**Steps to set up the ICOS usecase 'Footprint Tool'**

This document describes the steps to set up a usecase for testing the interoperability of EGI and EUDAT services. The steps follow largely the instructions provided on the EGI wiki, but references to additional information sources are added where needed. Direct contact to experts from EGI and EUDAT was indispensable for solving technical questions/problems.

The Footprint Tool is an interactive service of the ICOS Carbon Portal that computes and visualizes the sensitivity of GHG concentration signals at potential and existing ICOS atmospheric measurement stations to GHG emissions and fluxes from different sources.

Setting up a usecase for testing the interoperability of EGI and EUDAT services requires the following basic steps:

1. Obtain a certificate for access to EGI and EUDAT services

2. Set up a Virtual Machine in the EGI Federated Cloud

3. Add block storage to the VM

4. Prepare containerized version of Footprint Tool and install on VM

5. Access to B2STAGE/B2SAFE

6. EGI Open Data Platform

# **Obtain a certificate for access to EGI and EUDAT services**

A personal X.509 certificate and membership in a Virtual Organization (VO) is required to access EGI and EUDAT services.

[https://wiki.egi.eu/wiki/Federated\_Cloud\_user\_support - Access](https://wiki.egi.eu/wiki/Federated_Cloud_user_support#Access)

* 1. Obtain a personal access certificate from a recognized Certification Authority - only if not already available. The easiest way is to apply at Digicert <https://www.digicert.com/secure/saml/discovery/?entityID=https%3A%2F%2Fwww.digicert.com%2Fsso&returnIDParam=idp>

Enter the name of the organization (identity provider) you will use to authenticate, e.g. Lund University, select 'Grid Premium'

Instructions for Digicert at <http://docs.snic.se/wiki/Requesting_a_grid_certificate_using_the_Digicert_SSO_Portal>

* 1. Export a client certificate

<http://docs.snic.se/wiki/Exporting_a_client_certificate>

* 1. Prepare a client certificate

<http://docs.snic.se/wiki/Preparing_a_client_certificate>

* 1. Prepare a key pair to be able to access the VMs via ssh

[https://wiki.egi.eu/wiki/FAQ10 - How\_can\_I\_inject\_my\_public\_SSH\_key\_into\_the\_machine.3F](https://wiki.egi.eu/wiki/FAQ10#How_can_I_inject_my_public_SSH_key_into_the_machine.3F)

* 1. Apply for membership in VO, for the usecase join fedcloud.egi.eu VO: <https://perun.metacentrum.cz/cert/registrar/?vo=fedcloud.egi.eu>

Application will be confirmed by email.

Administrative interface of Perun system, where you can change you contact details and manage different settings, can be found at: <https://perun.cesnet.cz/cert/gui/>

1. **Set up a Virtual Machine in the EGI Federated Cloud**

A number of images for Virtual Machines (VM) are provided by EGI, with a variety of operating systems and pre-installed software/applications. In order to access EGI Federated Cloud resources (e.g. start a VM) an OCCI client and VOMS clients need to be installed on the local computer.

* 1. Install OCCI client and VOMS clients. Instructions for several operating systems: <https://wiki.egi.eu/wiki/Fedcloud-tf:CLI_Environment>

For my installation on a MacBook Pro (OS X 10.11.6) only the example using the egifedcloud/fedcloud-userinterface docker image worked, this requires docker software installed on the local computer.

<https://hub.docker.com/r/egifedcloud/fedcloud-userinterface/>

Command: docker pull egifedcloud/fedcloud-userinterface

* 1. Use the 'occi' script as wrapper for all occi and voms commands, available at

<https://github.com/enolfc/fedcloud-userinterface>

Obtain a VOMS proxy certificate each time access to EGI FedCloud is needed.

* 1. Select a VM image at <https://appdb.egi.eu/browse/cloud>

For the first tests of the ICOS usecase an Ubuntu 14.04 image with Docker pre-installed was used.

<https://appdb.egi.eu/store/vappliance/docker.ubuntu.14.04>

For access to EUDAT B2STAGE service use the EGI-EUDAT integration pilot software appliance and select one of the VMs offered there, read the instructions:

<https://appdb.egi.eu/store/swappliance/egi.eudat.integration.pilot>

Select a site to host the VM in the 'Availability and Usage' tab. Select memory and CPU specifications in the drop down menu and click 'get IDs' to get 'Site endpoint', 'Template ID' and 'OCCI ID', which are needed in the occi command to start the VM.

* 1. Download the EGI-EUDAT-Integration.yml from

<https://appdb.egi.eu/store/swappliance/egi.eudat.integration.pilot>

Open the EGI-EUDAT-Integration.yml contextualization file and copy your SSH public key where indicated.

* 1. Start a VM using the following occi command (adapt to shell syntax) or add this command to the occi-script.

[https://wiki.egi.eu/wiki/HOWTO11 - How\_to\_start\_a\_VM\_.28create\_a\_compute\_resource.29](https://wiki.egi.eu/wiki/HOWTO11#How_to_start_a_VM_.28create_a_compute_resource.29)

OCCI\_ENDPOINT=<paste here site endpoint>

X509\_USER\_PROXY=<paste here path to VOMS proxy>

OS\_TPL=<paste here template ID>

RES\_TPL=<paste here OCCI ID>

occi -n x509 -x ${X509\_USER\_PROXY} -X \

-e ${OCCI\_ENDPOINT} -a create -r compute \

--mixin ${OS\_TPL} --mixin ${RES\_TPL} \

--attribute occi.core.title="MyVM" \

--context public\_key="file:///ssh/fedcloud.pub" \

--context user\_data="file://egi-eudat-integration.yml"

By mixing in the EGI-EUDAT-Integration.yml contextualization script the GridFTP client globus-url-copy (needed to access EUDAT B2SAFE services) is installed in this VM and username / password are set to egieudat / egieudat.

A VM created without this contextualization script would have ubuntu as username and password.

A resource ID is returned by the create command.

* 1. Describe VM using the resource ID <VM\_ID>, get the status of the VM and the public IP address.

occi -n x509 -x ${X509\_USER\_PROXY} -X \

-e ${OCCI\_ENDPOINT} \

-a describe -r /compute/<VM\_ID>

Use the public IP address to access the VM.

* 1. Log in to the VM

The fedcloud key (cf. 1.4) has to be specified to log in to the VM

ssh -i .ssh/fedcloud egieudat@<IP-address>

Create a config file in the .ssh directory so that the key does not need to be specified each time.

Content of ./ssh/config :

Host MyVM

HostName <IP-address>

IdentityFile ~/.ssh/fedcloud

User egieudat

More information on managing VMs is found at:

[https://wiki.egi.eu/wiki/FAQ10 - Managing\_VMs](https://wiki.egi.eu/wiki/FAQ10#Managing_VMs)

1. **Add block storage to the VM**
   1. Create block storage device for the VM, at the same site that is hosting the VM.

[https://wiki.egi.eu/wiki/HOWTO09 - Block\_Storage](https://wiki.egi.eu/wiki/HOWTO09#Block_Storage)

occi -n x509 -x ${X509\_USER\_PROXY} -X \

-e ${OCCI\_ENDPOINT} \

-a create -r storage \

-t occi.storage.size='num(2000)' \

-t occi.core.title="MyStorage"

Storage size in this example 2000GB.

Command returns the storage ID

* 1. Attach the storage to the existing VM

occi -n x509 -x ${X509\_USER\_PROXY} -X \

-e ${OCCI\_ENDPOINT} \

-a link -r /compute/<VM\_ID> -j /storage/<Storage\_ID>

* 1. The first time the storage is used in the VM it has to initialized. The device will be initially empty, so you will need to format it and mount it.

Note:

This will remove all data stored on the device!

Only run this part the first time the device is used!

Log in to the VM.

Find the disk via the command fdisk

fdisk -l

This returns a list of devices, select the one which has the corresponding size (~20GB in this example: vdc)

Format the partition

mkfs.ext4 /dev/vdc

Mount the disk, e.g. as '/mnt/additional-disk'

mkdir /mnt/additional\_disk

mount /dev/vdc /mnt/additional\_disk

Now the disk is available in the VM.

1. **Prepare containerized version of Footprint Tool and install it in the VM**

The easiest way to install an application in the VM is to prepare a containerized version. There are two ways to install the application:

1. Upload the docker image to docker hub and in the VM pull the image using command docker pull <image>
2. Copy the Docker file to the VM and create the image in the VM.

Note: For access to the docker command first do

sudo bash

For testing purposes data can be copied to the VM using e.g. sftp.

1. **Access to B2STAGE/B2SAFE**
   1. Request authorisation to use EUDAT B2STAGE and B2SAFE services. Directly contact the EUDAT contact person at the computing centre offering B2STAGE/B2SAFE services. They will need the Distinguished Name (DN) of the personal certificate, e.g.

/DC=org/DC=terena/DC=tcs/C=SE/O=<your organization>/CN=<your name>

* 1. Create a proxy certificate and copy it to the VM (e.g. using scp). This is required for access to B2STAGE/B2SAFE. The proxy is only valid for one day!

This step is a bit more complicated when using the egifedcloud/fedcloud-userinterface docker image. The proxy exists only in the egifedcloud/fedcloud-userinterface docker container, because occi is only installed there. But scp is not available in the docker container.

Command to install openssh-client in egifedcloud/fedcloud-userinterface and to copy proxy certificate to VM:

docker run --rm --volumes-from occi-voms-proxy -it \

-v $PWD:/data:rw -v ~/.ssh\_egi:/ssh:ro \

egifedcloud/fedcloud-userinterface \

/bin/bash -c "(apt-get install -y openssh-client && scp -i /ssh/fedcloud ${X509\_USER\_PROXY} egieudat@< IP-address >:)"

* 1. Upload and download files to/from B2STAGE instance with globus-url-copy

globus-url-copy -vb -cred <X509\_USER\_PROXY on VM> file:///<local filename> gsiftp://<B2STAGEinstance>/<path>/<filename>

globus-url-copy -vb -cred <X509\_USER\_PROXY on VM> gsiftp://<B2STAGEinstance>/<path>/<filename> file:///<local filename>

List remote files on B2STAGE instance

globus-url-copy -vb -cred <X509\_USER\_PROXY on VM> -list gsiftp://<B2STAGEinstance>/<path>/

If you do not know the path on the B2STAGE instance use

globus-url-copy -vb -cred <X509\_USER\_PROXY on VM> -list gsiftp://<B2STAGEinstance>/~/

where ~ is the home directory

* 1. Install a GridFTP client in the VM, which allows also other file manipulations like deleting files on B2STAGE/B2SAFE, e.g. UberFTP

Instruction how to install UberFTP:

<https://github.com/EUDAT-Training/B2SAFE-B2STAGE-Training/blob/master/10-using-B2STAGE.md>

sudo apt-get install software-properties-common

sudo add-apt-repository ppa:maarten-kooyman-6/ppa

sudo apt-get update

sudo apt-get install uberftp

To use uberftp the certificate needs to be copied to /tmp/x509up\_u1000

cp <X509\_USER\_PROXY on VM> /tmp/x509up\_u1000

For file transfer or manipulations:

uberftp <B2STAGEinstance>

* 1. Transfer data from ICOS server to B2SAFE using B2STAGE

This is still work in progress and a detailed description will follow.

Note that the instructions on

<https://wiki.egi.eu/wiki/EUDAT_B2STAGE_cookbook_for_EGI_VOs>

are outdates because the 'Data Staging Script' is no longer in use.

1. **EGI Open Data Platform**

EGI Open Data Platform allows integration of various data repositories available in a distributed infrastructure. This could be of interest for the ICOS usecase.

A detailed step-by-step guide to EGI Open Data Platform is available at

<https://wiki.egi.eu/wiki/EGI_Opendata_platform>

At the time of testing the current release of the One Data software was not stable.

If needed, detailed descriptions will be included as soon as the new release is tested.