Security in a cloud context

David Crooks, for the EGI CSIRT

Lessons learned from recent incidents

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Cloud Security

Features of cloud security

- Separation between resource provider and application running on top
- Split responsibility for security between infrastructure (eg Openstack) and application/service
- Applications/services potentially run by non-admins (by design!)
- Reuse of images
  - Potential double edged sword: allows ready source for secure images...
  - ... but one insecure config could have wide impact

Incidents

What kind of incidents?

- Weak passwords
  - Brute force attacks
- Misconfigured services
  - Unexpected or unintended access to running VMs
  - Network storage with open permissions
  - Remote access mechanisms without proper controls

Attack via NFS

- Highlight particular example on FedCloud
  - EGI-20160509
- Attacker gained access to two FedCloud machines via world writeable NFS instances
- Contextualised via orchestrator service with vulnerable configuration
- Investigation spanned many sites
- Setup is easy using these services, but can lead to propagation of config flaws

Months later

Attack via NFS

- VMs created which were again vulnerable
  - But: detected prior to exploitation
  - EGI-20161013-01 and EGI-20161124-01
- Emphasises importance of taking action following incidents to avoid reoccurrence
  - And the importance of good monitoring!
- Particularly true in a cloud context
- In this case, lead to review of best practices

What could be done?

Community and education

- Maintain good links between Cloud and Security teams
- User education on importance of secure configuration and use of strong passwords/other access methods

SECANT

- Security cloud assessment framework
  - https://github.com/CESNET/secant
- Developed by CESNET
  - Checks security characteristics of virtual machines and their images
  - Combines external and internal checks
  - Aims at
    - typical configuration errors
    - vulnerabilities commonly misused by Internet attackers
  - Being developed for AppDB

Notes on good practice

- Signed images - ideally use images from trusted sources only
  - If not, look at SECANT?
- Storage encryption
- Remote logging and security auditing

Notes on good practice

- Match security groups to running VMs
- Shutdown VMs not in use (and isolate/update them when they come up)
- Don’t keep sensitive data in the images
- Monitor network activity

Notes on good practice

- Network isolation of cloud services
- Restrict access from cloud instance to hypervisor
- Isolate tenants; avoid memory optimisation which uses de-duplication
- Keep software patched!

Other cloud communities

- Work done in US by Trusted-CI
  - https://trustedci.org/cloud-service-provider-security-best-practices

Any questions?