How To Setup and Configure Globus Connect Endpoints V1.5

A technical howto document presented to H3ABioNet

Created by

The System Administrator Task-Force

Prepared for

The greater H3ABioNet Consortium community

1. Preamble

This Document provides a step-by-step tutorial of the installation and the configuration of Globus Connect () on the operating systems H3ABioNet supports. It also includes instructions about making a transfer to another endpoint.

This document is under revision; please provide feedback about suggestions or corrections to the task-force members.

2. Document Control

Date	Author	Authorization	Version	Description
May 14, 2014	Mohamed Alibi	Sys Admin task-force	1.0	Globus setup and configuration
May 20, 2014	Mohamed Alibi	Sys Admin task-force	1.1	Fix the first draft
May 29, 2014	Mohamed Alibi	Sys Admin task-force	1.2	Add new appendix
June 26, 2014	Mohamed Alibi	Sys Admin task-force	1.3	Add appendix and fix missing information
July 15, 2014	Mohamed Alibi	Sys Admin task-force	1.4	Fixing and update
April 1, 2015	Mohamed Alibi	Sys Admin task-force	1.5	Fixing and update

3. Task-Force Members

Last Name	First Name	Institution	Country
Alibi	Mohamed	Pasteur Institute of Tunis (IPT)	Tunisia
Brown	David	Rhodes University (RU)	South Africa
Indome	David	Noguchi Memorial Institute for Medical Research (NMIMR)	Ghana
Scheepers	Inus	Centre for High Performance Computing (CHPC)	South Africa
Maslamoney	Suresh	Computational Biology Group – UCT (CBIO)	South Africa
Panji	Sumir	Computational Biology Group – UCT (CBIO)	South Africa
Van Heusden	Peter	South African National Bioinformatics (SANBI)	South Africa

4. Table of Contents

5. Overview

In this document we are going to show you how to configure your server to act as a Globus endpoint, how to install Globus connect personal on a separate machine (Laptop, Mac, Workstation…), and how to make a Globus transfer between the two. We will also provide some information for Globus Endpoint Administrators.

In order to accomplish these things you will need:

- A server
- A secondary system (Laptop, Mac, Workstation…)
- Access to the internet
- Globus account (we will show how to have one during this documentation)
- A public IP address for the server

We expect that this will take approximately 4 hours for a new person.

6. Globus Connect Server Download and Installation

6.1. Server Basic Configuration

Before the installation of the Globus endpoint you should make sure that you have few things configured for Globus use.

6.1.1. Firewall Setting

Some ports need to be opened on the firewall. If there are multiples firewalls the ports need to be opened on all of them. The list goes like this:

GridFTP Settings: **2811**

GrifFTP Transfer: **50000:51000** (All the range, needed for the GridFTP tranfer)

MyProxy Server: **7512**

Iperf Speed Test: **5001**

PS: All of the services are on TCP as a network protocol.

This is what you should get with the command *iptables –L* after you make your changes:

```
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:5001
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:7512
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:gsiftp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpts:50000:51000
```

6.1.2. Network setting

Network Connectivity is very important to establish the endpoint. The server should be able to access the outside networks, and it should have its own host name viewable by an outside nodes, for example truck.ncsa.illinois.edu.

To know if the computer is connected to the Internet you can make a simple test on a common website (ping Google: *ping google.com*). If that fails, start by checking the hardware installation (Cable and network card) then check the network configuration at the server *(/etc/network* or *ifconfig Interface IP-address mask Net-mask-address broadcast Broadcast-address)*. If it's still not working, contact your network administrator to verify that your server should have access.

Making a data exchange between multiple sites in different countries needs to rely on a DNS server that has all the domains of all the nodes. In some countries you may need to use a third party DNS service like Google (Change it in */etc/resolve.conf*, and use the node local DNS server with the Google DNS 8.8.8.8 to make sure it will reach it's destination).

Some Network setup on the routers relies on associating the public (Internet) IP addresses to the private (local) ones. What we call NAT (Network Address Translation). In our case we need to make sure if the network configuration is

setup with NAT or without it. If NAT is being used you need to change the configuration file of Globus. The default setting is without NAT.

Now we should make sure that we have a hostname and a domain that can be located via the Internet. If your server already has a public host name we can check it with *host <<hostname>>.* If not you will need to request a fully qualified domain name from your network administrator. The domain name should be associated with a public IP address, for example: transfer-test.igb.illinois.edu: 128.174.124.25.

Once you have a host name, the first test is to check the host name by typing *hostname -f* to verify the domain address associated to the machine and to verify the host name we type *hostname –s*.

If you need to change the host name or the domain you should change the following files through this steps:

Ubuntu or Debian: *sudo nano /etc/hostname* (And write the domain associated to this machine)

sudo nano /etc/hosts (And change the name after the "*172.0.1.1*" to the hostname you associated to this machine)

sudo service networking restart

Scientific Linux: *sudo nano /etc/sysconfig/network* (And write the domain associated to this machine after "*HOSTNAME=*")

sudo nano /etc/hosts (And change the name after the "*172.0.0.1*" to the hostname you associated to this machine)

sudo service network restart

6.1.3. System Setting

Your system configuration needs to be checked before starting the installation to have a well working endpoint.

The endpoints will be installed on different site in a variety of time zone, some time setting need to be configured. In this case we will be using the NTP (Network Time Protocol) a network timeserver that will do al the job for us. If you already have a network time protocol server configured ignore the next part.

To install and enable the NTP server:

Ubuntu or Debian: *sudo apt-get install -y ntpdate ntp*

sudo service ntp status (To check if it's running)

sudo update-rc.d ntp enable 3 5 (To insure it start on a reboot)

Scientific Linux: *sudo yum install -y ntpdate ntp*

sudo service ntpd status (To check if it's running)

sudo chkconfig --add ntpd (To insure it start on a reboot)

We can also make a one time update of the time using the *ntpdate* command:

```
root@truck:/home/alibi# ntpdate pool.ntp.org
19 May 12:40:29 ntpdate[7591]: step time server 66.228.35.252 offset 15.863196 sec
root@truck:/home/alibi#
```

PS: pool.ntp.org is a common NTP Server.

The time may be wrong after the reboot, since the hardware clock keeps the time when power is turned off. When the clock in the operating system shows the correct time, set the hardware clock like this

sudo hwclock –systohc

At this step we should start checking if there is an old version of Globus installed that should be deleted. To check the installation and delete the package type:

Ubuntu or Debian: *sudo dpkg –l | grep –i globus*

sudo apt-get purge <<package_name>>

Scientific Linux: *sudo yum list | grep –i globus*

sudo yum erase <<package_name>>

After making sure every thing is done well we move to the installation phase.

Here is the summery of the things that you should have configured on the server before the installation:

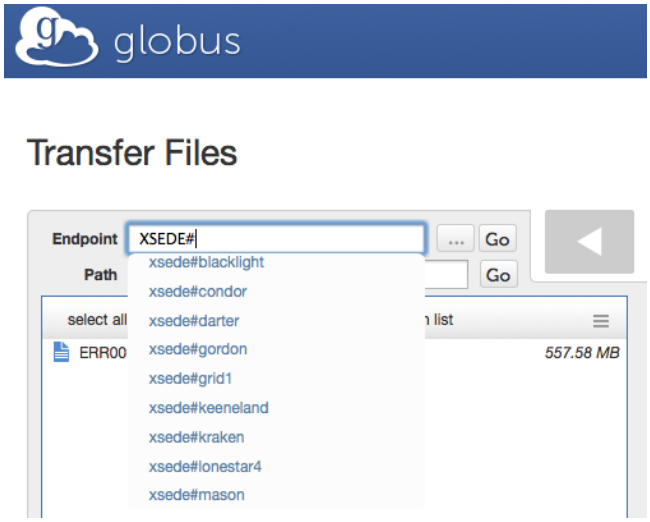
- Fully qualified domain name (hostname)
- Public IP address
- Open ports on all the firewalls
- Internet access from the server to the outside
- Time service protocol running
- Working global DNS service
- NAT configuration checked if necessary
- No Other Globus services installed

6.2. Globus Download and Installation

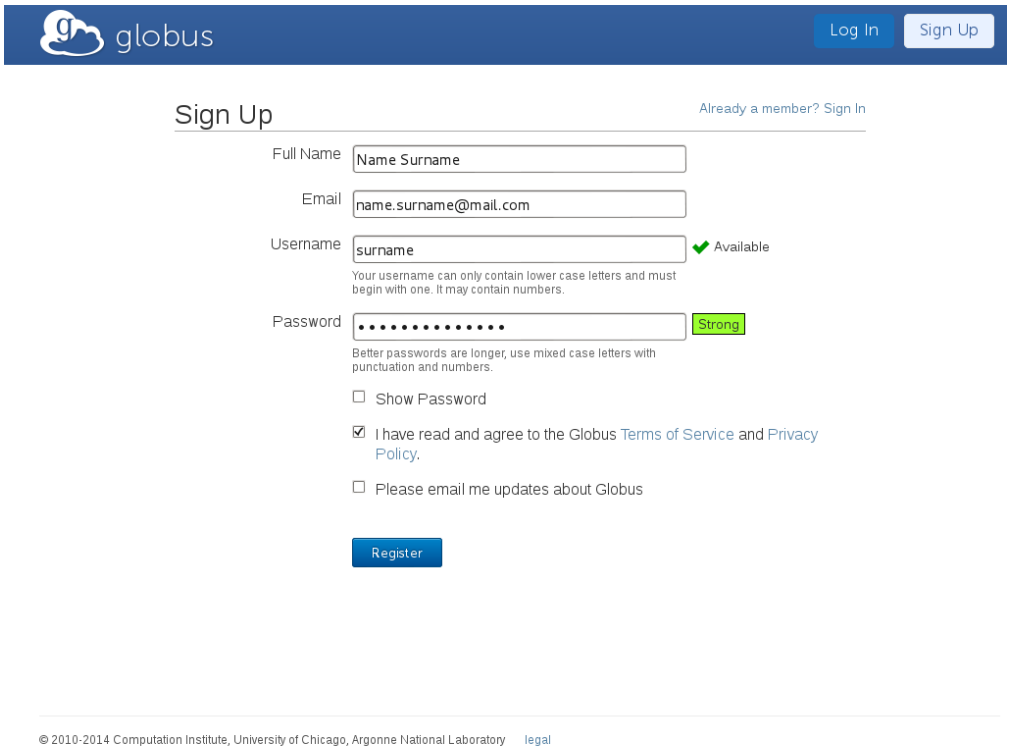
6.2.1. Obtain an account at Globus website

To use any Globus services you need to get an account at their website. This should be a personal account with your own identity. Later in the project will have

a community Account with a common Identity *H3ABioNet#*. So that all endpoints will be easier to find. Like XSEDE:



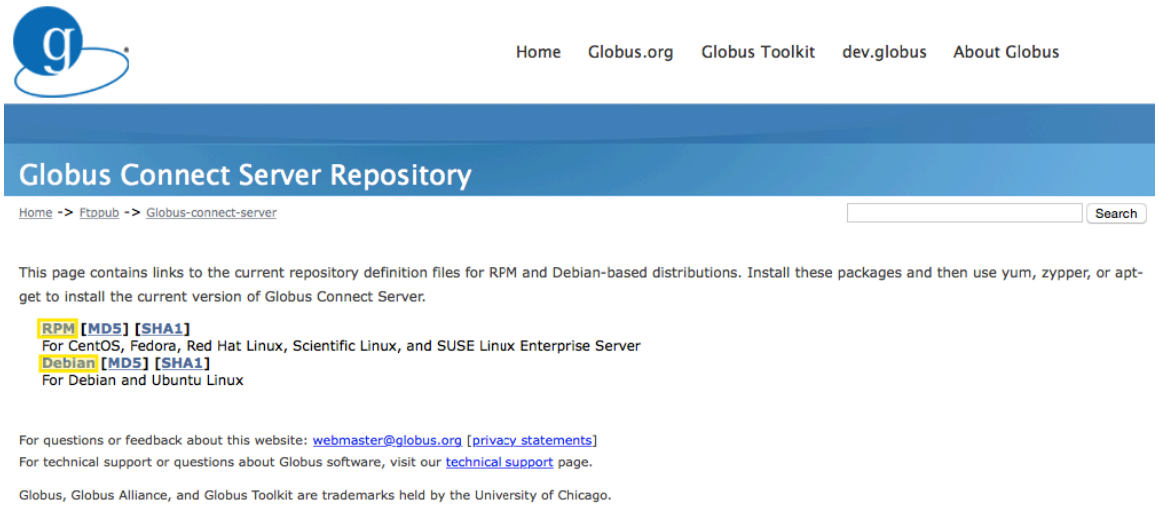
In order to sign up for a personal account you should go to this link and fill out the form. https://www.globus.org/SignUpsudo



After filling this form you will receive a mail that have the confirmation of your signup, go to that link to verify your account and there you have your Globus account. At that point you can login at Globus webpage and can see what the service provides. Now you have verified that you have an active account and you are ready to install your endpoint.

6.2.2. Download Globus server

Globus community offers some stable Globus packages for download for a variety of Operating Systems, which we can find at the official website repository: http://toolkit.globus.org/ftppub/globus-connect-server



Carefully choose the right repository package for the distribution installed on the server. Installing this package will add the Globus repository to your package manager's list of accepted software sources. To check the distribution installed on your machine type:

Ubuntu of Debian: *sudo lsb_release -a*

Scientific Linux: *sudo lsb_release –a* or *sudo more /etc/system-release*

```
root@plane:/home/alibi# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04 LTS
Release:        14.04
Codename:       trusty
root@plane:/home/alibi#
```

To download the appropriate Globus repository package using the command line: *sudo wget –c <<Link to the package>>*

6.2.3. Install Globus on Debian 7 Wheezy

The *wget* command for the current version of Debian is:

wget –c http://toolkit.globus.org/ftppub/globus-connect-server/globus-connect-server-repo_latest_all.deb

```
root@truck:/home/alibi# wget -c http://www.globus.org/ftppub/gt5/5.2/stable/installers/repo/globus-repository-5.2-stable-wheezy_0.0.3_all.deb
--2014-05-19 12:39:15--  http://www.globus.org/ftppub/gt5/5.2/stable/installers/repo/globus-repository-5.2-stable-wheezy_0.0.3_all.deb
Resolving www.globus.org (www.globus.org)... 50.16.193.77
Connecting to www.globus.org (www.globus.org)|50.16.193.77|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4578 (4.5K) [application/x-debian-package]
Saving to: `globus-repository-5.2-stable-wheezy_0.0.3_all.deb'

100%[======================================================================>] 4,578       --.-K/s   in 0s

2014-05-19 12:39:15 (279 MB/s) - `globus-repository-5.2-stable-wheezy_0.0.3_all.deb' saved [4578/4578]

root@truck:/home/alibi#
```

After downloading the Globus repository for the Debian distribution, we move to the installation part:

sudo cd <<package download folder>>

sudo dpkg –i globus-connect-server-repo_latest_all.deb

sudo apt-get update

Now to actually install the Globus Connect Server:

sudo apt-get -y install globus-connect-server

```
alibi@truck:~$ sudo su
[sudo] password for alibi:
root@truck:/home/alibi# cd Downloads/
root@truck:/home/alibi/Downloads# dpkg -i globus-repository-5.2-stable-wheezy_0.0.3_all.deb
(Reading database ... 141658 files and directories currently installed.)
Preparing to replace globus-repository-5.2-stable-wheezy 0.0.3 (using globus-repository-5.2-stable-wheezy_0.0.3_all.deb) ..
.
Unpacking replacement globus-repository-5.2-stable-wheezy ...
OK
Setting up globus-repository-5.2-stable-wheezy (0.0.3) ...
OK
root@truck:/home/alibi/Downloads# apt-get update
Hit http://http.us.debian.org wheezy Release.gpg
Hit http://http.us.debian.org wheezy-updates Release.gpg
Hit http://http.us.debian.org wheezy Release
Hit http://http.us.debian.org wheezy-updates Release
Hit http://http.us.debian.org wheezy/main Sources
Hit http://http.us.debian.org wheezy/contrib Sources
Hit http://http.us.debian.org wheezy/non-free Sources
Hit http://http.us.debian.org wheezy/non-free amd64 Packages
Hit http://http.us.debian.org wheezy/contrib amd64 Packages
Hit http://http.us.debian.org wheezy/main amd64 Packages
Hit http://http.us.debian.org wheezy/contrib Translation-en
Hit http://www.globus.org wheezy Release.gpg
Hit http://http.us.debian.org wheezy/main Translation-en
```

```
root@truck:/home/alibi/Downloads#
root@truck:/home/alibi/Downloads# apt-get install globus-connect-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

After making sure that the installation is done we should make some configuration changes in the Globus configuration file: */etc/globus-connect-server.conf*

```
root@plane:/home/alibi# nano /etc/globus-connect-server.conf
```

We need to change some lines in this file before starting the endpoint:

[Endpoint]

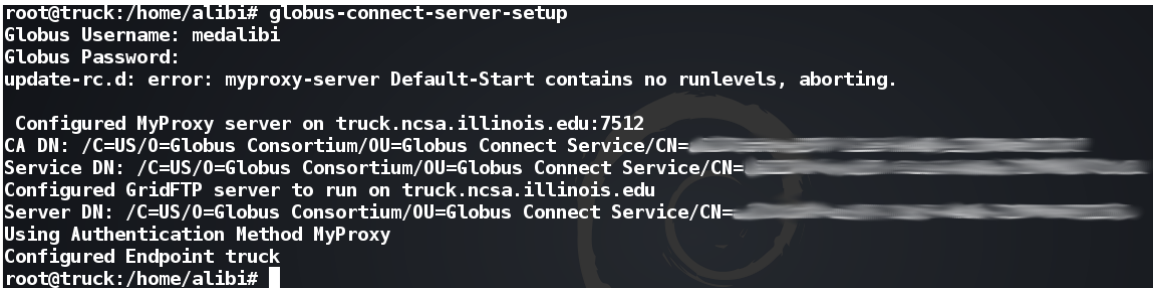
Public = True

ServerBehindNAT = True #set True if your server is on NAT.

After configuring Globus we should start the endpoint by typing:

sudo globus-connect-server-setup

Enter the Login and Password of your Globus account.



The setup is done if you get the message **Configured Endpoint <<Name>>.**

To verify that you endpoint is available you should check the Globus website and see if you can find it in the list of endpoints "Administrated by me".

6.2.4. Install Globus on Scientific Linux 6.5

Go to the download folder then start the installation. For the Redhat-based systems, we need to add a second repository called Epel before installing Globus.

cd /<<Download Folder>>

Download both repository rpms.

wget –c http://toolkit.globus.org/ftppub/globus-connect-server/globus-connect-server-repo-latest.noarch.rpm

wget –c http://download.fedoraproject.org/pub/epel/5/i386/epel-release-5-4.noarch.rpm

Install both repositories.

sudo yum install epel-release-5-4.noarch.rpm

sudo yum install globus-connect-server-repo-latest.noarch.rpm

PS: You may need to change some repository configuration file, if you get any trouble with the installation command (*sudo yum install globus-connect-server*):

/etc/yum.repo.d/Globus-5.2.stable-config.s.repo

Change all lines with:

*http://www.globus.org/ftppub/gt5/5.2/stable/packages/rpm/sl/**$releasever**/**

to:

*http://www.globus.org/ftppub/gt5/5.2/stable/packages/rpm/sl/**6.4**/**

Save that file then update the repositories with the latest information.

Now start the installation of the Globus Connect Server:

sudo yum install globus-connect-server

```
[root@ncsa alibi]#
[root@ncsa alibi]# cd Downloads/
[root@ncsa Downloads]# ls
epel-release-6-8.noarch.rpm  Globus-5.2.stable-config.sl-6.4-1.noarch.rpm
[root@ncsa Downloads]# rpm -ivh epel-release-6-8.noarch.rpm
Preparing...                ########################################### [100%]
        package epel-release-6-8.noarch is already installed
[root@ncsa Downloads]# rpm -ivh Globus-5.2.stable-config.sl-6.4-1.noarch.rpm
Preparing...                ########################################### [100%]
        package Globus-5.2.stable-config.sl-6.1-1.noarch is already installed
[root@ncsa Downloads]# yum update
Loaded plugins: refresh-packagekit, security
Setting up Update Process
No Packages marked for Update
[root@ncsa Downloads]#
```

We need to change the configuration file of Globus:

/etc/globus-connect-server.conf.

You need to change some lines in this file before starting the endpoint:

[Endpoint]

Public = True

ServerBehindNAT = True #set True if your server is on NAT.

Save the file, then we start the endpoint:

sudo globus-connect-server-setup

Put the Login and the password of your Globus account.

```
[root@ncsa Downloads]# globus-connect-server-setup
Globus Username: medalibi
Globus Password:
 Configured MyProxy server on plane.ncsa.illinois.edu:7512
CA DN: /C=US/O=Globus Consortium/OU=Globus Connect Service/CN=[redacted]
Service DN: /C=US/O=Globus Consortium/OU=Globus Connect Service/CN=[redacted]
Configured GridFTP server to run on plane.ncsa.illinois.edu
Server DN: /C=US/O=Globus Consortium/OU=Globus Connect Service/CN=[redacted]
Using Authentication Method MyProxy
Configured Endpoint plane
[root@ncsa Downloads]#
```

The setup is done if you get the message **Configured Endpoint <<Name>>.**

To verify that you endpoint is available you should check the Globus website and see if you can find it in the list of endpoints “Administrated by me”.

6.2.5. Install Globus on Ubuntu 14.04 Trusty

Since Ubuntu and Debian share the same packet architecture there will be no difference in the installation. You will be downloading the **Ubuntu Saucy 13.10** version for **Ubuntu Trusty 14.04** as that’s the latest version available. We have tested this and it works for Trusty.

cd <<Download Folder>>

sudo wget –c http://toolkit.globus.org/ftppub/globus-connect-server/globus-connect-server-repo_latest_all.deb

sudo dpkg –i globus-connect-server-repo_latest_all.deb

sudo apt-get update

sudo apt-get install globus-connect-server

```
root@ubutruck:/home/alibi# cd Downloads/
root@ubutruck:/home/alibi/Downloads# ls
globus-repository-5.2-stable-saucy_0.0.3_all.deb
root@ubutruck:/home/alibi/Downloads# dpkg -i globus-repository-5.2-stable-saucy_0.0.3_all.deb
(Reading database ... 188652 files and directories currently installed.)
Preparing to unpack globus-repository-5.2-stable-saucy_0.0.3_all.deb ...
Unpacking globus-repository-5.2-stable-saucy (0.0.3) over (0.0.3) ...
OK
Setting up globus-repository-5.2-stable-saucy (0.0.3) ...
OK
root@ubutruck:/home/alibi/Downloads# apt-get update
```

```
root@ubutruck:/home/alibi/Downloads# apt-get install globus-connect-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

We need to change the configuration file of Globus:

/etc/globus-connect-server.conf.

You need to change some lines in this file before starting the endpoint:

[Endpoint]

Public = True

ServerBehindNAT = True #set True if your server is on NAT.

Save the file, then we start the endpoint:

sudo globus-connect-server-setup

Put the Login and the password of your Globus account.

```
root@plane:/home/alibi# globus-connect-server-setup
Globus Username: medalibi
Globus Password:
 Configured HyProxy server on plane.ncsa.illinois.edu:7512
CA DN: /C=US/O=Globus Consortium/OU=Globus Connect Service/CN=[redacted]
Service DN: /C=US/O=Globus Consortium/OU=Globus Connect Service/CN=[redacted]
Configured GridFTP server to run on plane.ncsa.illinois.edu
Server DN: /C=US/O=Globus Consortium/OU=Globus Connect Service/CN=[redacted]
Using Authentication Method HyProxy
Configured Endpoint plane
root@plane:/home/alibi#
```

The setup is done if you get the message **Configured Endpoint <<Name>>.**

To verify that you endpoint is available you should check the Globus website and see if you can find it in the list of endpoints “Administrated by me”.

6.3. Globus Server Endpoint Online Activation

Any user can use a Globus Endpoint with a local account on the server. Each user must activate the endpoint for his personal use on the Globus website. To activate the endpoint the user logs in to Globus first and then selects the endpoint

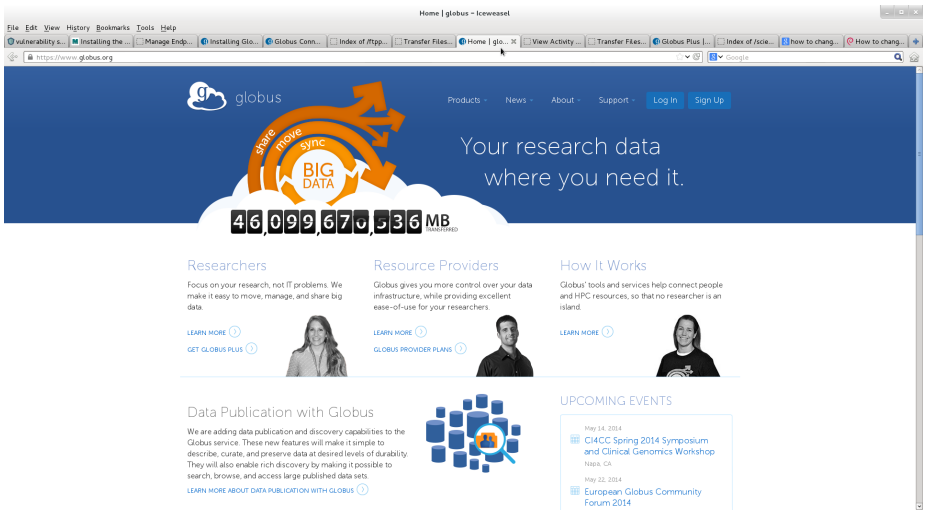
to activate. Using his local login and password for that server Globus allows the user to activate each endpoint separately.

Your Globus endpoint can be only activated by a local account on the server. It needs a non-root user to activate it.

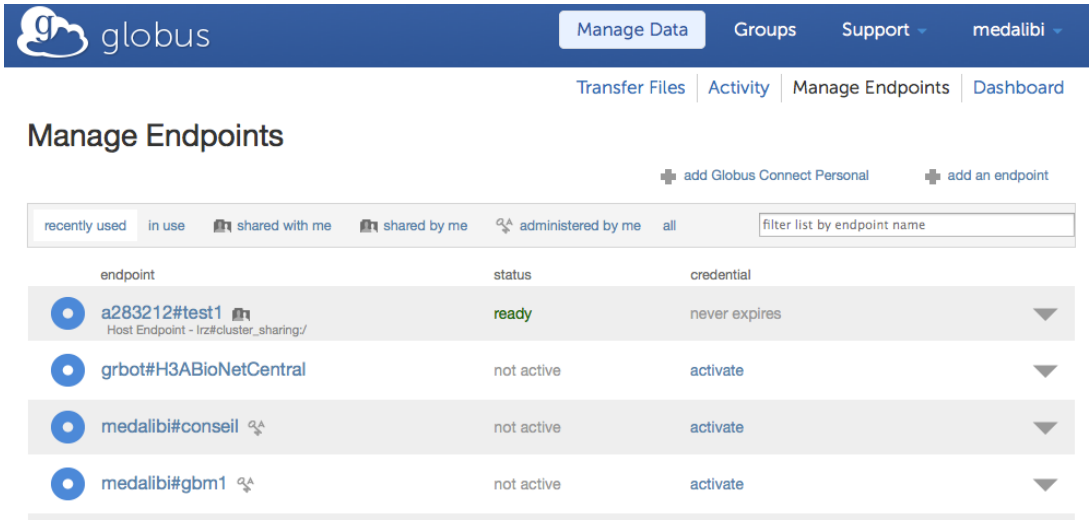
6.3.1. Example

To activate an endpoint you need to login with your Globus account and go to the **Manage Endpoint** page then click on **Administrated by me** and click **activate** on the **credentia**l of the endpoint desired to be activated, **Activate Now**, type local user and password and you can choose how many hours the endpoint should stay activated in **advanced.** Then **Authenticate.**

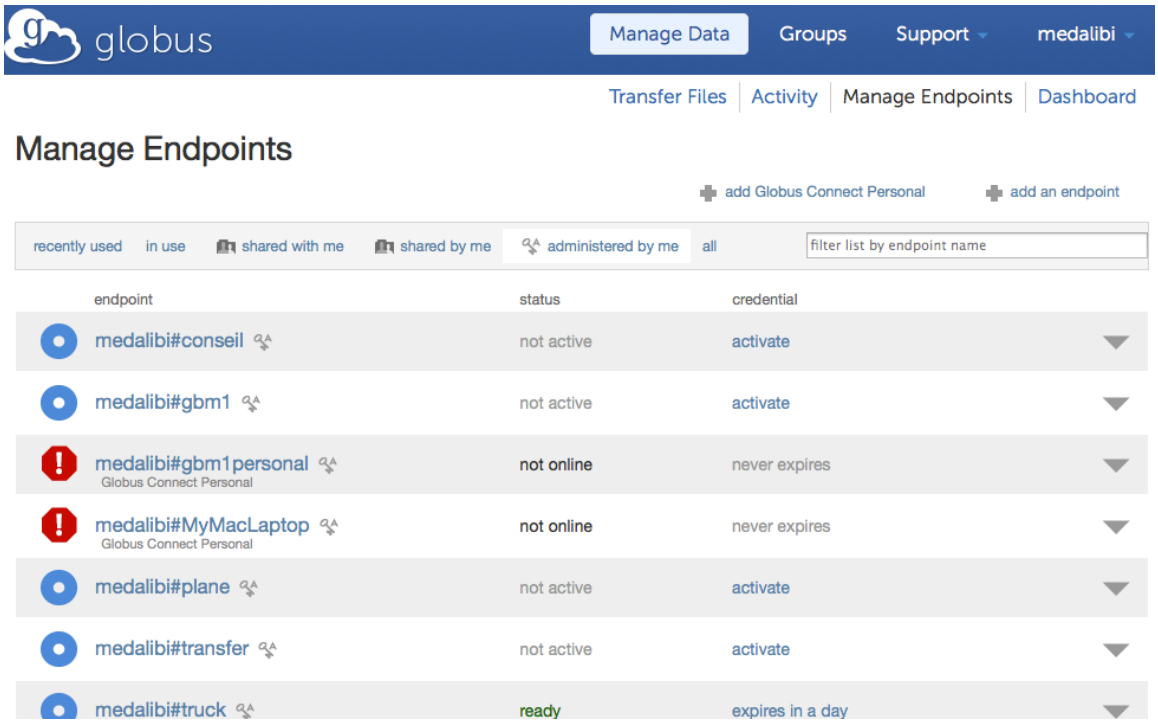
- This is the Globus main page:



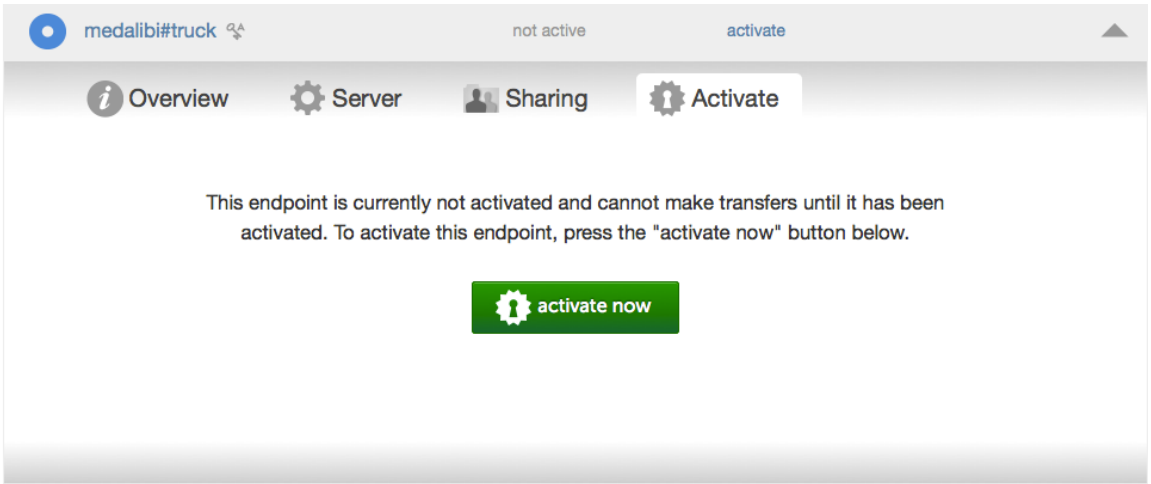
- This is the page where you can manage your endpoints:



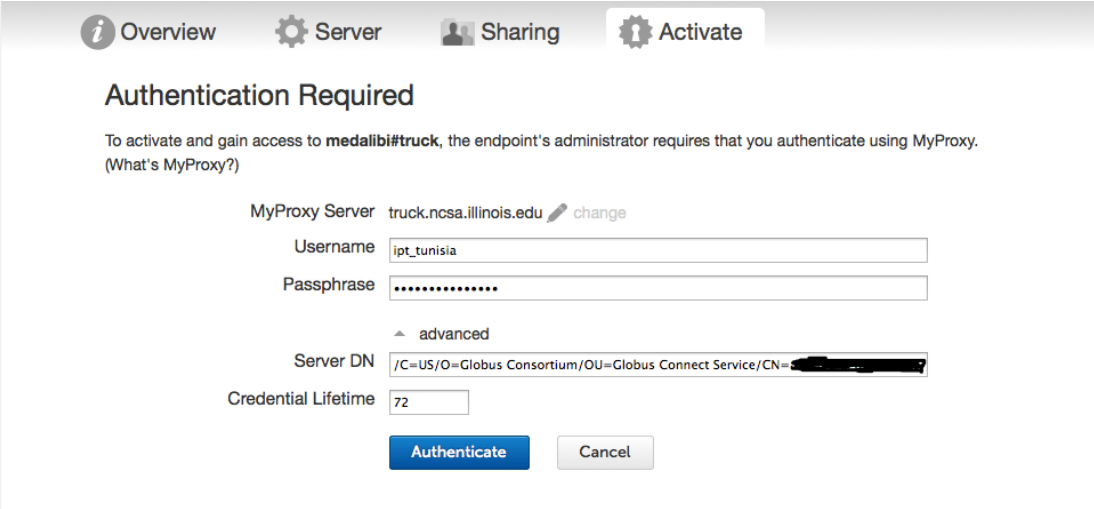
- This is the section where you can find the endpoint administrated by you:



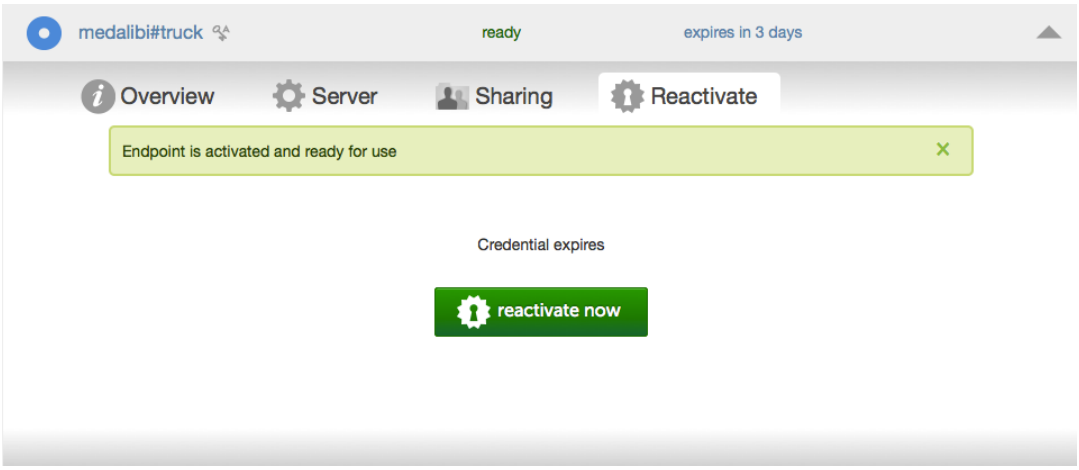
- When you try to activate an endpoint you get this section:



- This is the form where you enter your local user name and password. You can set the duration of activation of your endpoint as well:



- There you have your endpoint activated:



7. Globus Connect Personal Installation and Activation

Globus Connect personal turns your laptop or other personal computer into a Globus endpoint through some simple steps. Which you can use it to move data without any administrative privileges. Globus Connect Personal is for an individual user only and we will use it here simply to verify that the server works.

7.1. Globus Connect Personal Download and Installation

Download the Globus Connect Personal for your desired system from the Globus webpage at this link:

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

You can choose between three major operation systems Type:

Mac: https://support.globus.org/entries/23879396

Linux: https://support.globus.org/entries/23881557

Windows: https://support.globus.org/entries/24000367

After downloading the software you can install it on your laptop. For both Windows and Mac all you need is to double click on the software icon then fellow the steps. On Linux you should open a terminal and type as follow:

cd <<Download Folder>>

tar –xzvf globusconnect-latest.tgz

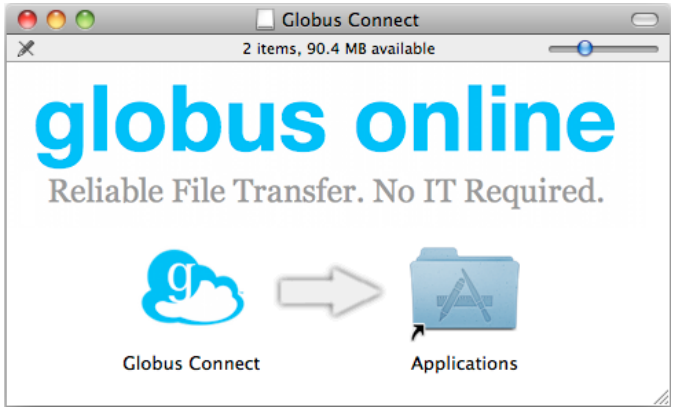
cd globusconnectpersonal-x.y.z (x.y.z is the Globus Connect version)

sh globusconnect &

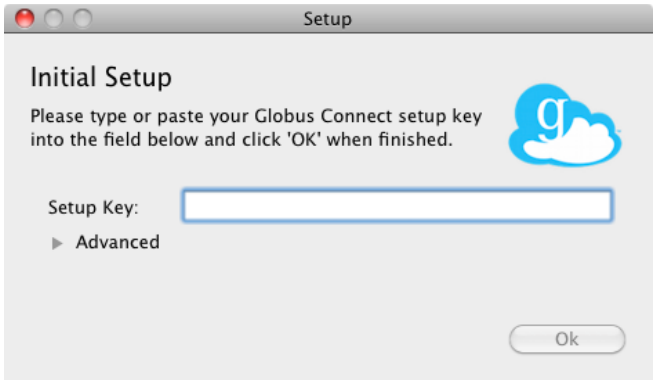
7.1.1. Example

This is the installation of Globus on MacBook laptop.

- This how to add the Globus Connect personal to you Application folder



- After you open Globus connect Personal you get this page to initialize the service and activate the Endpoint. Which we will see in the next section



7.2. Globus Connect Personal activation

Globus Connect Personal gets activated at the first use. It's a permanent activation. While the program is running the endpoint is working.

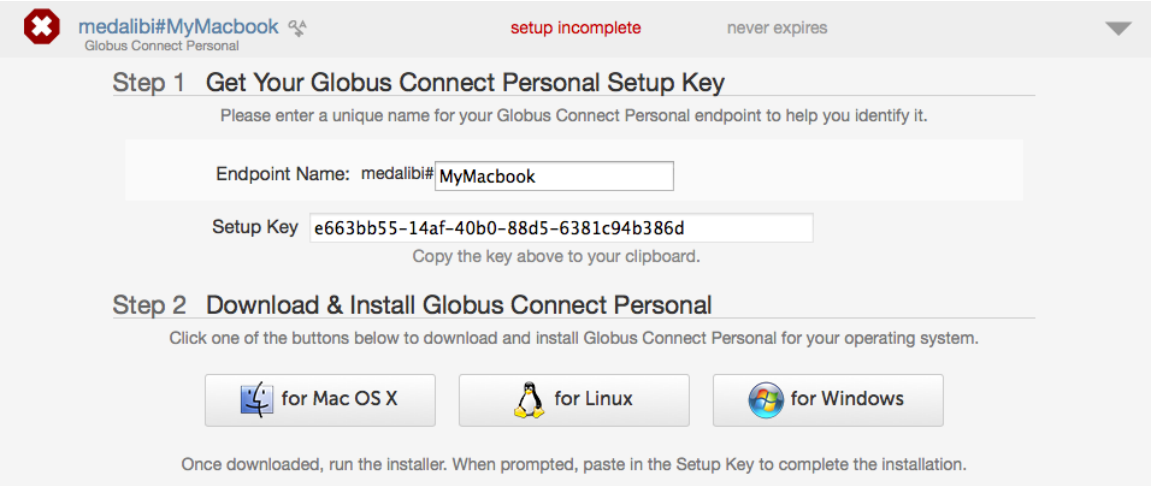
This is how to activate it:

Go to the Manage Endpoint link at Globus website and add an Globus Connect personal endpoint, name it, and generate the setup key to type it at the machine when initializing the program for first use.

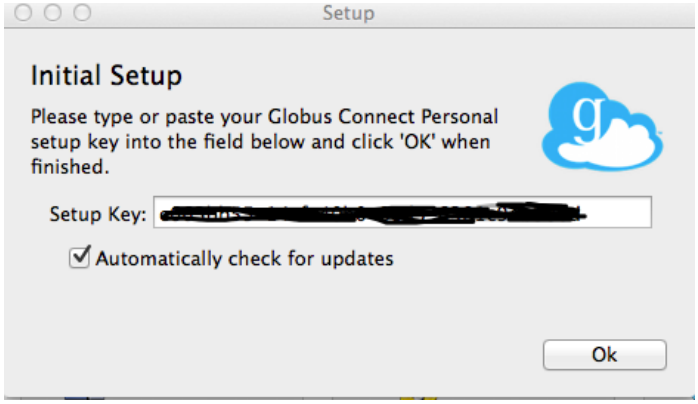
https://www.globus.org/xfer/ManageEndpoints#

7.2.1. Example

- Get the setup code from the **Manage Endpoint** page after clicking on the **add Globus Connect Personal** Type the Endpoint name and then click on **Generate Setup Key**.



- Then go back to the installation and put the **Setup Key** there.



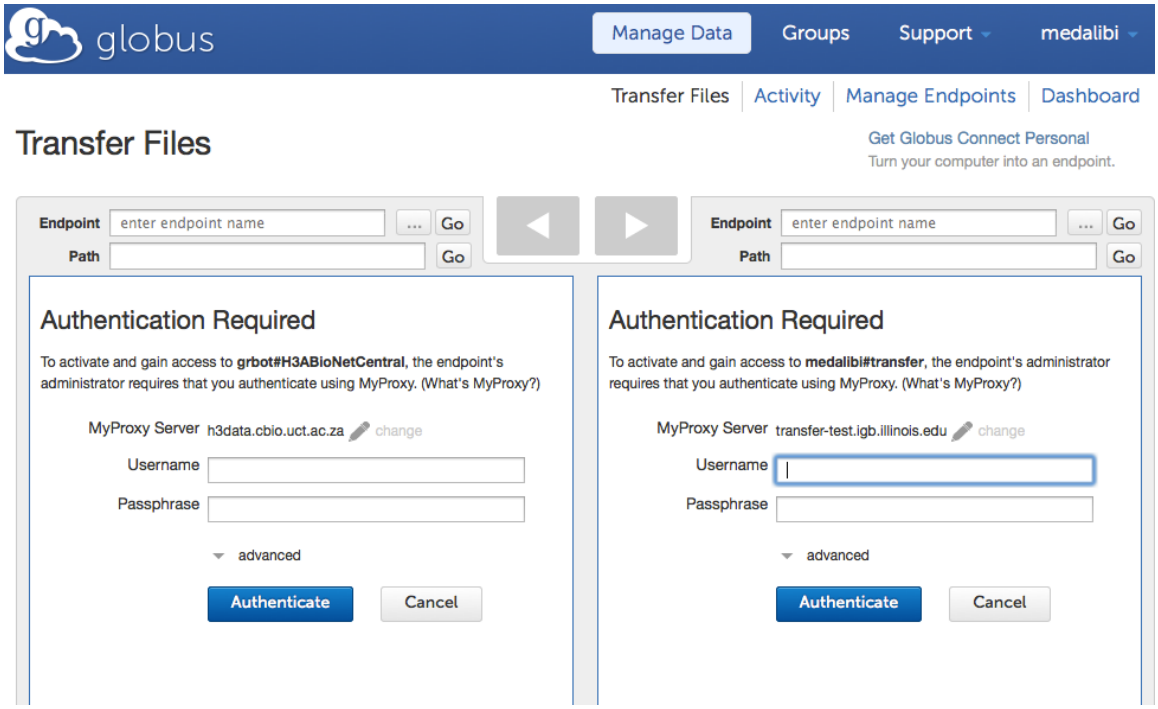
- And then you will have Globus Connect endpoint activated and ready to move data.

8. Transfer File between two Endpoints

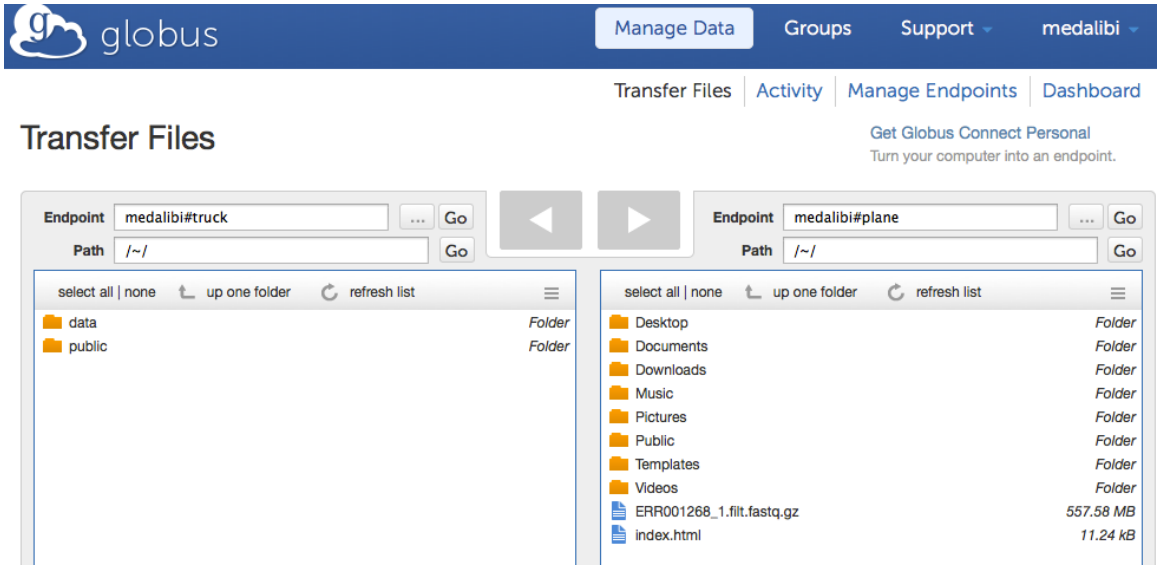
Now we are ready to use Globus to move data

To transfer file between two Globus endpoints you need to get them both activated and then you can start the transfer.

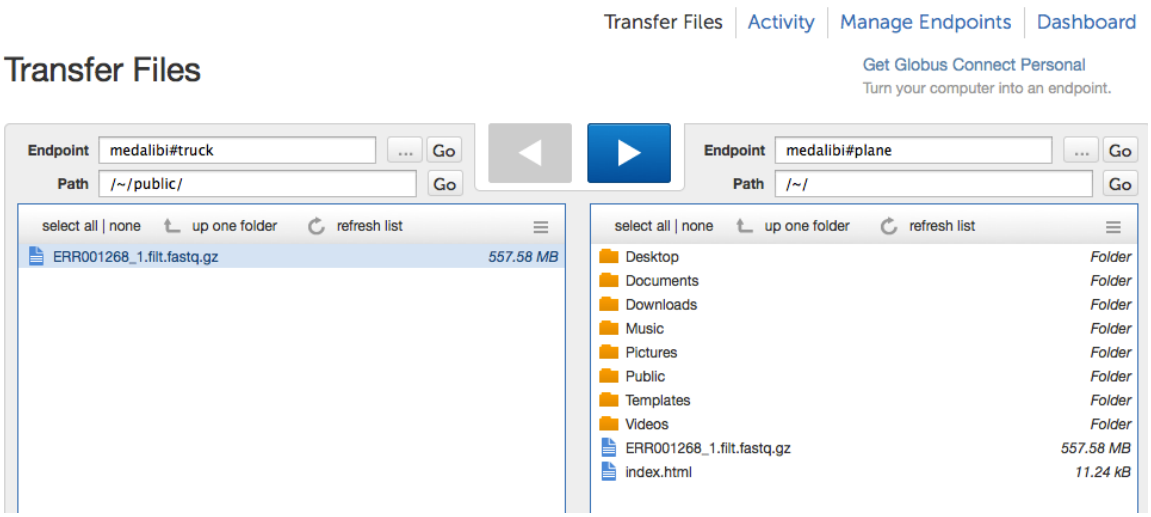
- Open the Transfer Files page



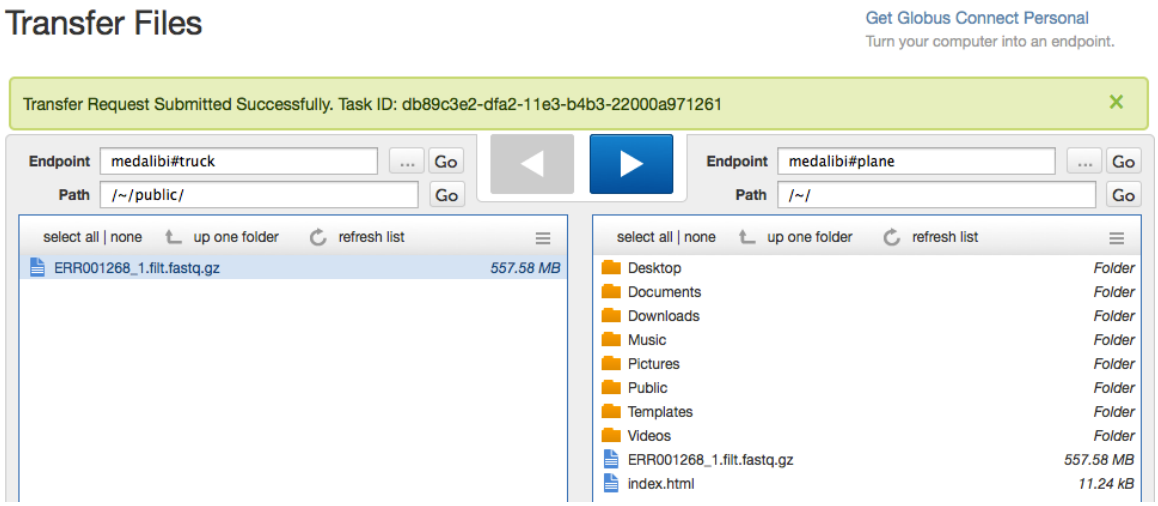
- Choose your two endpoints (Server/Personal)



- Choose the files to send.

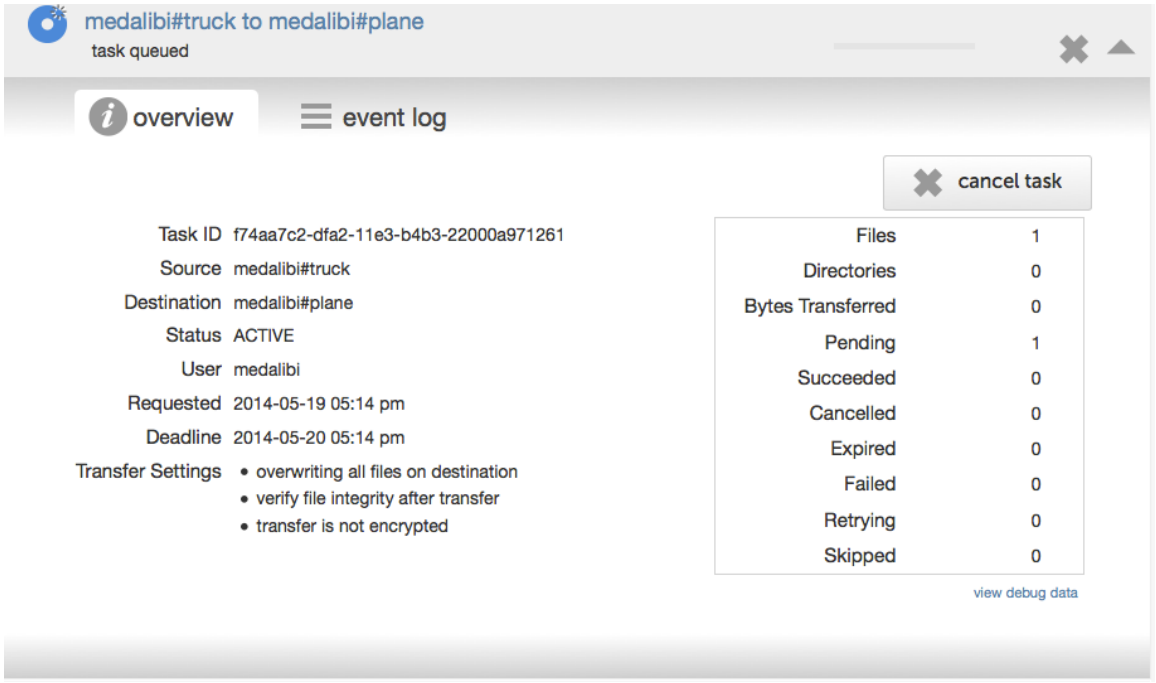


- Click on the arrow to start the transfer.

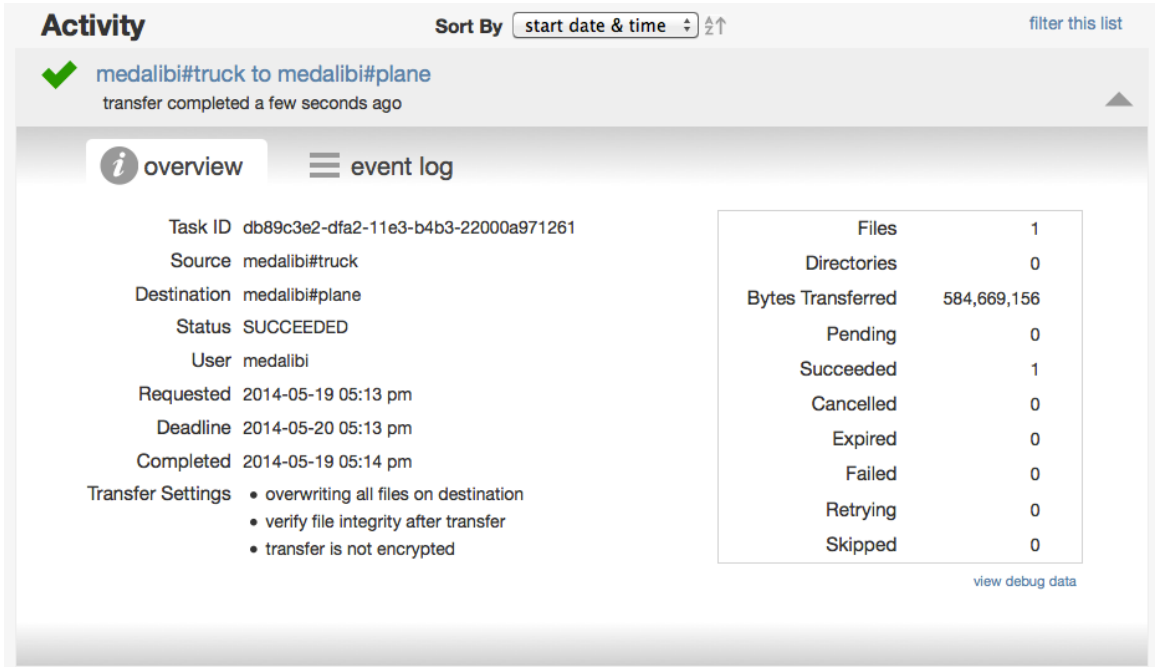


- Verify that the transfer was given a task ID at the Activity page
- At this point Globus accepted the transfer job, it may not succeed but Globus thinks it's possible, and will keep trying for at least 24 hours.

- You can always check the progress of the transfer



- If it succeeds you will get this message



Some advanced transfer options can be made via the advanced options menu. You can see how to make it at the **Appendix D**.

9. Globus Endpoint Administration

In our case many researchers will be using the same Endpoint to send or receive data. Having all users and the administrator account in one machine need to be well configured for better security.

9.1. Account creation and restriction management

The accounts in each server should be categorized in three types:

- **The remote administrators:** They are the ones who help setting up things (Task-force members). They have the capacity to login to the server via SSH (Secure Shell) and can execute some commands to install software for H3ABioNet.
- **The Standard users:** They are the people who are normally at the local site. They may run some applications on the server. They login via SSH. And they can do transfers between nodes.
- **The data transfer users only:** Also known as the Community Users. They only need to transfer data. They must have an account on the system to make them login using Globus. They should not be able to login via SSH nor execute command via any other service (Galaxy, FTP-server…).

The Data transfer users should only have an account at the Main archive node (UCT) or if needed between a group of node that work on collaboration so they may need to add some community account or a user account from an other node so they can transfer data to that site.

How do we separate the three types of accounts on the system so that they all have the correct permissions?

We need to add all the users the same way with no exception, and then we start configuring some services and changing some files to separate the three types of accounts.

9.1.1. Add Users to the endpoint

Add the new users to your endpoint with your standard process. If you're not familiar with this see **Appendix B**.

9.1.2. Configure the Remote Administrator Settings

Then we start defining every user to each category.

If the user has the right to install application and some administration then you should add the user to the administrators group and sudoers:

sudo usermod –a –G adm <<user_name>>

sudo usermod –a –G sudo <<user_name>> (If you have sudo installed)

Because they will not be restricted no further action will be necessary.

9.1.3. Configure the Standard User Settings

Because they will not be restricted no further action will be necessary.

9.1.4. Configure the Data Transfer Only (DTO) User Settings

For the DTO user category after adding them we should deactivate some privilege like remote login and shell execution.

To prevent a login and shell execution by the DTO users you should modify the passwd file */etc/passwd* .

Change the line associated to the user we need to deactivate. Change the users shell from */bin/*sh* to */bin/false*. Example:

*username:x:1000:1001:Full Name,,,:/home/username**:/bin/tcsh***

*username:x:1000:1001:Full Name,,,:/home/username**:/bin/false***

You can see how to only disable SSH access at **Appendix C**.

Check this link for more security measure if needed:

http://plusbryan.com/my-first-5-minutes-on-a-server-or-essential-security-for-linux-servers

9.1.5. User Account Deactivation

We have well explained user account creation and restriction management, and now we are going to explain how to disable a user from using the endpoint or deleting it from the system.

To disable a user type:

sudo passwd -l <<username>> This command disable the user form using the password to login so he won't be able to activate the endpoint.

9.1.6. User Account Reactivation

To restore the user privilege:

sudo passwd -u <<username>>

You don't need to retype the password. The user will activate the endpoint using his original password.

9.2. File restriction management

For user privacy in sharing and transferring data between sites, we need to create a private folder for each user in the server. These folders will be on the shared data space in the server. Usually it will be mounted as */data.*

For some data broadcast cross the H3ABioNet Grid we need to have a shared folder to so that every one have the capacity to read data from that folder and download it to his site.

9.2.1. Create the Private Folder for Each User

First you need to create a folder in the shared space for each user

sudo mkdir /data/<<username>> #Replace username with the actual user name for each user.

Then assign the correct ownership and permissions

sudo chown –R <<username>> /data/<<username>>

sudo chmod –R 700 /data/<<username>>

Then you link the folder to the users home directory

sudo ln –s /data/<<username>> /home/<<username>>/data

```
root@truck:/home/alibi# mkdir /data/ipt_tunisia
root@truck:/home/alibi# chown -R ipt_tunisia /data/ipt_tunisia
root@truck:/home/alibi# ls -l /data/
total 20
drwxr-xr-x 2 ipt_tunisia root  4096 May 19 12:54 ipt_tunisia
drwx------ 2 root        root 16384 May  1 05:28 lost+found
root@truck:/home/alibi#
```

```
root@truck:/home/alibi# ln -s /data/ipt_tunisia/ /home/ipt_tunisia/data
```

9.2.2. Create the Public Folder

We will create one public folder and we will provide a link to it for each user.

sudo mkdir /data/public

Set the folder permissions to allow access to all.

sudo chmod -R 755 /data/public

Link it in every User home folder.

sudo ln –s /data/public /home/<<username>>/public

9.3. Endpoint Service Management

After finishing the installation and the test you have an endpoint ready to move data. Some management may be needed.

9.3.1. Endpoint Automatic Startup

When you install Globus Connect server or Personal they may not start automatically then you may need to add the to the startup application.

Globus Connect Personal Startup activation:

- **Windows:**

For the Windows users of Globus Connect personal you need to add the application to the system configuration *msconfig* at *Statup* list.

- **Mac OS X:**

At the OS X System preferences go to *Users and Groups* icon and add Globus Connect Personal to the *Login Items*.

- **Linux Desktop:**

Ubuntu Gnome use a tool named *Startup application,* it's possible to add application so they start automatically during the OS startup.

Globus Connect Server Startup activation

Globus Connect server is based on three services that should be running to so the endpoint will be working properly.

- myproxy-server
- globus-gridftp-sshftp
- globus-gridftp-server

- **Debian and Ubuntu server:**

To activate Globus Connect server you need to add the three services to the system startup services using the command *update-rc.d.*

sudo update-rc.d myproxy-server defaults

sudo update-rc.d globus-gridftp-sshftp defaults 20 80 (the 20 and 80 are optional to indicate when the process should run and get killed)

sudo update-rc.d globus-gridftp-server defaults 20 80 (the 20 and 80 are optional to indicate when the process should run and get killed)

To disable the auto startup replace *defaults* by *remove:*

sudo update-rc.d globus-gridftp-server remove

- **Scientific Linux:**

We need also to activate the three services using the command *chkconfig*.

sudo chkconfig --add myproxy-server

sudo chkconfig --add globus-gridftp-sshftp

sudo chkconfig --add globus-gridftp-server

To disable the auto startup replace the *--add* by *--del*:

sudo chkconfig --del globus-gridftp-server

9.3.2. Endpoint deactivation

For some reason and endpoint may need to be deactivated. For the Globus Connect personal all you need is to close the program running and the endpoint is deactivated. And for deactivating the Globus Connect Server we need to use the command *service* for al Linux systems:

sudo service myproxy-server stop

sudo service globus-gridftp-server stop

sudo service globus-gridftp-sshftp stop

```
root@truck:/etc/init.d# service globus-gridftp-server stop
[ ok ] Stopped GridFTP Server.
```

If we like to activate it after we can use the same command with different option.

sudo service globus-gridftp-server start

```
root@truck:/etc/init.d# service globus-gridftp-server start
[ ok ] Started GridFTP Server.
```

10. Appendix A: How to Use Nano (File Editor)

Here a short section about editing files in Linux using command line for those who are not familiar with it.

You can use whatever editor you want. We have included a short intro to nano, is a simple Terminal file editor included by default in the supported OS's.

In this tutorial most of the files that we have been editing are only root editable. So you will be using sudo every time you use nano. To use nano you should type: *sudo nano <<file_location/file_name>>*

Example:

sudo nano /etc/ntp.config

To move around in the file you should use the cursor keys

To save and exit nano: Type *Ctrl + x* then type *Y* then *Enter*

To exit without saving: Type *Ctrl + x* then type *N* then *Enter*

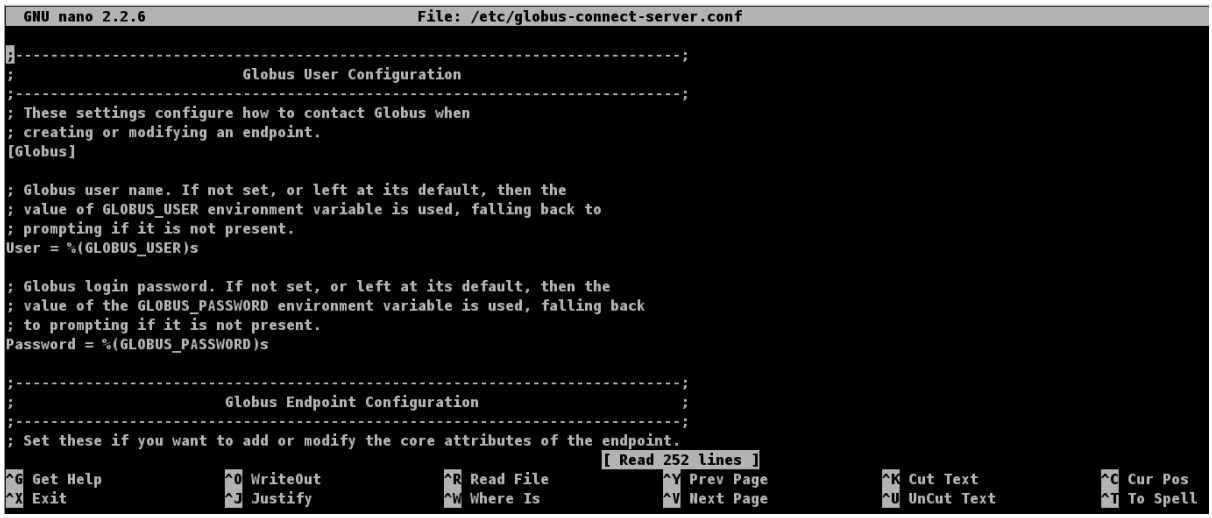
To search for a line: Type *Ctrl + w* then type *the work you looking for* then *Enter*

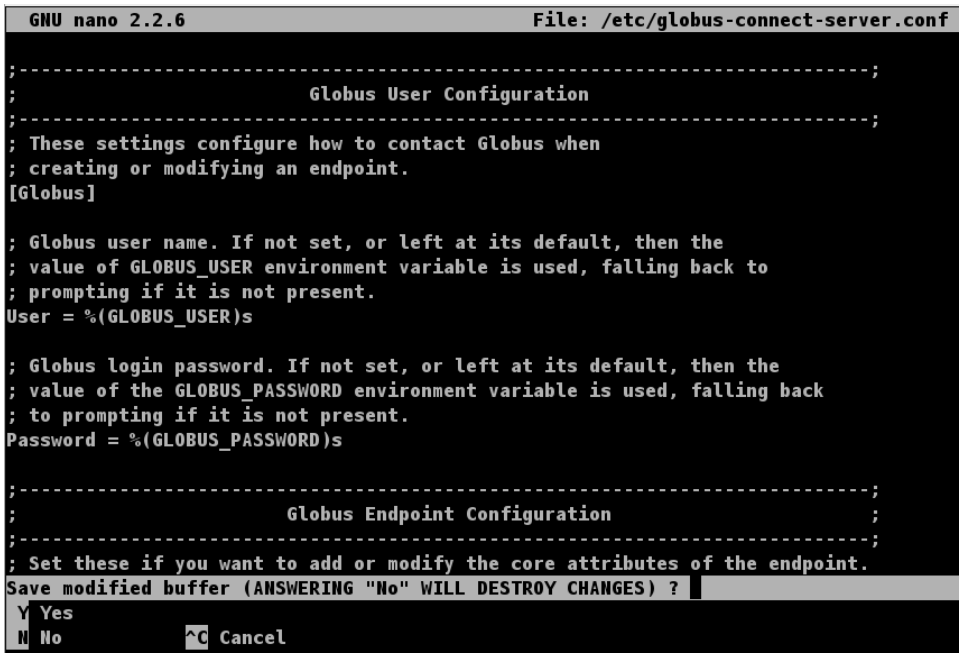
To check to line number: Type *Ctrl + c*

To delete a line: Go to the line then type *Ctrl + k*

To copy something: Select the line or the word then type *Ctrl + Shift + c*

To past something: Select the position then type *Ctrl + Shift + v*





Useful link to learn more about nano commands:

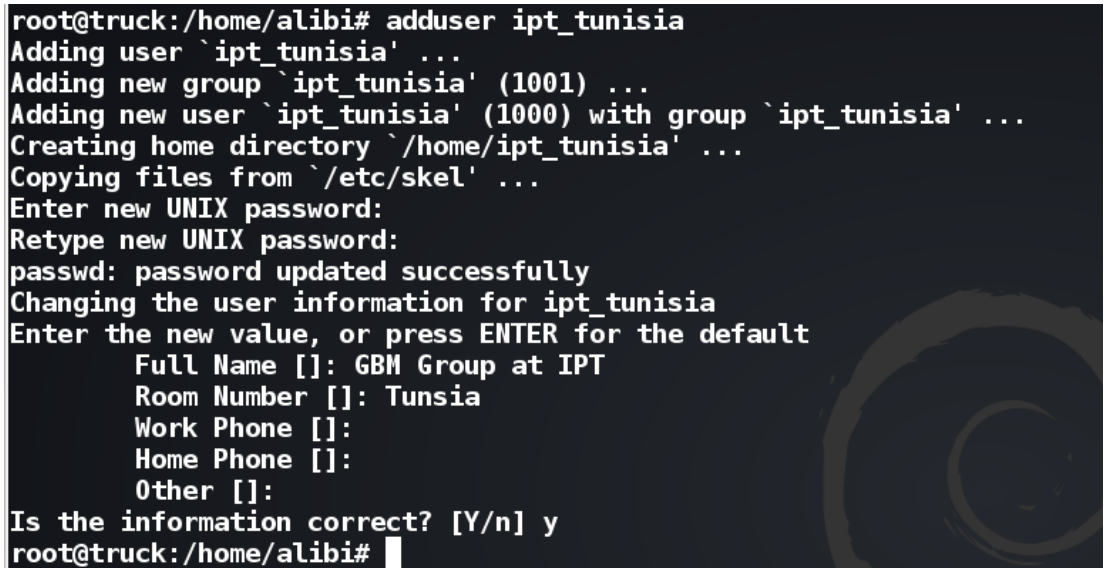
http://mintaka.sdsu.edu/reu/nano.html

11. Appendix B: Add Simple User to the System

Here is a basic guide to adding a user in Linux.

To add a user on a system you can use the *adduser* command, when you do the command it will ask you for a password and you have the opportunity to add other information. By default the user ID is set automatically. You should have the password ready and saved before typing the command, because you need to get that information to the user so they can log in.

sudo adduser <<user_name>> (Type password twice it then Full name etc.. then confirm Yes.)



12. Appendix C: Disable SSH Access

To disable SSH Access only to some user you need to do as follow:

Edit the file: */etc/ssh/sshd_config*

Change the *PermitRootLogin* line from yes to no

Add this line *DenyUsers <<first user name>>, <<second user name>>…* This line should include all the users who are DTO.

Save and then restart the SSH service.

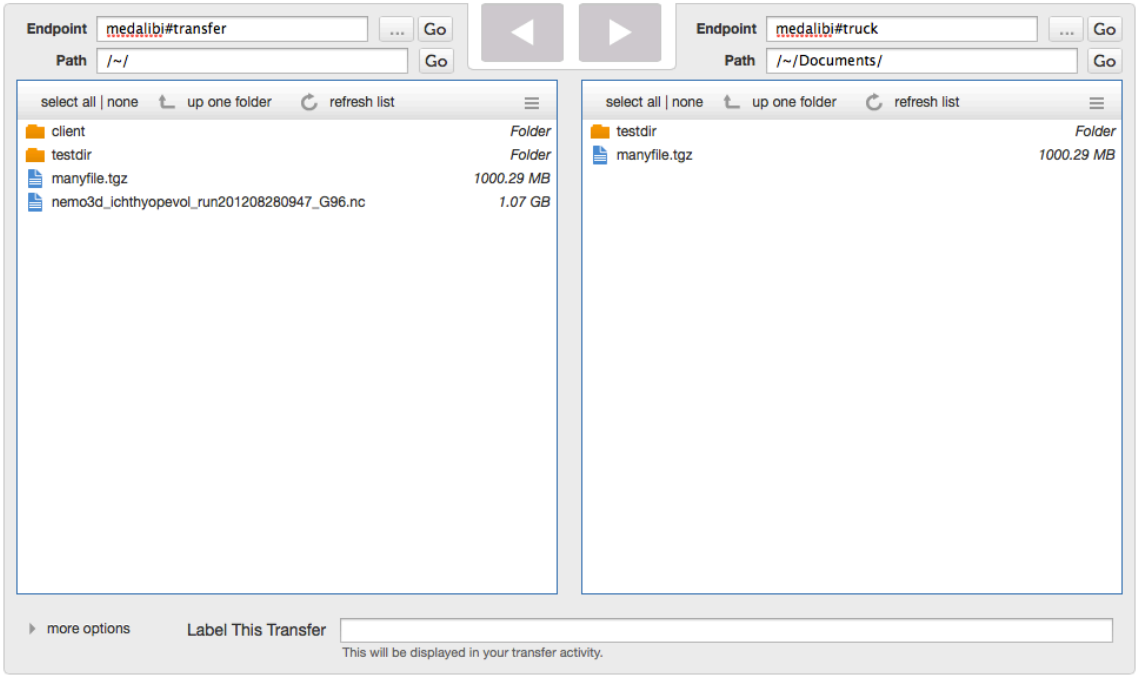
sudo service ssh restart (Some system it is sshd)

Be careful Editing the file */etc/ssh/sshd_config*. If you make a mistake you may disable the SSH service altogether.

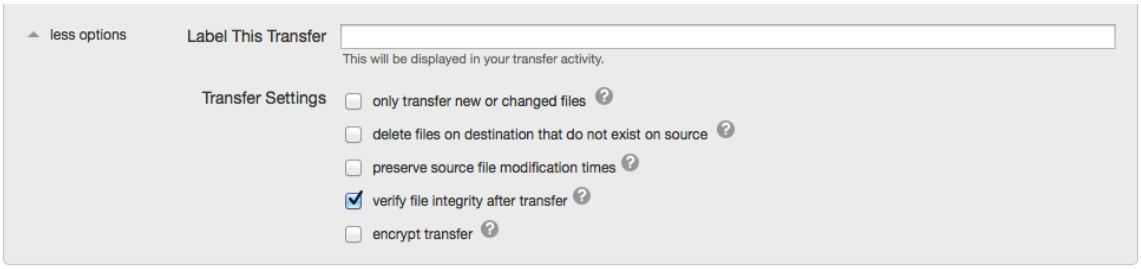
13. Appendix D: Make an Encrypted Transfer

We are going to present how to make an advanced transfer option to have an encrypted transfer.

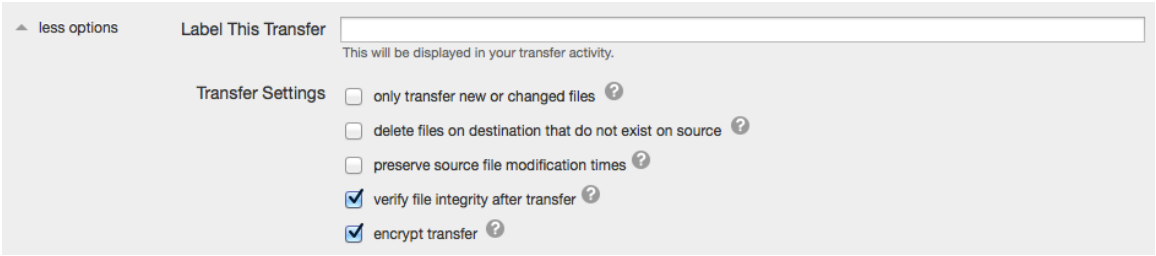
First we should open the transfer page and choose the two endpoints:



Then you should open the advanced option menu in the bottom of the page *more options*:



Then check the encrypt transfer case:



Finally start the transfer like the standard way.

The encryption does not affect the transfer speed that much (tested).

14. Appendix E: Schedule a Globus Transfer

At this section we will be presenting how to script a transfer using Globus and GridFTP features. This method will make the users free to arrange their transfer. For this tutorial we will use the command *globus-url-copy*.

First we need to install some Globus toolkit packages: *globus-gridftp globus-ftp-client-progs*.

sudo apt-get install –y globus-gridftp globus-ftp-client-progs

After making sure the installation is done we can test the command with the basic settings:

globus-url-copy -vb -p 4 source_url destination_url

- Example of two different servers:

globus-url-copy -vb -p 4 sshftp://truck.ncsa.illinois.edu/home/alibi/testdir.tgz sshftp://gbm1.pasteur.tn/home/alibi/

- Example of upload from local to other server:

globus-url-copy -vb -p 4 testdir.tgz sshftp://gbm1.pasteur.tn/home/alibi/

- Example of download from other server to local machine:

globus-url-copy -vb -p 4 sshftp://gbm1.pasteur.tn/home/alibi/testdir.tgz ./

The command options are as follow:

-vb : specifies verbose mode and displays.

-p : Specifies the number of parallel data connections that should be used. This is one of the most commonly used options.

-cc : Specifies the number of concurrent FTP connections to use for multiple transfers.

-cd : Creates destination directories, if needed.

-r : Copies files in subdirectories.

Now we will present the script need to be written for the automatic management of the failures and retries. To retry a transfer after a server or network failure, use the `-rst` option. To store the non-transferred urls for restarting the transfer after a client failure, use the `-df` option.

This is the script code:

```
#!/bin/sh
  STATEFILE=/path/to/statefile;
  while  [ ! -e $STATEFILE -o -s $STATEFILE ];
  do
  globus-url-copy -rst -p 4  -cc 4 -cd -vb -r -df $STATEFILE Source Destination ;
```

sleep 10;

done;

For more information about how to use the *globus-url-copy* command check this link:

http://toolkit.globus.org/toolkit/docs/5.2/5.2.4/gridftp/user/#gridftp-user-advanced-failures

15. Appendix F: GridFTP Log File Generation

This section will be presenting the steps to follow to have a log file that generated by Globus services for the endpoint tractability.

By default Globus services generate a log file in the system logs but they don't really have that much of information about what's going on the endpoint every time it get used.

And there is always a configuration needs to be done at the configuration file of the services. My proxy server is already configured to send every activity to system log you can get the information needed via the *grep* command:

cat /var/log/syslog | grep –I myproxy This command will show you the information about the and point activation.

Most of tractability will be to get information about transfer so we will be tracing the GridFTP log file. GridFTP offers a variety of configuration to its log file so we can choose what to trace. To make so we need to add some line to its configuration file */etc/gridftp.conf*.

The standard lines needs to be put are:

log_level ALL Generate all type of activity haven with this service

log_module syslog Use the syslog module

log_single /var/log/gridftp Generate a specific log file

log_transfer /var/log/gridftp.stats Generate a separate log file for transfer only.

Then you should restart the service so this lines will make affect.

For more information about how to configure the GridFTP log file check this link:

http://toolkit.globus.org/toolkit/docs/4.0/data/gridftp/admin-index.html

16. Appendix G: Globus Transfer Shaping

As far as we have been using Globus we have noticed that it get all the bandwidth available on site and that may cause a bad internet experience with the other users on site. This section will provide a solution to limit bandwidth for upload and download in the server for Globus services only.

To do so I have written a script shell based on *tc* and *iptables* that work as service that you can add it to */etc/init.d* and it have the options "start/stop/restart/show" so you can control it on the server as follow:

After coping the script file inside */etc/init.d*

service trafficShaper start

service trafficShaper stop

PS: This script should run as root. And this script will be sent with the document with the name "trafficShaper".

This script is easy to change. You can use any text editor to change:

- The download and the upload limit rate
- Network Interface name
- The GridFTP ports range

This is the script text:

```
#!/bin/bash
#
#  tc uses the following units when passed as a parameter.
#  kbps: Kilobytes per second
#  mbps: Megabytes per second
#  kbit: Kilobits per second
#  mbit: Megabits per second
#  bps: Bytes per second
#       Amounts of data can be specified in:
#       kb or k: Kilobytes
#       mb or m: Megabytes
#       mbit: Megabits
#       kbit: Kilobits
#  To get the byte figure from bits, divide the number by 8 bit
#

#
# Name of the traffic control command
TC=/sbin/tc
IPTAB=/sbin/iptables

# The network interface we're planning on limiting bandwidth.
```

```
IF=eth0             # Interface

# Download limit (in mega bits)
DNLD=60mbit          # DOWNLOAD Limit

# Upload limit (in mega bits)
UPLD=60mbit          # UPLOAD Limit

# Start and end port to shape the bandwidth on
MINPORT=50000
MAXPORT=51000

# Filter options for limiting the intended interface
U32="$TC filter add dev $IF parent 1:0 prio 1 protocol ip"

start() {

# We'll use Hierarchical Token Bucket (HTB) to shape bandwidth.
# For detailed configuration options, please consult Linux man
# page

    $TC qdisc add dev $IF root handle 1: htb

    $TC class add dev $IF parent 1: classid 1:1 htb rate $DNLD
    $TC class add dev $IF parent 1: classid 1:2 htb rate $UPLD

    $U32 handle 5 fw flowid 1:1
    $U32 handle 6 fw flowid 1:2

    $IPTAB -A INPUT -t mangle -p tcp --sport $MINPORT:$MAXPORT -j
MARK --set-mark 5
    $IPTAB -A OUTPUT -t mangle -p tcp --sport $MINPORT:$MAXPORT -
j MARK --set-mark 6


# The first line creates the root qdisc, and the next two lines
# create two child qdisc that are to be used to shape download
# and upload bandwidth
#
# The 4th and 5th line creates the filter to match the mark for
# the iptables command which is at the 6th and the 7th line
# that indicate the upload or the download data direction and
# the specific ports to do so

}

stop() {

# Stop the bandwidth shaping.
    $TC qdisc del dev $IF root
```

```
    $TC qdisc add dev $IF root handle 1: htb default 9999

}

restart() {

# Self-explanatory.
    stop
    sleep 1
    start

}

show() {

# Display status of traffic control status
    $TC -s qdisc ls dev $IF

}

case "$1" in

  start)

    echo -n "Starting bandwidth shaping: "
    start
    echo "done"
    ;;

  stop)

    echo -n "Stopping bandwidth shaping: "
    stop
    echo "done"
    ;;

  restart)

    echo -n "Restarting bandwidth shaping: "
    restart
    echo "done"
    ;;

  show)

    echo "Bandwidth shaping status for $IF:"
    show
    echo ""
    ;;
```

```
  *)

    pwd=$(pwd)
    echo "Usage: tc.bash {start|stop|restart|show}"
    ;;

esac

    exit 0
```

To run this script daily and make it shape the traffic every working day you should do as follow. First you make sure that you have copied it in the */etc/init.d* folder as a root. Then you should type like this:

sudo crontab –e

A file editor will be opened then you type those two phrases at the end of it:

*30 7 * * 1,2,3,4,5 service trafficShaper start*

*30 18 * * 1,2,3,4,5 service trafficShaper stop*

This example of line is a *cron* job that runs every day of the month and every month of the year but only in weekdays without the Sundays and the Saturdays. The first one will start the traffic shaping at 7:30 AM and the second one will stop it at 6:30PM.

This is an example you can always adjust it to your node working time.

17. Appendix H: Open Port on the Local Firewall

At this phase we are going to use the "Ferm" as our local Firewall on the server. Ferm is a tool to maintain complex firewalls, without the trouble to rewrite the complex rules over and over again. Ferm allows the entire firewall rule set to be stored in a separate file, and to be loaded with one command. The firewall configuration resembles structured programming-like language, which can contain levels and lists.

To use ferm al you need to edit the file */etc/ferm/ferm.conf*

And add those lines:

```
# allow HTTP and HTTPs connections
proto tcp dport http ACCEPT;
proto tcp dport https ACCEPT;

# allow SSH connections
proto tcp dport ssh ACCEPT;

# allow iperf connections
proto tcp dport 5001 ACCEPT;

# allow globus online connections
proto tcp dport 2811 ACCEPT;
proto tcp dport 7512 ACCEPT;
proto tcp dport 50000:51000 ACCEPT;
```

And then restart the ferm service:

sudo service ferm restart