EGI Federated Cloud Security - Questionnaire for sites deploying cloud

Welcome

This survey contains the basic security related checks which must be carried out with Cloud Resource providers offering “Infrastructure-as-a-Service” clouds based on the execution of virtual machine images.

The survey is divided in following parts:
1. General information
2. About the Cloud Resource Providers (mandatory)
3. About the Cloud services provided (mandatory)
4. About the virtual machines instantiated in the cloud (mandatory)
5. About EGI and non-EGI co-tenancy (Not applicable if only EGI FedCloud VMs are used.)

This survey is a part of Resource Centre certification procedure and this is a mandatory step to join EGI Production Infrastructure.

For more detailed description of questions please check https://documents.egi.eu/document/2114

Please fill in this survey carefully. If you have any questions please contact irtf@mailman.egi.eu.

EGI Federated Cloud Security - Questionnaire for sites deploying cloud

General information

***1. Please, provide your name and contact details.**
These information will not be shared, but may be used to contact you for clarification.

Your name

Your email address

***2. What is your role in the resource centre?**

□ Site Operations Manager

□ Site Operations Deputy Manager

□ Site Security Officer

□ Site Administrator

***3. Please, provide the resource centre name you are representing (the site you are referring to in this survey)**
Please: use the site name as it is registered in GOCDB (http://goc.egi.eu)

About the Cloud Resource Providers

4. Check that CSIRT email is set in the GOCDB, and that it works, and provides a response.

○ Checked

***5. The Cloud enabling technology used at the Resource Centre (e.g. Open Nebula):**

***6. What is the process for keeping the service(s) and OS patched and up to date, especially with respect to security patches?**

***7. Describe the network separation of management and service traffic.**
This includes aspects such as: presence of a separate network for management of physical hosts and the (virtual) network(s) to which customer VMs can be connected; whether that is a physically separated network; what are the (network) security controls separating the management network from the systems running the cloud enabling software; can customer traffic be separately monitored?

***8. Do you agree to be bound by the EGI security and other policies?**
See: The EGI Security Policy Group wiki pages

○ Yes

○ No

***9. What processes exist to maintain audit logs ?**
In general, outbound connections must be logged and traceability must be ensured

About the Cloud services provided

*10. Who is allowed access to the management of the cloud services, and how do they obtain access?

Not applicable to the virtual machines.

*11. 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 (e.g. grid services)?

○ Dedicated system

○ System shared with other interfaces - please state how this access is obtained.

*12. Are identity providers other than EGI approved enabled?

○ Only EGI approved identity providers

○ Also other identity providers (please specify)

*13. Is it possible to suspend a User or group of users?

State whether you are able to take the information provided centrally by the EGI security teams and suspend users.

○ No

○ Yes

○ Yes with limitations (please describe)

14. If Q13 Yes, please state how suspensions are effectuated with regard to currently executing VMs.

About the virtual machines instantiated in the cloud

***15. For EGI users, do you follow exclusively the EGI Federated Cloud model of running 'endorsed' virtual machines from a trusted EGI market place?**
See the EGI policy for VM endorsement.

○ Yes

○ The policy is not followed for all the VM running in the cloud

16. What mechanism is in place to ensure only endorsed VMs are executed on the infrastructure?
Which controls are used to ensure this is applied for all VMs? Which mechanisms are used to ensure VMs in the local image store are all endorsed and no non endorsed VMs are executed?

***17. Can and does your cloud management framework separate operators (those with responsibility for the security of the VM, typically having root access to the VM, see definition) and users ?**
If so, do you apply different controls for each of these groups?

***18. Describe how network monitoring is implemented for customer VMs. Describe how all network traffic can be traced to a specific VM instance and its associated operator. If the user has root to the VM, can you confirm that the user's connections are still monitored externally to the VM.**

***19. Your ability to participate in incident response and investigation. Please, check which of the following sentence are true for your site:**

□ Yes, we are capable of preserving point in time snapshots of the state of a virtual machine executing in your infrastructure.

□ I am allowed and willing to share the images related to EGI FedCloud users and user communities with the EGI security incident response team(s).

□ None of the above.

If any, please describe briefly if you have any preconditions related to investigations and incident response. Or any other relevant comment.

EGI Federated Cloud Security - Questionnaire for sites deploying cloud

Not applicable if only EGI FedCloud VMs are used.
Many of the questions below should then be addressed by the VM endorsers and/or the VM operators, who are subject to their own policy sets.

Running customer VMs from customers that are not controlled through EGI security policies can potentially pose a risk to the EGI FedCloud infrastructure, other cloud providers, VM operators, or end-users. For the EGI security teams, it is important to be able to assess the associated risks. While we understand that due to privacy issues with some customers, you may not be able to give full answers to all questions; it is important to explain how 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. Please provide as much information as possible to allow judgement as to whether we can have confidence in the operation and separation of these services.

20. 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?

21. 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? How (if so) are EGI and non-EGI customers separated? How (if applicable) are EGI customers protected from other tenants?

22. Policies: which of the following sentence are true for your site?

□ You require that all customers abide by a set of security policies and/or do you have an acceptable use policy (AUP)

□ Your terms and conditions publicly available

□ Your terms and conditions protect customers from each other

□ Your AUP include clauses that permit participating in incident response by, e.g., providing network and systems information

□ 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

23. Are all non-EGI customers able to execute VM images?

○ Yes, any customer can execute virtual machines

○ No, only a subset of the users can instantiate virtual machines

Please, describe which customer groups are allowed to instantiate VM

24. Process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches?
Please, check the sentences that can be applied to your cloud service.

□ Your terms and conditions or AUP put requirements on the VM images with regards to vulnerability patching

□ 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, &c)

□ You have systems in place for the enforcement or monitoring that (non-EGI) customers comply with these policies

□ None of the above

Comments

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

○ Yes

○ No

Comments

26. How long are identity and audit records for Non-EGI customers retained? (Months)

EGI Federated Cloud Security - Questionnaire for sites deploying cloud

Thank you for filling in the survey!
EGI CSIRT team will contact you as soon as possible with the result of the evaluation.

If you have any questions please contact irtf@mailman.egi.eu.