Table of Contents

This installation guide will provide instructions about how to install an ESGF data/compute node. For instance, the VM should have 1 core 2GB of RAM memory and 20GB of Hard Disk.

For the installation process it is highly recommendable to provide more than 1 core

Pre-requisites

TCP and UDP ports firewall configuration [[FootNote(...)]]

Corporate Firewall

Port	Direction	Type	Application	Description
80	in	tcp	Tomcat	Web server access
443	in	tcp	Tomcat	SSL - Secure Web Server Access.
5432	in	tcp	Postgres	Postgres Access. ***(not external: by default bound ONLY TO LOCAL INTERFACE)***
2811	in	tcp	GridFTP	user-configured GridFTP Server control channel
(60000-61000)	in/out	tcp	GridFTP	user-configured GridFTP Server data channel (or as defined in the global variable GLOBUS_TCP_PORT_RANGE)
2812	in	tcp	GridFTP	BDM-configured GridFTP Server control channel. May run together with the user-configured one though **not** recommended - system resource intensive!
(60000-61000)	in/out	tcp	GridFTP	BDM-configured GridFTP Server data channel. May run together with the user-configured one though **not** recommended - system resource intensive!
7512	out	tcp	MyProxy	MyProxy client access to the certificate repository
8984	-	tcp	esgf-search (Tomcat)	local connection to the Solr master instance ***(not external!)***
8983	in/out	tcp	esgf-search (Tomcat)	Connection to remotes Solr slave instance. Used in distributed search (shard).
80	out	tcp	esg-publisher	Local connection to THREDDS server (e.g., to check catalogs) and other nodes (node-manager)
443	out	tcp	esg-publisher	Local secure connection to THREDDS server (e.g., to restart the application) and to the idp

IPTables configuration

Add these rules to the IPTables configuration file, i.e. `/etc/sysconfig/iptables`

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2811 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2812 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8984 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8983 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60000:61000 -j ACCEPT
```

and restart IPTables services

```
$ services iptables restart
```

Install RPM packages

Install the sourceforge RPM repository for the `*ExtUtils*` packages:

```
$ rpm -i -U -h http://dag.wieers.com/packages/rpmforge-release/rpmforge-release-0.3.6-1.el4.rf.x86_64.rpm
```

And now the ESGF required RPM packages

```
$ yum install autoconf automake bison file flex gcc gcc-c++ gettext-devel libtool libuuid-devel libxml2 libxml2-devel libx
```

Please make sure that the `ntp` package is installed: `$ yum install ntp`

User configuration

Add the `esgf` user:

```
$ adduser esgf
...
$ passwd esgf
...
```

configure `esgf` user with `sudoers` privileges. Add the following line to `/etc/sudoers`

```
esgf    ALL=(ALL)       ALL
```

Install the ESGF data/compute node

As reference guide the instructions used has been provided by IPSL[1].

```
$ cd /usr/local/bin
$ wget -O esg-bootstrap  http://198.128.245.140/dist/esgf-installer/esg-bootstrap
$ diff <(md5sum esg-bootstrap | tr -s " " | cut -d " " -f 1) <(curl -s  http://198.128.245.140/dist/esgf-installer/esg-boo
$ chmod 555 esg-bootstrap
$ esg-bootstrap --devel
```

```
.............
```

Index peer configuration

Configure host certificate and CA public key

I think the procedure I sent in the below mail is correct but a little to technical. it might be better to use esg-node commands in order to federate:

Here is where you should put the signed csr we sent via scp to your server yesterday

```
/etc/grid-security/data.meteo.unican.es-esg-node-globus.csr.signed
```

Then if the tomcat key is not in /etc/grid-security, copy it inside:

```
$ cd /etc/grid-security; cp /esg/conf/tomcat/hostkey.pem ./
```

Then run this command to install the key pair in tomcat:

```
$ cd /etc/grid-security; esg-node --install-keypair data.meteo.unican.es-esg-node-globus.csr.signed hostkey.pem
```

You will be prompted to enter the cacert file; enter the url to the index node cacert.pem:

```
Please enter your Certificate Athority's certificate chain file(s):
[enter each cert file/url press return, press return with blank entry when done]
certfile> http://vesgint-idx.ipsl.jussieu.fr/cacert.pem
```

This process should fetch the CA cert to `/etc/grid-security/certificates`

Then set auto fetch certs false otherwise `/etc/grid-security/certificates/*` will be overwritten by `esgf-prod` peer groups certificates

```
$ esg-node --set-auto-fetch-certs false
```

Then restart your node

```
$ esg-node restart
```

Then register

```
$ esg-node --register vesgint-idx.ipsl.jussieu.fr
```

Then rebuild the Tomcat's trustore

```
$ esg-node --rebuild-truststore
```

Data Publishing

?http://devel.esgf.org/wiki/ESGF_Data_Publishing