Introduction to Globus 5

GridKa Summer School 2010
Overview

• **General**
  - Grid, Globus Toolkit Overview
  - Authentication & Authorisation (A&A)
    ‣ PKI, Certificates
    ‣ GSI, Proxy Certificates, MyProxy, Short Lived Credentials

• **GT5**
  - Interactive Access
    ‣ GSI–OpenSSH
    ‣ Clients
  - Data Transfer
    ‣ Globus GridFTP
  - Job Submission
    ‣ GRAM5
  - Data movement service
    ‣ Globus.org
Grid Architecture

http://www.gridcafe.org
It’s about Grid computing

- Resource sharing
  - Distributed computing
  - Computing sites

- Secure access
  - Trust between resource providers and users
Grid Computing at LRZ

- LRZ provides resources via Globus, UNICORE, gLite

- D-GRID
  - LRZ is centre of excellence for Globus in D-Grid

- DEISA and PRACE
  - LRZ coordinates Globus related activities

- EGI
  - Start support for Globus in EGI–InSpire
IGE (Initiative for Globus Europe)

- Coordination of European Globus activities
- Introduce adjustments critical for Europe into Globus code base
- Act as Globus service provider for European Grids like DEISA, PRACE, and EGI
- Measure Globus software quality
- Training, promotion, and documentation
- Organize Globus Europe conference and Globus community forum
- Bundle European input to Globus
Globus Overview

• Globus Alliance
  - International community to drive the development of Globus

• Globus Toolkit
  - Set of tools for building Grid systems and applications
  - Open source
  - Developed worldwide
Authentication and Authorisation

- Public Key Cryptography and Infrastructure (PKI)
- User and CA Certificates
- Grid Security Infrastructure (GSI)
- Proxy Certificates
- MyProxy Service
- Short lived credential service
Authentication and Authorisation (AA)

• **Authentication is the process to**
  - Verifying that s.b./s.th. is who he claims to be
  - Identify a user or a resource

• **Authorisation is the process to**
  - Give permission to perform certain operations or access specific resources
Public Key Cryptography

- **Private Key**: File - only the owner may know the content
- **Public Key**: File - one can/have to give it to other people

  - **Sender** uses his **Private Key** to **sign** his message. Then the receiver can **verify** if the message was created by the sender and not **tampered** with the sender’s public key.

  - **Sender** uses recipient’s **Public Key** to **encrypt** the message. Then the message is only **decryptable** with the recipient’s corresponding **Private Key**.
Grid Security Infrastructure (GSI)

- Based on Public Key Infrastructure (PKI)
- Allows to identify a person to be authorized by a resource provider without previous communication
- Certificate Authority (CA)
  - Trusted 3rd party that confirms identity and issues certificate
  - Using a CA means you trust that this CA verified person/host after common rules

---

The International Grid Trust Federation - IGTF

- EUGridPMA
  - UK CA
  - DutchGrid CA
- APGridPMA
  - Japan CA
- TAGPMA
  - USA CA
- TACAR
  - TERENA Academy CA Repository

---

users
Certificates

- **Certificates - Central concept in GSI**
  - Distinguished Name - unique Grid id for user/service
    ‣ Example: "/C=DE/O=GridGermany/OU=Leibniz/CN=Your Name"

- **Certificate proves who you are - security!**
  - Keep your user certificate in a private directory
  - Revoke your certificate immediately if there are indications that your certificate is compromised

- **Authentication**
  - Both sides must have CA certificates that they trust
  - Certificate is used to authorise user and resource provider against each other
Certificate Formats

- **PEM-format:**
  - Separate files for certificate and private key (.pem)
  - Used by Globus toolkit (gsissh, gridftp, ...)

- **PKCS12 (Certificate Container):**
  - Can include private key, certificate and/or CA certificate
  - Used by web browsers, also by Globus
  - Transformations are possible, e.g. via openssl
Grid-mapfile

• Authorisation in GSI via grid-mapfile

• Mapping of global DN to a local system account

• Format: Textfile ("DN" local Account)
  Example entry:
  › "/C=DE/O=GridGermany/OU=Leibniz/CN=Your Name" lrz28230

• All GSI-Services use grid-mapfile
• Resource can delegate a proxy for its access to further resources (Delegation)
Proxy Certificates

- **Proxy Certificates**
  - Backbone of trust delegation
  - **Security gain:**
    ‣ No password has to be transmitted
    ‣ Limited life time of the proxy certificate
    ‣ Limited capability
  - **Generated from user certificate key pair**
    ‣ Signed with your normal private key

- **Proxy certificate consists of**
  ‣ User normal public certificate
  ‣ Newly generated proxy private key – without password

- **Single sign-on: Login only once**
  - Only type your password once (for your private key)

- **Used by Globus services**
MyProxy - Credential Repository
Short Lived Credential Service (SLCS) (1)
Short Lived Credential Service (SLCS) (2)

- Alternative for long-lived certificate
  - Without visiting a RA
- Institutes/companies already checked your id
- User is authenticated by **home institute** via web browser with username and password and gets a short-lived certificate
  - Only valid for a short period of time (e.g. one week)
  - Proxy certificate
Globus Toolkit

- GSI
  - The backbone
- GSI-ssh
  - Secure access
- VOMS
  - VO membership service
- OGSA-DAI
  - Data integration
- GridFTP
  - Super fast data transfer
- GRAM
  - Job submission framework
What’s new in GT5?

- **Job submission is now GRAM5**
  - Compatible with Globus v. 2.x. NOT with v. 4.x Web Services GRAM

- **There is no Web Services interface (Java container) any more**
  - Crux toolkit will be released later to overcome this issue
    Keywords: "service oriented"

- **No MDS information system anymore**
  - Integrated Information Services (IIS) to replace in the future

- **New GridFTP features**
  - Resumeable file transfer
  - Compatible with older versions.
    No Reliable File Transfer (rft) anymore

- **GSI-SSH and MyProxy are compatible with older versions**
Interactive Access Overview

- GSI-OpenSSH
- Clients
- Login to a remote site
GSI-Enabled OpenSSH Server

- GSI-OpenSSH is a modified version of OpenSSH
- Added support for GSI authentication and credential forwarding (delegation)
- Provides a single sign-on remote login
Setup the GSI-Enabled OpenSSH Server

- Acquire a host certificate for the GSI-SSHD host.
- Authorise users you want to be able to connect with GSI SSH
  - grid-mapfile
- Configure and run the GSI-SSH daemon
  - Optional: Allowing only GSI authentication
## GSI-Enabled OpenSSH Clients

<table>
<thead>
<tr>
<th>gsissh</th>
<th>gsissh-term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native shell tool</td>
<td>Java (+ Java-Webstart)</td>
</tr>
<tr>
<td>Needs to install (a subset of) GT</td>
<td>Easy installation – cross platforms</td>
</tr>
<tr>
<td>As your user interface</td>
<td>Java look and feel</td>
</tr>
</tbody>
</table>
Client: GSI-Enabled OpenSSH Client

- Creating proxy credentials: grid-proxy-init
- Information about your created proxy: grid-proxy-info
- Login: gsissh host
- Delete your proxy: grid-proxy-destroy
  ‣ highly recommended – for security reason!
Client: GSISSH-Term

- GSISSH-Term login to HLRB-II (operated at LRZ):

Welcome to the HLRB-II Phase 2 system hlrb2
- 9728 Itanium2 cores, 62.3 TFlop/s -
operated by
*** Leibniz Supercomputing Centre in Munich ***

Please read the introductory documentation at
http://www.lrz.de/services/compute/hlrb
In case of problems please submit a trouble ticket via
http://www.lrz.de/services/compute/hlrb/troubleticket

Please do not run or test jobs in the login partition directly, since the 32
cores available there are shared with all other users. Instead, reserve some
CPUs exclusively for your interactive work by using "qsub -I". Please refer
to the section "Interactive PBS Shells" in the web documentation at
http://www.lrz-muenchen.de/services/compute/hlrb/batch

pr28te's budget [cpuh]: total:20000 used:13318 (66%) credit:6682 (34%)
Current filesystem quota for your project:
Filesystem Size Avail (GB)
nas10.hlrb2.lrz-muenchen.de:home/deisa/lrz/lrz00001/1 429 16
lrz024cl@a01:~  
Data transfer with GridFTP Overview

- What is GridFTP?
- Third Party Transfers
- Performance Options
- Clients
  - GSISSH-TERM
  - globus-url-copy
What is GridFTP?

- High-performance, reliable data transfer protocol optimized for high-bandwidth wide area networks

- Based on FTP protocol - defines extensions for high-performance operation and security
  - Authenticate control and data channels with GSI

- Standardized through Open Grid Forum (OGF)

- GridFTP is the OGF recommended data movement protocol
Understanding GridFTP

- Two channel protocol like FTP

- Control Channel
  - Command/Response
  - Used to establish data channels
  - Basic file system operations eg. mkdir, delete etc

- Data channel
  - Pathway where file is transferred
GridFTP’s Third Party Transfers

- **Two party transfer**
  - The client connects to the server
  - Information is exchanged to establish the DC
  - A file is transferred over the DC

- **Third party transfer**
  - Client initiates data transfer between 2 servers
  - Information is routed through the client to establish DC between the two servers.
  - Data flows directly between servers
  - Client is notified by each server when the transfer is complete
GridFTP Performance Options

- Adjustable buffer size of data channels (-tcp-bs)
- Parallel TCP streams (-p)

- Striped GridFTP
  - Multiple network endpoints for the transfer of the same file
Globus-url-copy

- Command line client
  - scriptable
- Commonly used client for GridFTP
- Syntax overview
  - `globus-url-copy [options] sourceURL destinationURL`
  - `globus-url-copy gsiftp://host/foo file:///tmp/bar`
- URL
  - `protocol://[user@][host]/path`
  - [host] can be IP address, localhost, DNS name
File transfer with GSISSH-Term
Job Submission Overview

- Grid job management
- GRAM introduction
- Job execution management
Grid Job Management Goals

• Grid Middleware provides common interface for different Local Resource Management Systems (LRMS)

• Functionality
  - Certificate based A&A
  - Stage files to/from resource
  - Initiate execution of job process(es)
  - Monitor execution
  - Signal important state changes to client
GRAM On Local Site

- Provides LRM abstraction

**Diagram:**

- GRAM Jobs
  - Local Jobs
  - GRAM API
  - GRAM Service
    - LRM (e.g. PBS)
    - Compute Nodes
  - GRAM Service
    - LRM (e.g. SGE)
    - Compute Nodes

**Resource A**

**Resource B**
Job Execution Management

• **Globus Resource Allocation Manager (GRAM5)**
  - GRAM is a Globus Toolkit component for grid job submission
  - Interfaces to many batch systems:
    ‣ PBS/Torque, LSF, SGE

• **GRAM is a unifying remote interface to Resource Managers**

• **GRAM provides stateful job control**
  - Asynchronous monitoring and control
  - Remote credential management
  - Remote file staging and file cleanup
User submits a Globus job using
- Globus commands
- and optionally a job script (in Resource Specification Language (RSL))

Globus will
- Translate your job script for the specific LRMS
- Use native LRMS commands to submit the job

User can monitor the job state
- Globus will check the job state using LRMS log file

User can cancel the job:
- Globus will call LRMS cancellation command
GRAM5 Components

- **Gatekeeper**
  - Authentication
  - Starts job management service (on request)

- **Job Manager**
  - Processes job requests and coordinates file transfer
  - One process per user per LRSM

- **Job Manager Script (RM adapter submit)**
  - Interacts with LRMS and does the file transfer

---

Diagram:

1. **Client** → **Gatekeeper**
2. **Gatekeeper** → **Job Manager**
3. **Job Manager** → **Resource Manager**
   - **RM adapter submit**
4. **Resource Manager** → **User Job(s)**
GRAM Client Interfaces

- Globus’s (job related) command line commands:
  - `globus-job-submit`
  - `globus-job-status`
  - `globus-job-get-output`
  - `globus-job-clean`

- Application Programming Interface (API) for C and JAVA
Globus.org Overview

- Data movement service
- Usage with gsissh
- Globus.org webservice
Globus.org Service

• Globus.org manages third party transfers
Globus.org Service

• Every user gets its private resource (Amazon EC2 instance)

• Access via gsissh
  - On login you don’t get a shell but
  - Text interface

• Functions
  - Manage end-points
  - Delegate your proxy
    ‣ Direct via gsi-ssh
    ‣ Indirect via myproxy
  - Initiate, observe, stop your transfers
  - Notifications

• API
  - REST interface
Anatomy Of Globus.org CLI Call

- **gsissh** -p 2222 -o "GSSAPITrustDNS no" user@host command

Example:
- Delegate/Refresh Your Credential to an endpoint with MyProxy:
  - gsissh -t lcc@cli.globus.org
    activate -m myproxy.lrz.de lrzhome
  - **Enter MyProxy pass phrase**
  - **Credentials are delegated for the endpoint**
    and can be used to transfer to/from this endpoint

- **ssh** -t <user>@<machine> <command> <options> <params>

**Override DNS checks because the host certs do not currently match the Amazon IPs (will not be required in future releases)**

**GSI-OpenSSH server port**
Globus.org Webservice

• Functionality of globus.org service in the web browser
  - Graphical user interface
  - Access from every computer
  - Easy to use – you don’t need globus toolkit

• Mock-up Live Demo
Globus.org Webservice
Where To Find Help

• http://www.ige-project.eu/

• LRZ globus contact: grid-support@lrz.de

• http://www.grid.lrz.de/