IBERGRID

Towards Federated Cloud Image Management

A. Simón, E. Freire, R. Rosende, I. Díaz, A. Feijoo, P. Rey, J. López-Cacheiro, C. Fernández and O. Synge

Outline

- ☐ **Introduction**
- ☐ **VMcaster**
- ☐ **VMcatcher**
- ☐ **Image management event handlers**
- ☐ **Links**
- ☐ **Conclusions & Future work**

Introduction

❑ The new federated cloud infrastructures require the development of specific utilities.

❑ One of the most crucial features is the virtual image management and distribution system.

❑ These new utilities must be cloud framework agnostic.

Introduction

❑ VMcaster and VMcatcher are two different tools to generate and subscribe to virtual machine image list.

❑ These tools use an internal SQLite database (or MySQL) which contains images information.

❑ These tools try to match the requirements set by the HEPIX virtualisation group.

❑ VMcaster/VMcatcher tools are based on the X.509 certification authentication model.

iBERGRiD

VMcaster

- ❑ VMcaster is a simple tool for publishing, managing an updating VM image lists.

- ❑ Image lists metadata is signed and trusted with a X.509 certificate.

- ❑ Any user can check the image list <u>expiration date</u>, if it was <u>revoked</u> or it has been <u>tampered</u> by a third party.

- ❑ All images and image lists have an **UUID** (generated with uuidgen):

dfc470ab-0845-4c3b-bc6a-02f990388a17

- ❑ We can use the UUID with VMcaster to create a new empty image list:

vmcaster –select-imagelist dfc470ab-0845-4c3b-bc6a-02f990388a17 –add-imagelist

VMcaster

❑ The last command generates a local image list in our database (*vmcaster.db*).

❑ The database information is shown in JSON format.

❑ At this moment the image list does not include any relevant information an <u>it is not signed</u>.

❑ Thanks to VMcaster tool we can include the most important objects for the image list:

- ▪ The image list title.
- ▪ Description.
- ▪ Image list location (*valid url*).
- ▪ Image list endorser certificate DN.

❑ As example to include the image list name:

```
vmcaster –select-imagelist <image_list_UUID> --key-set-imagelist "dc:title"
--key-value-imagelist "My new image list"
```

IBERGRID

VMcaster

❑ When the image list information is ready the endorser can include new images metadata.

❑ Image insertion procedure is similar to image list creation.

❑ The relevant VM image objects are:

- ▪ *dc:title* Image title name.
- ▪ *sl:comments* to include image comments such user login or default passwords.
- ▪ *sl:osversion* The Operating System version as LSB compliant.
- ▪ *sl:arch* System architecture (x86_64, i386)
- ▪ *sl:os* Operating System name (Ubuntu, Debian, RedHat...)
- ▪ *hv:uri* Image location endpoint (an accessible url to download the new image)
- ▪ *hv:format* VM image format (RAW,QCOW2, etc)

❑ All the new images should be assigned to an image list!

```
vmcaster –select-imagelist <image_list_UUID> --imagelist-add-image --select-image <image_UUID>
```

```
{
    "hv:imagelist": {
        "dc:date:created": "2013-09-11T12:29:33Z",
        "dc:date:expires": "2013-10-09T12:29:33Z",
        "dc:description": "CESGA image list for internal usage",
        "dc:identifier": "2204eed5-f37e-45b9-82c6-85697356109c",
        "dc:source": "CESGA",
        "dc:title": "CESGA image list",
        "hv:endorser": {
            "hv:x509": {
                "dc:creator": "Alvaro Simon Garcia",
                "hv:ca": "/DC=es/DC=irisgrid/CN=IRISGridCA",
                "hv:dn": "/DC=es/DC=irisgrid/O=cesga/CN=alvarosimon",
                "hv:email": "asimon@cesga.es"
            }
        },
        "hv:images": [
            {
                "hv:image": {
                    "dc:description": "Fedcloud EGI-Demo-CESGA",
                    "dc:identifier": "b268b87b-fe42-477e-b4d4-087ad9fde61b",
                    "dc:title": "EGI-Demo-CESGA",
                    "hv:hypervisor": "QEMU,KVM",
                    "hv:size": 1960378368,
                    "hv:uri": "http://cloud.cesga.es/images/debian-6.0.5-x86_64-base.qcow2",
```

VMcatcher

- ❑ VMcatcher utility allows to image consumers to subscribe to VM image lists generated by VMcaster.
- ❑ Using this utility users can select and download trusted images.
- ❑ It validates the list with X.509 based public cryptography and also checks SHA512 hashes.
- ❑ I provides events for further applications to process, update or expire changes of VM images.
- ❑ <u>These events can be used by third party listeners or event handlers.</u>
- ❑ VMcatcher also verifies if the cached images have expired or not.

VMcatcher

- ❑ The image consumer must trust in a endorser.
- ❑ Users can include and trust in an image endorser including his/her X.509 certificate DN and CA.

> *vmcatcher_endorser –create –endorser_uuid=<endorser_name> –subject=<endorser_DN> –issuer=<endorser_CA>*
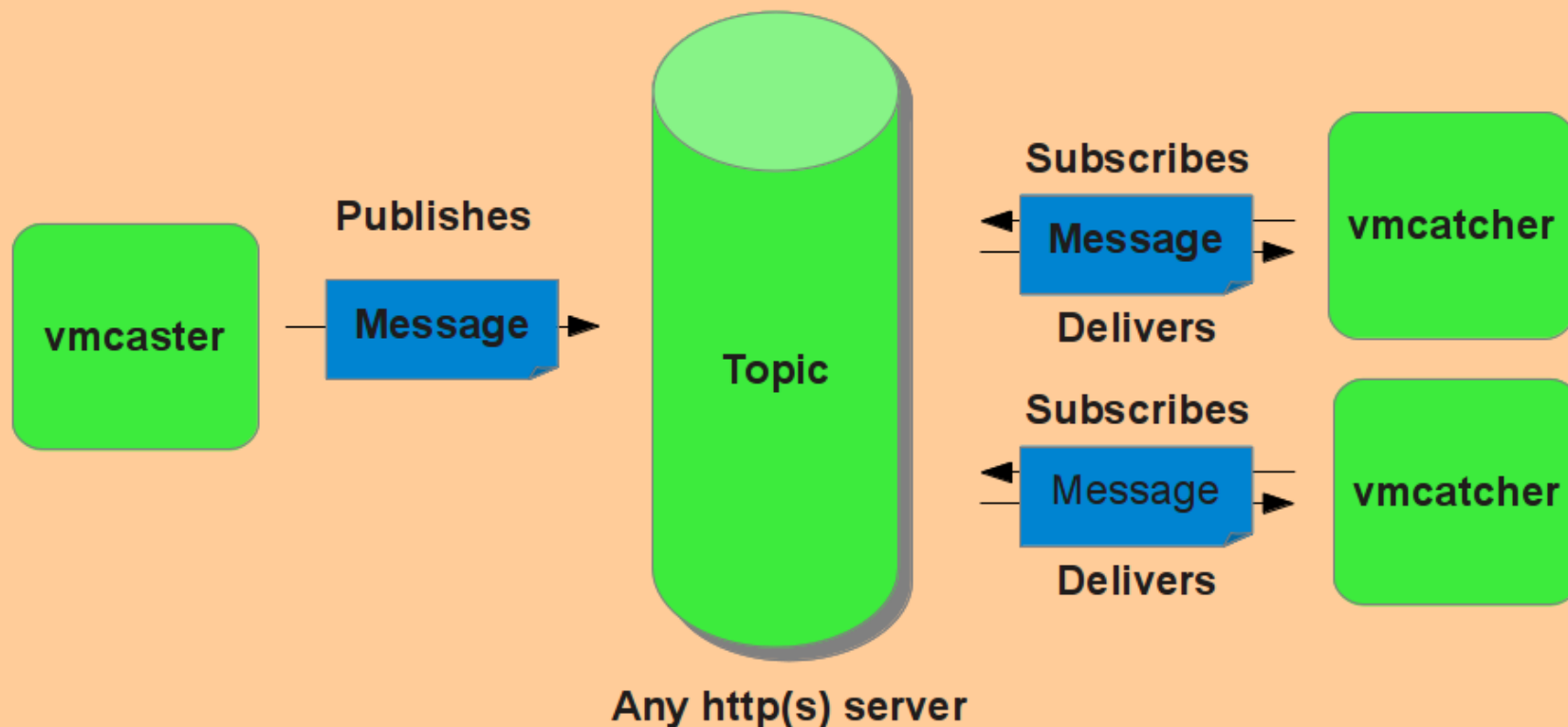
- ❑ And now we can import the desired image list into our database.

> *vmcatcher_subscribe -s <image_list_url>*

- ❑ At this point the image user can show and select any image UUID from the list to be downloaded.

> *vmcatcher_subscribe -U*
> *vmcatcher_cache*

Secure Data Publishing any data:

SMIME Secured JSON meta data with x.509 signatures and secure payload referencing.

Image management event handlers

❑ VMcatcher was written in Python and generates pre-defined events.

❑ These events can be received by asynchronous callback subroutine or event handler.

❑ The cloud community has developed event handlers to interact with the most popular frameworks like OpenNebula or OpenStack.

❑ OpenNebula event handler was developed by CESGA team and it is available from VMcaster/VMcatcher repository.

- Generates a new OpenNebula image template.
- Includes the new image into OpenNebula datastore.
- For security reasons the new images are not public (only oneadmin user has access).
- It also detects image revocations and disables the revoked images.
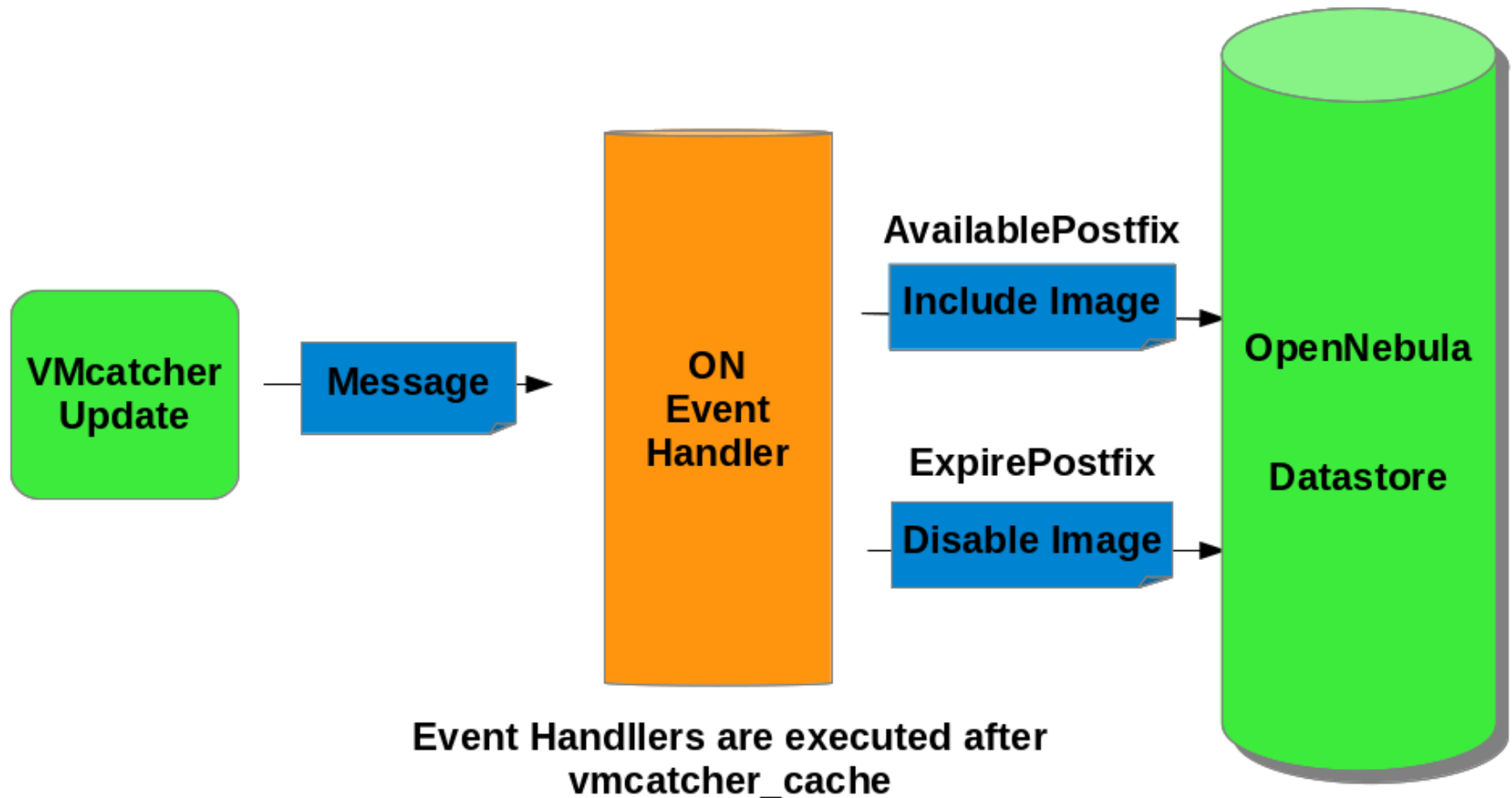
Image management event handlers

- ❑ OpenStack administrators can also use *Glancepush* event handler.
- ❑ This service was developed at IN2P3.
- ❑ *Glancepush* updates OpenStack Image Service (Glance) if it detects any image change.
- ❑ The new package glancepush-vmcatcher is available from IN2P3 ftp server.
- ❑ It requires a working glance service and an OpenStack user account to push images into OS catalog.

IBERGRID

Conclusions and Future work

- [ ] The management of virtual machine images is a critical task within a federated cloud architecture.
- [ ] Fedcloud task force has chosen VMcaster/VMcatcher utilities to distribute and validate VM images.
- [ ] VMcatcher can be used by any cloud framework thanks to event handler tools.
- [ ] EGI SA2.3 task is using VMcaster and ON to distribute and publish verified VM images after SA2 verification.
- [ ] AppDB developers are working to include VMcaster image lists (work in progress).
  - https://appdb-dev.marie.hellasgrid.gr/store/software/cern.virtual.machines/vaversion/latest

Links

- VMcaster on github: https://github.com/hepix-virtualisation/vmcaster.git
- VMcatcher on github: https://github.com/hepix-virtualisation/vmcatcher.git
- VMcaster/VMcatcher repo: http://www.yokel.org/pub/software/yokel.org/release/
- OpenNebula event handler: https://github.com/grid-admin/vmcatcher_eventHndlExpl_ON.git
- OpenStack Glancepush: https://github.com/EGI-FCTF/glancepush/wiki

IBERGRID

Thank You For Your Attention!
Questions?