EGI Federated Cloud F2F Security Issues in the cloud Introduction

Linda Cornwall, STFC

In general

- Focus is on making things happen
  - Getting the functionality in place
  - What the user wants to do
  - Not a bad thing
- Security tends to get added later
  - Security groups in EGI still very focused on the Grid
  - Lack manpower for doing much more
  - However, Federated cloud and EGI security groups need to better engage

I’ve heard it said…

- Security doesn’t matter in the Cloud
- If something is running in a VM then no-one is interested in what I am doing, it doesn’t affect anyone else.
- I can do it easily on Amazon, why not here?

No one interested in what I do on VM

- The VO who is providing access may not want something done outside policy
  - E.g. bitcoin mining
- Something may be done which affects us
  - Attempts at RSA cracking

Work not confined to VM

- Users will need to access and store data
  - Credentials will need to be used to access and store data
  - External connectivity is needed
- Jobs will not all be confined to 1 VM
  - Many jobs may require a number of VMs
  - A need for connectivity between them
- If a VO sets up a Virtual grid in federated cloud, similar security implications apply to current Grid infrastructure

Non-Repudiation

- With discussions on the possibility of billing a user, this becomes more important.
- High impact on traceability, secure logging,

EGI Security Threat Risk Assessment

- In 2012 EGI carried out a security Threat risk assessment.
  - Threat of highest risk value was

“New Software or technology may be installed which leads to security problems”

- Also High, specifically

“The move to Cloud technologies may lead to security problems”

Attack from the EGI Federated Cloud

- One of the highest impact risk factors in the Security Threat Risk assessment was

“Resources used for on-line attack to external parties”

- Assuming external access is possible, then this could happen.
  - Traceability is important
  - Tools to kill VMs, prevent further malicious jobs needed.
- Hopefully won’t happen, but due diligence is needed

EGI Security Policy Group

- The EGI Security Policy Group provides various documents https://wiki.egi.eu/wiki/SPG
  - These continue to apply in the Federated Cloud environment
  - These will probably get updated, new ones added as the need arises
  - Particularly relevant: Security Policy for the Endorsement and Operation Of Virtual Machine images https://documents.egi.eu/public/ShowDocument?docid=771

Security issues continue

- Many of the issues concerning the Grid continue into the Cloud e.g.
  - Authentication, Authorization
  - Data access and storage
  - Protection of credentials
  - Traceability
- Security related activities need to continue,
  - Policy definition
  - Security Monitoring
  - Software Vulnerability handling
  - Incident handling,
  - Provision of software to enable secure sharing of resources

Getting Federated Cloud Certification for EGI infrastructure

- There is a plan to have a questionnaire concerning Federated Clouds
- Check that appropriate security measures are in place
- CSIRT will not recommend certification unless they are happy

- Sven Gabriel will talk about this

Questions

- ??