Cloud Resource Providers

The EGI CSIRT Questionnaires - analysis of the responses

Sven Gabriel, sveng@nikhef.nl

Nikhef http://nikhef.nl

EGI-CSIRT https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

EGI RP Certification

Questionnaires and Certification

- Certification and registration:
- `https://wiki.egi.eu/wiki/PROC18_Temporary_Cloud_Resource_Centre_Registration_and_Certification`
- Checks that the Resource Centre passes the basic security assessment tests The security assessment is performed by the the EGI CSIRT. Site administrator should fill in EGI Federated Cloud Security - Questionnaire for sites deploying cloud technology. This step also applies to certified Resource Centers which introduce cloud resources for the first time.

CRP Questionnaire

How the Information is gathered

- Web Form, Survey Monkey
- Additional/background Information in EGI-Docs
  https://documents.egi.eu/public/ShowDocument?docid=2114
- Doable in less then 1h
- feedback received from 19 CRPs

CRP Questionnaire

General / Cloud RP Set-Up I

- General part: Role in the RC? **All Site Admin/OpsManager and Site Security Officer 9**
- Cloud enabling technology used? **Openstack 10 / OpenNebula 8 / Synnefo 1**
- What is the process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches? **automated sec. updates / monitoring of security lists / apply sec. patches when availabable**
- Provider network separation (management/services) ? **VLANS 9 / phys. sep. 3 / fw,routing 3 / No sep 1 / unclear 2**
- Does the CRP agree to be bound by the EGI security and other policies? **18 yes / 1 No**

CRP Questionnaire

General / Cloud RP Set-Up II

- What processes exist to maintain audit logs (e.g. for use during an incident)? In general, outbound connections must be logged and traceability must be ensured (EGI may provide a general instructions for sites on how to configure this). **No answer 1 / unclear 3 / connection logs 11 / flows 2 / Only Hypervisor 2**

CRP Questionnaire

About the cloud service provided

- Who is allowed access to the management of the cloud services, and how do they obtain access? **Only Site admins 16 / unclear 1 / No answer 1 / Members of VOs? 1**
- Are the cloud-enabling services run on a dedicated system to which only cloud customers have access, or are services also offered through other interfaces? (Are there other forms of access besides through the Federated Cloud access mechanisms.) **19 dedicated system, 1 stated: OCCI/EC2**
- State whether identity providers other than EGI-approved are enabled. **only EGI appr. 14 / + local users 3 (2 on sep cloud endpoints) / keystone tenants (per VO) 1 / unclear 1**
- Is it possible to suspend a User or group of users? **yes 17 / No 2**
- how suspensions are effectuated with regard to currently executing VMs **autom. terminated 5 /manual intervention**

CRP Questionnaire

About the Virtual Machines instantiated in the Cloud

- Image sources and the EGI Federated Cloud model (only endorsed VMs?) **Yes 10 / unclear 1 / any image 4 / locally endorsed 4**
- What mechanism is in place to ensure only endorsed VMs are executed on the infrastructure? **image upload is blocked 6 / vmcatcher 1 / unclear 3**
- Differentiating operators and users, (root access to VM y/n?) **root access 12 / no root access 6 / unclear 1**
- Network monitoring, how network monitoring is implemented for customer VMs, what if user has root? **None 6 / unclear 5 / net,sflows 5 / Central FW 2 / billing 1**
- Incident response and investigations, can you do snapshots/share them etc? **Snapshots 6 / + share images 13**

CRP Questionnaire

About EGI and non-EGI co-tenancy

- How do you ensure that the co-tenancy does not give rise to security problems for EGI and that actions from other users cannot interfere with or be incorrectly associated with EGI users? **No answer 6 / unclear 5 / sep. network 7 / only EGI 1**
- How are your non-EGI customers identified? Can these users be authenticated and positively distinguished from EGI users? What mechanisms are in place to ensure actions are not inadvertently associated with identified EGI users? **No answer 5 / Different Groups,Tenant 5 / Hardware,Network 2 / Unclear 7**

CRP Questionnaire

Policies, do you require that all customers abide by a set of security policies/

- You require that all customers abide by a set of security policies and/or do you have an acceptable use policy (AUP) **12 require / 7 not**
- Your terms and conditions publicly available **8 available / 11 na**
- Your terms and conditions protect customers from each other **7 yes / 12 na**
- Your AUP include clauses that permit participating in incident response by, e.g., providing network and systems information **yes 5 / na 14**
- You would consider the EGI security incident response task force forensics expert(s) as an appropriate third party in such investigations, when they pertain to incidents involving EGI users, VM operators, and/or VM endorsers **yes 9 / na 10**

CRP Questionnaire

VM execution

- Any Customer can instantiate VMs **13**
- No, only a subset of the users can instantiate virtual machines **1**
- No answer **5**

CRP Questionnaire

Process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches?

- Your terms and conditions or AUP put requirements on the VM images with regards to vulnerability patching. **10 yes**
- Your terms and conditions or AUP put requirements on the external behaviour of the VMs executing (such as: no security violations, no network abuse nor spoofing, no email or message abuse, etc) **yes 10**
- You have systems in place for the enforcement or monitoring that (non-EGI) customers comply with these policies 7
- None **1**

CRP Questionnaire

If a non-EGI customer(s) are implicated in a security incident, are you able to suspend/prevent their usage of the system?

- Yes **14**
- No / No answer **5**

CRP Questionnaire

How long are identity and audit records for Non-EGI customers retained?

- 3+ Months **10**
- no answer **9**

CRP Questionnaire

Questionnaires and Certification II

- All sites are certified with Proc 09 or Proc 18 ... **really?**