Globus-connect installation on COSMA

Lydia Heck, ICC Durham University
2015/8/5

Using the On-Line Grid

The information on the software of globus-connect can be found at:

https://www.globus.org/globus-connect-server

On the right hand side of the page is a list of "Common Installation Scenarios". These scenarios have a list of steps that should be followed. We will follow the first of these ‘Install Globus Connect Server’.

When the page is opened it will show clear and detailed instructions for different flavours of Linux of how to install the software. The recipe is very easy to follow. Follow these instructions for your Linux distribution until you get the ‘Edit Globus Connect Server Configuration’ section.

Local configuration

Once the software is installed, you will need to configure it. For that edit the file: /etc/globus-connect-server.conf

When configuring globus-connect you will need to have a globus online account. If several people will use the installation and if the installation is on centrally managed system, the manager might not want to register with his/her chosen personal account and/or email address. For the centrally installed service on COSMA, I chose the username cosma and the cosma-support email address. And I would advise not to use one of your own personal passwords, but think of one specifically for this account. Other people, who co-adminster your system, might need access to this password. The account name you choose will be required as part of the endpoint name.

One thing I found very important is the chosen name name of the computer system on which you run your configuration.

If you have an internal network and an internal network name and an external network and an external network name for the system, which you might have, if you are running this node as part of a cluster system and if the cluster itself is on a non-routed internal network, then you should choose the internal name and external name to be the same before you start configuring. The configuration process looks at the `hostname' output.

The configuration file consists of different sections. Under the heading "Globus User Configuration" and opened with the keyword [Globus] I have accepted the defaults. When the configuration script *globus-connect-server-setup* is run, this means that you will be prompted for the Globus Online user name and the password, with which you have previously registered at Globus Online.

The next section in the configuration file is the "Globus Endpoint Configuration", opened with the keyword [Endpoint]. Here I have chosen *myuser#mysystem* where *myuse*r is COSMA's Globus Online user name and *myname* is the short system name of COSMA without the full specification of .cosma.dur.ac.uk.

I allow that the endpoint is displayed in the list of endpoints for Globus Online, so *Public* = *True*. This means that when one browses endpoints *myuser#mysystem* is visible to everybody. As default directory I choose a directory that is writable but is not a home space.
DefaultDirectory = /somedir/ (***Please note, the end-slash on the name must be added.)***

In the section [Security] I have chosen
FetchCredentialFromRelay = False

If the service that is setup is only for globus online, you might want to choose *FetchCredentialFromRelay* to be true, as then hostcert.pem and hostkey.pem, will be fetched from the globus online server and installed into a default location specified by the keywords *CertificateFile* and *KeyFile*, respectively and any existing files with the the chosen names will be overwritten.

CertificateFile = /etc/grid-security/hostcert.pem

KeyFile = /etc/grid-security/hostkey.pem

The permissions for hostkey.pem must be 400 or 600!

I have chosen to specify the locations for the host certificate file and for the host key file to be in line with the gridftp service for other applications for which this system is used. For COSMA, the hostcert.pm and hostkey.pem are properly signed certificate and key, which I requested through the Grid Certificate authority. On a vanilla globus online installation and configuration, the default location for these files are

/var/lib/globus-connect-server/grid-security/hostcert.pem
var/lib/globus-connect-server/grid-security/hostkey.pem

Next
 IdentityMethod = OAuth

This will ensures that authentication for Globus Online does happen against the user name and user password on the system, but will NOT use ssh.

In the [GridFTP] section I entered the fully qualified name of the system
Server = machinename.cosma.dur.ac.uk

I also configured Restricted path only to list those path that can be seen:

RestrictPaths = R/somedir,RW/dir/firstdir,RW/dir/seconddir/subdir,N/

This means that the defaultdirectory is only readable, the directories /dir/firstdir and /dir/secondir/subfir are readable and writeable and no other directory is visible.
If at a later date other directories should be added to the list, then the configuration /etc/globus-connect-server.conf:RestrictPaths has to be modified and the command globus-connect-server-setup has to be re-run.

All other parameters have been left to the default.

I did not set any sharing options

In the [MyProxy] section I explicitly set
Server = mymachine.cosma.dur.ac.uk

Note: .... before running the configuration script for the first time, make sure that /var/lib/globus-connect-server/myproxy-ca does not exist.

In the section [OAuth] I again set the `Server' explicitly:

Server = mymachine.cosma.dur.ac.uk

All other variables will assume the default.

Once the configuration file has been modified then you can run the setup script

globus-connect-server-setup

At this point, you will require your globus user name and password; this username will be used as part of the endpoint that will be configured during running the globus-online setup script. You might decide not to use a personal account for this. However the account must be connected with a valid email address; please see the comments above.

The configuration will create a host key and certificate pair and will put that into the directory
/var/lib/globus-connect-server/grid-security
(this is the default, unless you changed it in the configuration file).
As this is a self-signed certificate, users will be faced with the splash screen of a non-trusted certificate. For a proper server it might be more advantageous to acquire a fully authorized host certificate from a certification authority. In the UK that could be a GridPP based authority. Remember to change the configuration section accordingly. See above.

So it might be more advantageous to apply for a Grid host certificate. You can acquire a fully authorized host certificate from a certification authority. In the UK that could be
a GridPP based authority. The path to the certificate will be, when all the defaults are accepted in the [Security] section

Even though I have a fully signed certificate from the GridPP community, this splash screen does appear.

And then you and your users are ready to go.

For security reasons and to protect data I have configured `RestrictedPaths' explicitly. So when you add more directories to the path, the script will have to be rerun each team you change the path. This can be done safely, even if data transfer is going on at the time.

Should any other configuration parameter change in the configuration file, the globus-online-setup script does have to be run.

Additional configuration:

Firewall rules (which ports to open and to/from where) -

The ports that are required by default are:

2811 ... tcp to/from 184.73.189.163/32 (smtp.globusonline.org),
174.129.226.69 (cli.globusonline.org)
7512 ... tcp from 174.129.226.69 (cli.globusonline.org)
2223 ... tcp from 184.73.255.160 (relay.globusonline.org)

2811 ... tcp to/from any other gridftp site, from which you would allow gridftp access
50000 - 51000 tcp n/out anywhere

If you intend to use fts-transfer, 50000-51000 also needs to be open for udp
The firewall rules for globus online are described in the following document:
https://support.globus.org/entries/20999723-What-ports-does-Globus-Connect-Server-need-open

When you are setting up your globus online configuration you should check for related entries in the system's /var/log/messages if you have problems with the OAuth/MyproxyCA once you are testing and trying to activate the endpoint via globus-online.

The Durham's system OS is CentOS 6.6

The repo configuration to install globus-connect-server:

[root@data yum.repos.d]# cat globus-toolkit-6-stable-el6.repo
[Globus-Toolkit-6-el6]
name=Globus Toolkit 6 (el6)
baseurl=http://toolkit.globus.org/ftppub/gt6/stable/rpm/el/6/$basearch/
failovermethod=priority
enabled=1
priority=98
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-Globus

[Globus-Toolkit-6-Source-el6]
name=Globus Toolkit 6 (el6)
baseurl=http://toolkit.globus.org/ftppub/gt6/stable/rpm/el/6/SRPMS/
failovermethod=priority

enabled=0
priority=98
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-Globus

To install the globus connect server software do:

yum install globus-connect-server

the packages that are installed are:

globus-common-14.7-3.el6.x86_64
globus-gsi-openssl-error-2.1-9.el6.x86_64
globus-openssl-module-3.2-5.el6.x86_64
globus-gsi-cert-utils-8.3-5.el6.x86_64
globus-gsi-sysconfig-5.3-3.el6.x86_64
globus-gsi-callback-4.3-3.el6.x86_64
globus-gsi-credential-5.3-5.el6.x86_64
globus-gsi-proxy-core-6.2-5.el6.x86_64
globus-gssapi-gsi-10.7-4.el6.x86_64

globus-xio-3.3-5.el6.x86_64
globus-callout-2.2-5.el6.x86_64
globus-gss-assist-8.6-1.el6.x86_64
globus-gssapi-error-4.1-9.el6.x86_64
globus-xio-gsi-driver-2.3-5.el6.x86_64
globus-io-9.3-4.el6.x86_64
globus-authz-callout-error-2.2-5.el6.x86_64
globus-authz-2.2-5.el6.x86_64
globus-ftp-control-4.4-5.el6.x86_64
globus-gfork-3.2-4.el6.x86_64
globus-xio-pipe-driver-2.2-4.el6.x86_64
globus-gridftp-server-control-2.7-2.el6.x86_64
globus-usage-3.1-8.el6.x86_64
globus-gridftp-server-6.14-1.el6.x86_64
globus-common-progs-14.7-3.el6.x86_64
globus-gass-transfer-7.2-5.el6.x86_64
globus-gsi-cert-utils-progs-8.3-5.el6.x86_64
globus-gss-assist-progs-8.6-1.el6.x86_64
globus-gridftp-server-progs-6.14-1.el6.x86_64
globus-xio-popen-driver-2.3-4.el6.x86_64
globus-ftp-client-7.4-3.el6.x86_64

globus-gass-copy-8.6-1.el6.x86_64
globus-gass-copy-progs-8.6-1.el6.x86_64
globus-proxy-utils-5.0-9.el6.x86_64
globus-gridftp-5.2.2-1.el6.x86_64

In addition you will require an up-to-date list of certification authorities. For that you should add a reference to the EGI-trustanchors repository in /etc/yum.repos.d with the content (https://wiki.egi.eu/wiki/EGI_IGTF_Release for further reference)

[EGI-trustanchors]
name=EGI-trustanchors
baseurl=http://repository.egi.eu/sw/production/cas/1/current/
gpgkey=http://repository.egi.eu/sw/production/cas/1/GPG-KEY-EUGridPMA-RPM-3
gpgcheck=1
enabled=1

Then install the package *ca-policy-egi-core*
It is highly important to keep the CA-policy packages up-to-date when using normal grid traffic and for that the command *fetch-crl* should be run in a cronjob frequently. By default this is run every six hours upon installation.

As part of the installation of globus-online an apache service was configured automatically.

check that your service are running:

data:/etc # chkconfig --list httpd
httpd 0:off 1:off 2:off 3:on 4:off 5:on 6:off

data:/etc # chkconfig --list globus-gridftp-server
globus-gridftp-server 0:off 1:off 2:off 3:on 4:off 5:on 6:off

data:/etc # chkconfig --list myproxy-server
myproxy-server 0:off 1:off 2:on 3:on 4:on 5:on 6