MiG User Introduction

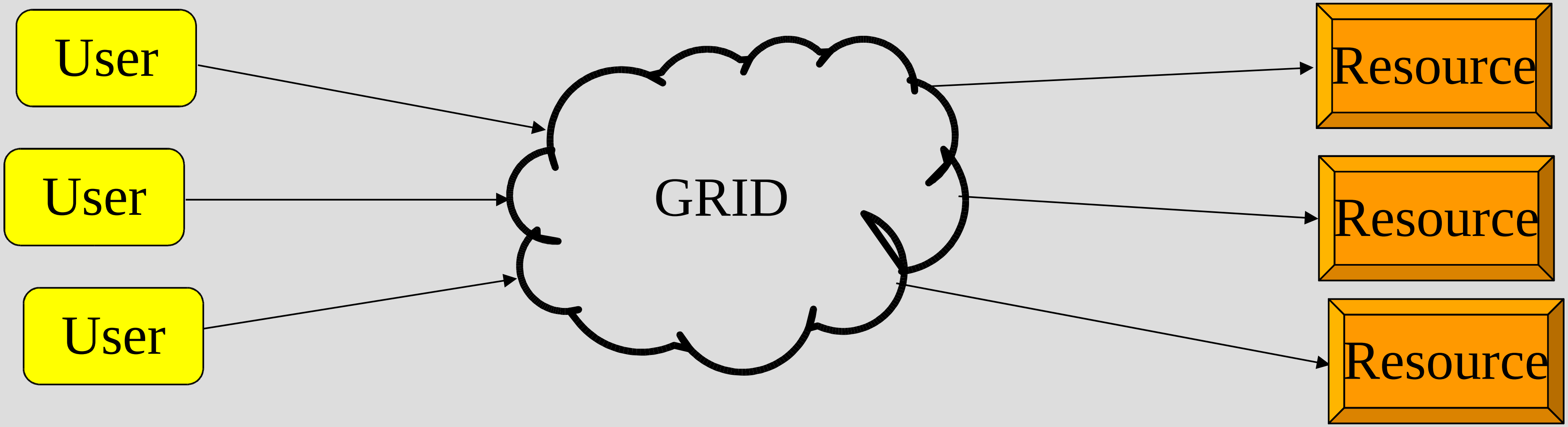
This document is an introduction for **users** of the Minimum intrusion Grid (MiG).

It covers the basic steps required to begin running jobs on MiG. This document is not meant to be exhaustive, so for more information please refer to the on-line docs at:

http://mig-1.imada.sdu.dk

Please direct any questions and comments to the MiG developers at mig@imada.sdu.dk .

MiG Overview



The simplified diagram above depicts the workings of MiG. The user interacts with the Grid through a MiG server. The inner workings and interactions of these servers are not transparent to the users so the servers are simply shown as a GRID cloud. A user can store data on MiG and utilize available computing power on connected resources. Even better, as soon as the user hands over the data or tasks to MiG, the responsibility of storing the data in suitable locations and getting the tasks done is left to the Grid.

Prerequisites

Security in MiG builds on 'digital signatures' in the form of key and certificate files issued by the MiG team.

Thus to get started with MiG, it is necessary to contact us and obtain such a signature.

We strive to respond within a few days, but there's no guarantees.

You can begin using MiG as soon as you receive your signature along with further details about where you can access MiG.

Interacting with MiG

We provide two ways of interacting with MiG. The web interface is simple to use and requires no software installation at all – You just need your key and certificate.

In some cases is may be more convenient and efficient to download and use the simple command line applications instead. In that way it's possible to manage thousands of files and tasks with little extra effort.

Web Interface - Access

The web interface is the fast track to getting started with MiG: Simply import your MiG P12-formatted certificate in your favorite browser and go to your personal MiG page (the address supplied along with your certificate).

During import or use you will be prompted for the password you were given for your key. Please refer to your browser documentation for information about managing certificates.

NorduGrid users: please refer to Appendix A!

Web Interface - Navigation

Now that you've made it through the security check you can start using MiG. The first page you see is the main page where you have access to upload and download of files as well as job management. The page includes a few job description examples to help get you started with MiG. The job description language is documented on the next pages and on: http://mig-1.imada.sdu.dk/cgi-bin/docs.py

MiG User Scripts - Access

The MiG User Scripts is the alternative to the web interface:
They require a Bourne Shell or similar and the curl library (http://curl.haxx.se/).

Download and extract http://mig-1.imada.sdu.dk/MiGscripts.tar.gz
Create the directory ~/.MiG
Copy MiGuser.conf to ~/.MiG/
Edit ~/.MiG/MiGuser.conf to match certificate path and MiG server
Use the scripts as specified on next slide.

MiG User Scripts - Commands

MiGallstatus.sh	status for all jobs
MiGcat.sh file	cat a file on the MiG server
MiGput.sh localfile remotefile	
MiGget.sh remotefile localfile	
MiGlist.sh	list all personal files at MiG server
MiGremove.sh file	delete a file on the MiG server
MiGstatus.sh jobid	status (single job)
MiGsubmit mrslfile	submit job (actually just MiGput.sh mrslfile)
MiGuser.conf	configuration file used by all MiGscripts

User Scripts - Example

Download job specification (mRSL file):

http://mig-1.imada.sdu.dk/example4.mRSL

This example creates and uploads 'inputfile' which is used for outputfile

Run the job:

- echo “test job” > inputfile
- MiGput.sh inputfile inputfile
- MiGsubmit.sh example4.mRSL
  - returns a job_id that is used for further treatment of the job
  - the job creates a file (outputfile)
- MiGstatus.sh job_id
  - to get the status of the job
- MiGcat.sh outputfile
  - to show the job output when job is done
  - Further examples at https://mig-1.imada.sdu.dk/

mRSL keywords (part 1)

"EXECUTE"	one or more commands to execute
"INPUTFILES"	files that should be send from the central MiG server to the resource before executing the commands
"OUTPUTFILES"	the files that should be sent from the resource to the central MiG server when the job is done
"EXECUTABLES"	same as inputfiles, but will be chmod +x by the resource
"CPUTIME"	#minutes will it take to execute the job
"MEMORY":""	MB of memory needed by job
"DISK":	GB of disk space needed by job
"RUNTIMEENVIRONMENT"	specify the needed runtimeenvironments, eg. povray-3.6

mRSL keywords (part 2)

“JOBNAME":	friendly name of the job (not being used ATM)
"NOTIFY":""	email address to notify when the job is done. It is also possible to use jabber: jabberid@jabberserver.com to get a jabber notification
"ARCHITECTURE":	needed architecure (i386)
"ENVIRONMENT":""	env=envvalue will set the environment env to envvalue before the job is executed
"CPUCOUNT":	number of CPU's needed
"MAXPRICE":""	price function of 'exec_delay': must evaluate to an integer or float for all values of exec_delay. Examples: “0” (only exec if it is for free) “200-exec_delay” (only exec within 200 seconds)

Appendix A – NorduGrid users

In case you already own a valid NorduGrid certificate, you don't need a MiG-specific certificate. If so, please supply the Common Name (CN) of your certificate when you request MiG access. When we add you as a MiG user you can simply use your existing NorduGrid certificate and key with the user scripts and a P12 formatted version for the web interface. Create the P12 certificate with:

```
openssl pkcs12 -export -in ~/.globus/usercert.pem -inkey \
~/.globus/userkey.pem -out ~/migcert.p12
```

... type passwords (Export Password is for the new P12 certificate)