Integration of CMF in EGI production infrastructure

Enol Fernández

(most info taken from Tadeusz Szymocha)

PROC19 for Cloud Management Frameworks

Ongoing PROC19 for already existing frameworks in the infrastructure:

- OpenNebula
  - https://ggus.eu/?mode=ticket_info&ticket_id=111798
  - CESNET
- OpenStack (OCCI)
  - https://ggus.eu/?mode=ticket_info&ticket_id=111659
  - IFCA

Status

PROC19 define how to integrate new cloud/grid platforms into EGI Production Infrastructure

- Configuration Management (GOCDB service types)
- Information system (BDII publishers)
- Availability Monitoring (Nagios probes)
- Operations Dashboard
- Support (GGUS SU)
- Accounting (integration with APEL)
- VM image MarketPlace (cloud only)
- Documentation
- Resource Allocation (eGrant)
- Security
- UMD
- Final steps (broadcasts)

Next actions

Availability Monitoring:

- Add missing tests (VM image management)
- Formalize set of tests and have them on cloudmon Nagios instance

VM Market Place:

- Define what is needed

Security

- Fill in questionnaire and apply recommendations

UMD

- Contact UMD representative and follow UMD Software Provisioning Process

Other Certifications

Native interfaces can also be part of EGI intfrastructure:

OpenStack (native Nova)

- https://ggus.eu/?mode=ticket_info&ticket_id=111296 (IFCA)
- Missing: manual tests for certification, BDII integration

OpenStack (native Swift)

- Not started
- Some pieces already available (probe)

Status of FedCloud

Vincenzo Spinoso

EGI Operations

Status of FedCloud

- All FedCloud sites tested
- Test developed by Enol (thank you!)
- Trying running a specific image: https://appdb.egi.eu/store/vappliance/egi.ubuntu.14.04
  - 12 sites failing OCCI test
  - “Image missing” from the sBDII
    - Could be BDII failing, vmcatcher not getting the image, configuration “on purpose” to skip the image…
- 4 solved; 8 still have issues, in progress

To be done

- Cycle on tickets until everything is solved
- Please have a look at the tickets if corresponding to your NGI and provide help if possible
- Documentation here: https://wiki.egi.eu/wiki/Fedcloud-tf:ResourceProviders#Documentation

Endorsement

Vincenzo Spinoso

EGI Operations

Endorsement

- Discussion started a while ago
- Recent proposals by Linda Cornwall
  - “(Security) Requirements related to Virtual Machines” but actually triggering discussion at all levels (very good, thank you!)
  - https://documents.egi.eu/secure/ShowDocument?docid=2570&version=3
- Endorsement meeting on September 17
  - ACTION on Vincenzo to “prepare subsets of Linda's document by type of requirements/tools TBD with developers and translated into software requirements”
- Discussion ONGOING, we are just reporting the status

Endorsement

- Endorsement: assigning full responsibility of a given Virtual Appliance to one person

- Virtual Appliance
  - set of images to be run together as part of the same application
  - VA can collapse to a single image
  - Most of VAs are made of a single image
  - We often refer to images instead of Vas
  - Endorsement actually is about VA versions, not VAs

Endorsement

- Endorsement is a declaration that means that a given VA has successfully *passed a checklist*
- Endorsement means *responsibility*
  - If image X results vulnerable because misconfigured (i.e. weak root password set), the endorser is accountable
- Endorsement is identified by (VA version, VO, endorser, timestamp, lifetime)

Repository

- Images constituting Virtual Appliances may be stored anywhere
  - AppDB is not a repository. Only appliance metadata can be stored on AppDB

How it works

- At the moment
  - Everybody (with valid credentials) can add images to AppDB
  - All images are **publicly** available
    - Is this a security concern? For instance, what if credentials are stored in an image by mistake?
  - VO Manager can manage his own VO image list
  - VO “A” Manager adds image X to the list, and at the moment this **means** it is endorsed for VO “A”
- If an image is changed, it must be re-endorsed
- <u>This implementation can be enough</u>

Endorsement as “tagging”

- New possible model
- Endorsement means **tagging** (with signature) the VA version
- Hence a VO image list will contain endorsed and non-endorsed appliances
- Security requirement: “*It must be possible to trace the (Security) Infrastructure Endorser, in a way that satisfies non-repudiation*”

BUT

- Signing images and/or metadata are very hard to implement and not easily doable with the current implementation of AppDB
- Also difficult to implement in a way that keeps procedures easy from the user point of view
- If no signature is possible, a new model using tags could be useless

New role: VO Endorser

- Operation Portal provides role management
- VO Manager (already supported)
- VO Endorser (new role)
  - the VO Manager is Endorser by default
  - there can be more than one Endorser per VO, sharing the same permission about the endorsements of the same VO
- Who can be VO Endorser?
  - It's up to the VO to decide if a VO member can be a VO Endorser
- CSIRT should be able to remove the VA Endorser Role if a particular Endorser is responsible for problematic images
  - CSIRT will simply request that the role is removed
- Who can upload images? EVERYBODY with proper credentials
  - Is this really correct?

Endorsement expiration

- If lifetime expires, the endorsement is considered expired
- If endorsement expires, the image is equivalent to “non-endorsed” for that particular VO
- A VO Endorser can re-endorse the image on his own responsibility

Banning

- If an image is affected by serious security issues (say credentials stored within the image), the image can be unpublished by the AppDB
  - CSIRT can simply request that the image is unpublished

Sites

- Can sites run non-endorsed images?
  - Yes. At the moment, they can run whatever is in the VO image list for each VO they support (endorsement **means** adding to the VO list)
  - With the new proposed implementation of the endorsement it could be allowed to sites to choose to download only endorsed images

To be done

- Circulate the proposal for comments
  - Security experts
  - Developers (at the moment, only AppDB involved)
  - Users
  - Sites representatives
- Finalize endorsement procedure
- Automation

Thank you for your attention.

Questions?

www.egi.eu