

Cloud Security Implementations/Policies/Certification

Sven Gabriel, sveng@nikhef.nl

Nikhef <http://nikhef.nl>

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



History 10+ years: Data Grid / EGEE / EGI / WLCG

- Current Infrastructure grew under coordination of the Grid-Projects Data-Grid/EGEE 1-3/EGI.
- Framework of SLAs, Policies, Procedures was developed to assure that reliable operation of the Infrastructure is possible.
- Procedures/Policies define how to get part of the infrastructure, how to access resources, how to use the resources (AUP)
- Grid Security Policy ¹

¹<https://documents.egi.eu/public/ShowDocument?docid=86>

Resource Provider/Centers (RP/C) Certification <https://documents.egi.eu/document/>

- The name, email address and telephone number of the Site Manager and Site Security Contact in accordance with the requirements of the Site Operations Policy. ¹.
- It is checked that they are operationally ready to fulfil the SLAs.
- It is checked the RP/C does not expose known vulnerabilities.
- RP/Cs security teams have a incident reponse procedure, know how to apply it (checked in SSCs).
- Details on RP/C certification can be found in PROC09 ²

¹ <https://documents.egi.eu/document/75>

² https://wiki.egi.eu/wiki/PROC09_Resource_Centre_Registration_and_Certification

Cloud Technology / Evolution of VO-WMS / CVMfs / ID Management

- Grid Environment is Constantly changing, new technologies have to be integrated.
- This does not change the policies.
- To help to understand potential Security issues with new technologies a questionnaire should be answered.

Incident Response related

- Keep logfiles centrally to allow for an audit trail
- Keep your systems updated
- Have mechanisms in place for fine grained access control.

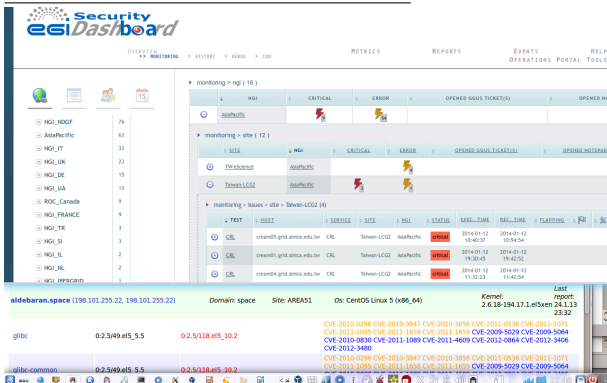
EGI-CSIRT / SVG / Incident Prevention

- Vulnerability Assessment (SVG, chaired by Linda)
- If CRITICAL: Advisories ¹/ Patch status Monitoring (pakiti, nagios)
- Enforce application of software updates ².

¹ https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts

² <https://documents.egi.eu/public/ShowDocument?docid=283>

Security Monitoring: Pakiti, Nagios



The screenshot displays the ESI Security Dashboard interface. At the top, there is a navigation bar with tabs for OVERVIEW, MONITORING, HISTORY, SERVIC, and CSD. Below this, there are sections for METRICS, REPORTS, EVENTS, OPERATIONS, PORTAL, and HELP TOOLS.

The main content area is divided into several sections:

- Monitoring > ngi (16)**: A table showing monitoring data for 'ngi' with columns for CRITICAL, ERROR, OPENED GOUUS TICKET(S), and OPENED NO.
- Monitoring > site (12)**: A table showing monitoring data for 'site' with columns for CRITICAL, ERROR, OPENED GOUUS TICKET(S), and OPENED NOTIFIA(S).
- Monitoring > issues > site > Taiwan-LCG2 (4)**: A table showing issue data for 'Taiwan-LCG2' with columns for SERVICE, SITE, NSG, STATUS, EXEC_TIME, RES_TIME, and FLAPPING.

At the bottom of the dashboard, there are several status bars and a CVE list:

- aldebarn.space** (198.101.255.22, 198.101.255.22): Domain: space Site: AREA51 Os: CentOS Linux 5 (x86_64) Kernel: 2.6.18-194.17.1.el5xen 24.1.13 23:32
- glbc**: 0.2.5/49.ef5.5.5 0.2.5/118.ef5.10.2
- glbc-common**: 0.2.5/49.ef5.5.5 0.2.5/118.ef5.10.2

A list of CVEs is displayed at the bottom right, including CVE-2010-0296, CVE-2010-3847, CVE-2010-3856, CVE-2011-0536, CVE-2011-1071, CVE-2011-1095, CVE-2011-1658, CVE-2011-1859, CVE-2009-5029, CVE-2009-5064, CVE-2010-0830, CVE-2011-1089, CVE-2011-4609, CVE-2012-0864, CVE-2012-3406, CVE-2012-3480, CVE-2010-0296, CVE-2010-3847, CVE-2010-3856, CVE-2011-0536, CVE-2011-1071, CVE-2011-1095, CVE-2011-1658, CVE-2011-1859, CVE-2009-5029, CVE-2009-5064, and CVE-2012-3406.

Incident Response Task Force (IRTF): Leif Nixon

- Provides Incident Response capabilities for the Infrastructure.
- Weekly Rota / Handover Telco / Minutes Recorded in private wiki
- Private Ticket System (RT-IR) for handling/follow up on security issues.

Interfacing to other (Grid/NREN/VO) CSIRTs

- Collaboration with other CERTs, share Information, **Trust**
- Describe / Document your CSIRT, operational requirements to be met
- RFC-2350
- Provided information gets evaluated.

Interfacing to other (Grid/NREN/VO) CSIRTs



EGI CSIRT

has been accredited by
TF-CSIRT Trusted Introducer since
29 October 2012

Valid for

2013

On behalf of
Trusted Introducer

Dr. K-P. Kossakowski
TI Service Manager

On behalf of
TERENA

Valentino Cavalli
Acting Secretary General



TF-CSIRT Trusted Introducer
is a service of TERENA.

Cloud Security

- Mostly apply to cloud (missing threats)
- Most important identified asset: Trust
- Most dangerous threat: Misused identities
- Focuses on traceability for:
 - Incident containment
 - Incident re-occurring prevention

Security Policy for the endorsement and operation of Virtual Machine images¹

- 2 roles:
 - Endorser: Certify VM Image
 - VM Operator: Root access on the VM
- Security requirements for both roles
- Users are not endorsers:

An Endorser should be one of a limited number of authorised and trusted individuals appointed either by the Infrastructure Organisation, a VO or a resource centre

¹ <https://documents.egi.eu/public/ShowDocument?docid=771>

- endorser/operator = site: current situation
- endorser = VO: could provide more flexibility
- operator = VO: could provide technical debugging
- endorser/operator = end user: not foreseen useful

Grid Security Traceability and Logging Policy²

- Idea: understand and prevent incidents
- Requirements:
 - Grid software **MUST** produce application logs:
 - Source of any action
 - Initiator of any action
 - Logs **MUST** be collected centrally
 - Logs **MUST** be kept 90 days

²<https://edms.cern.ch/document/428037>

		Endorsement		
		Site	VO	User
Operator	Site			
	VO			
	User			

Virtualization only introduces new possibilities:

- Logging requirements not changed/impacted:
 - Every action/every user
 - Forwarded to a central server
- New logs required (policy extension?):
 - Which endorsed VM is running?
 - Who is operating it (Site/VO) ?
- User compartmentalization:
 - Similar to glxexec? (one UID per user)
 - Re-instantiate VM for each user (not job)
 - Perfect easy compartmentalization
 - High impact for unique short jobs

Complete root access for user is dangerous:

- Endorsed VM:
 - Contains up-to-date software (by policy)
 - Contains secured configuration (by policy)
 - Can include protections/logging...
- User in full-power:
 - Can break configuration (maliciously or by error)
 - Can disable logging (maliciously or by error)
 - Can falsify data (non-trusted logs)
- Simple accountability/traceability: user responsible
- Difficult detailed incident analysis
- VM cannot be re-used by different users

No identified reason for such situation: highly discouraged

Complete user control: no security

- Unknown VM:
 - Can be vulnerable (not patched, outdated...)
 - Can be badly configured (no logs, anonymous access...)
 - Could be fully-encrypted (no forensics possible)
- User in full-power:
 - Can falsify data (non-trusted logs)
- Simple accountability/traceability: user responsible
- Potentially impossible incident analysis
- VM cannot be re-used by different users

No identified reason for such situation: highly discouraged

- VM creation/deletion easy (could be VO/user initialized)
- VM lifetime foreseen shorter than current WN
- If trusted operator/endorser:
 - Application logs centrally kept
 - More system logs probably needed
 - Unknown/modified file preservation would help forensics
- If non-trusted operator/endorser:
 - Application logs (central) not trustworthy
 - System logs (central) not trustworthy
 - VM disk **MUST** be preserved after deletion

Policy extension required?

Three evolutions possible:

- Probe every VM for vulnerabilities:
 - Much more work than now (who?)
 - Extremely diverse security contacts
- Limit VM lifetime:
 - Vulnerability window restricted (automatic)
 - How long (soft/hard limits ?) ?
 - Hours ?
 - 2-3 days ?
 - Week(s) ?
 - Month(s) ?
- If Trusted endorser/operator:
 - Identify vulnerable VM in trusted VM store
 - Contact *all* VM operators (who?)
 - *Kill* switch to be implemented (who?)

- Need well defined security contacts
- Require root access on VM for:
 - Site admin ?
 - EGI/OSG security team, WLCG security officer ?
- VM freezing/isolation (could break jobs):
 - Who is authorized to do it?
 - Procedure (under which circumstances ?) ?
- Analysis using backend services (e.g. disk providers):
 - Who is authorized to do it?
 - Procedure (under which circumstances ?) ?
 - Private data protection ?

- Need well defined security contacts
- How to ban a user:
 - From site/VO operated VM ?
 - From cloud system (user-operated VM) ?
- How to ban a cloud provider (site) ?
- How to ban a glitched VM (from the VM store):
 - For newly created VMs ?
 - *Killing* running VMs ?

- Some documents may need to be revisited/extended:
 - Risk assessment (new threats)
 - Traceability requirement (new layer, VM deletion)
 - Incident procedures
- All operators and final user need to abide by a potentially extended *Acceptable Use Policy (AUP)*:
 - Recognizing liability
 - Allowing security teams to intervene

Hypervisor containment might be broken:

- Require separated hypervisor clusters for:
 - Infrastructure ?
 - Worker Nodes (Site/VO operated) ?
 - Untrusted VM (End User operated) ?
- Require physical host for critical infrastructure?
- Hypervisor traceability needed:
 - VM traceability (On which hypervisor each VM is)
 - System & audit central logs

- Incident response procedure?
- Abuse detection (IDS not available) ?
- Security incident costs, e.g. Amazon agreement³:

If we or our affiliates are obligated to respond to a third party subpoena or other compulsory legal order or process described above, you will also reimburse us for reasonable attorneys' fees, as well as our employees' and contractors' time and materials spent responding to the third party subpoena or other compulsory legal order or process at our then-current hourly rates.

³ <https://aws.amazon.com/agreement/>

Questionnaire on potential security issues in a cloud environment in prep.

- Describe how user proxies are handled from the moment a user submits work to the system to the moment that a user task runs, through any intermediate storage.
- How can a user or a site be blocked?
- What site security processes are applied to the machine(s) running the cloud-related services, centrally and/or at sites?
 - Who is allowed access to the machine(s) on which the service(s) run, and how do they obtain access?
 - How are authorized individuals authenticated on the machine(s)?
 - What processes exist to maintain audit logs (e.g. for use during an incident)?
 - What monitoring exists on the machine(s) to aid detection of security incidents or abuse?