Table of Contents

This installation guide will provide instructions about how to install an ESGF data/compute node. In order to do it, 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

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 the rules below 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
```

then, restart the IPTables services

```
$ services iptables restart
```

Install RPM packages

First, install the sourceforge RPM repository for the `*ExtUtils*` packages:

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

after that, 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 `$ rpm -qa | grep ntp`, otherwise instal it `$ yum install ntp`

ESGF user configuration

Fist, add a `esgf` user:

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

After that, change the password:

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

To finish, configure the `esgf` user with `sudoers` privileges. Add the following line to `/etc/sudoers` file:

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

Install the ESGF data/compute node

The instructions have been provided by the IPSL[1].

Do it as `esgf` user

```
$ whoami
esgf
$ 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
```

In our case, we are going to configure only `data` and `compute` types:

```
$ sudo ./esg-node --type data compute --install
-----------------------------------------------------
Welcome to the ESGF Node installation program! :-)

What is the fully qualified domain name of this node? [vesgdev-data.ipsl.jussieu.fr]: data.meteo.unican.es
What is the admin password to use for this installation? (alpha-numeric only) []: *******
Please re-enter password: ********
What is the name of your organization? [jussieu]: unican
Please give this node a "short" name: []: data-unican
Please give this node a more descriptive "long" name []: data-unican
What is the namespace to use for this node? (set to your reverse fqdn - Ex: "gov.llnl") [fr.jussieu.ipsl]: es.unican.meteo
What peer group(s) will this node participate in? (if not sure, use default) [esgf-test]: esgf-test
What is the default peer to this node? [esgf-node1.llnl.gov]: data.meteo.unican.es
What is the hostname of the node do you plan to publish to? [esgf-node1.llnl.gov]: vesgdev-idx.ipsl.jussieu.fr
What email address should notifications be sent as? []: meteo@unican.es
Is the database external to this node? [y/N]:
Please enter the database connection string...
(form: postgresql://[username]@[host]:[port]/esgcet)
What is the database connection string? [postgresql://dbsuper@localhost:5432/esgcet]: postgresql://
entered: postgresql://dbsuper@localhost:5432/esgcet
What is the (low priv) db account for publisher? [esgcet]: esgcet
What is the db password for publisher user (esgcet)? []: *****
```

If you want to re-install it, you have to use the `force` option :

```
$ sudo ./esg-node --type data compute --install --force
```

Index peer configuration

Configure host certificate and CA public key

Do it as `root` user

First, you have to send the csr file located under `/esg/config/tomcat/` directory to the CA.

```
$/esg/config/tomcat/data.meteo.unican.es-esg-node.csr
```

Then you should put the signed csr we sent via scp to the `/etc/grid-security/` directory.

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

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

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

Install the key pair in tomcat. You will be prompted to enter the cacert file; enter the url to the index node cacert.pem:

```
$ esg-node --install-keypair data.meteo.unican.es-esg-node-globus.csr.signed hostkey.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