenStack may at least unify the port managing and make it closed by default and user-manageable (so explicitly opening ports when needed)
  - [https://wiki.egi.eu/wiki/Federated\\_Cloud\\_siteconf](https://wiki.egi.eu/wiki/Federated_Cloud_siteconf)
- Orchestration/automation
  - Trend in operations to use ansible for EGI's tooling, INDIGO IM and Orchestrator also heavily rely on ansible
  - Can we do any kind of security checks of relevant ansible roles? (at least of those offered in the AoD)



## Network policies for OpenStack sites

- 13 OpenStack sites (+1 missing, recently certified)
- which is the *default network type*?
  - **private** more secure but gateway needed to expose to internet
  - **public** less secure and public IP number limited
- 7 private, 6 public
  - (similar situation with OpenNebula)

# Network policies for OpenStack sites

- Ports can be opened/closed
  - at frontier level
  - at CMF level using security groups
- which is the **policy regulating open/closed ports?**

port default firewall policy	ports default CMF policy	Count
All open	All closed	7
All closed	All open	4
All closed	All closed	1
All open	All open	1

- How users can ask for **opening ports?**
  - GGUS (all), email (1 site)
  - Horizon web interface (7 sites) → where «all open/all closed» is used

# Thank you for your attention.

## *Questions?*

