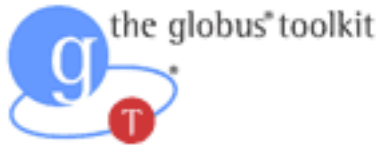
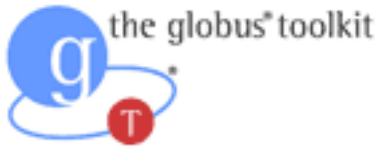
Grid Roll: Users Guide



Version 4.1 Edition



Grid Roll: Users Guide :
Version 4.1 Edition
Published Nov 2005

Table of Contents

Preface

The Rocks Grid Roll is based on Globus 4.0.1 (GT4). This release includes ANT which is required to build Globus, and is configured to support all bundled webservice GRAMS, and the non-webservice GRAM. Globus was compiled using the configure, make, install procedure and no patches have been added.

Chapter 1. Requirements

1.1. Rocks Version

The Grid Roll is for use with Rocks version 4.1 (Fuji).

1.2. Other Rolls

The Grid Roll is does not require any other Rolls (other than the HPC Roll) to be installed on the Frontend. Compatiblity has been verified with the following Rolls.

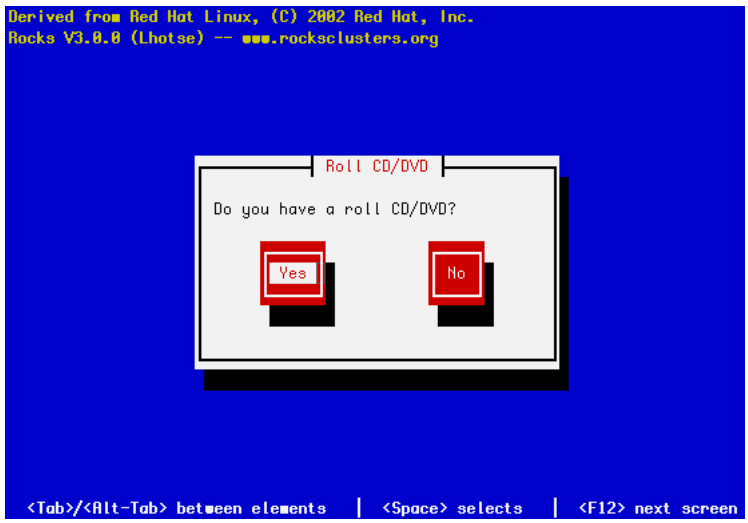
- HPC
- Patch

Chapter 2. Installing the Grid Roll

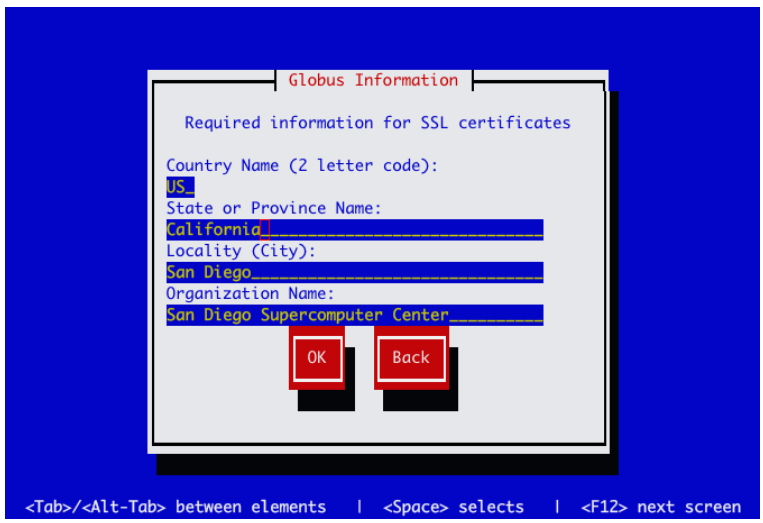
2.1. Adding the Roll

The Grid Roll must be installed during the Frontend installation step of your cluster (refer to section 1.2 of the Rocks usersguide). Future releases will allow the installation of the Grid Roll onto a running system.

The Grid Roll is added to a Frontend installation in exactly the same manner as the required HPC Roll. Specifically, after the HPC Roll is added the installer will once again ask if you have a Roll (see below). Select 'Yes' and insert the Grid Roll.

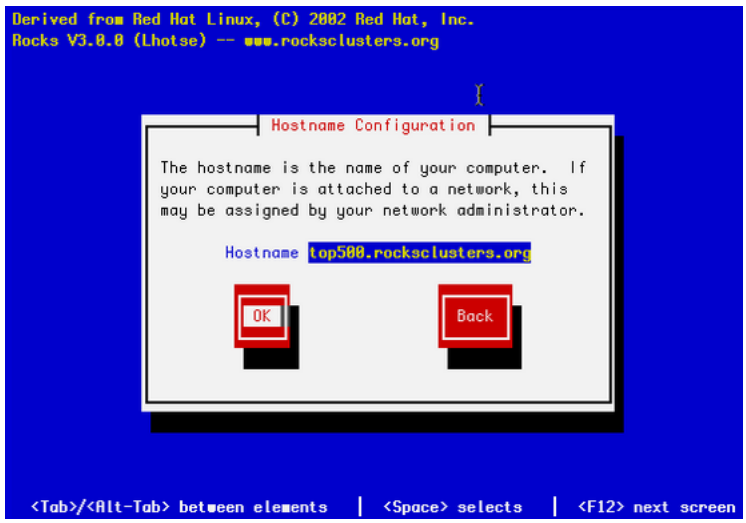


Once the Grid Roll is loaded the installer will continue to prompt for the standard Rocks configuration screens. The Grid Roll adds the following configuration screen to provide information to the Globus Certificate Authority. This information is used to build the Distinguished Name (DN) of you host, and user certificates.



You must use a Fully Qualified Domain Name (FQDN) for your Frontend.

Globus and its openssl-based PKI tools require the hostname of you cluster Frontend to be the primary DNS fully-qualified domain name. You may not name use DNS aliases, or an abbreviated hostname. This is because all certificate checks do a reverse DNS lookup and must resolve to the correct distinguished name (DN) used to build the certificate. To insure you configure your Frontend correctly when you are presented with the hostname configuration screen (see below), be sure to enter the FQDN of your host.



2.2. Root Login

The Grid Roll installs the Globus Simple Certificate Authority (CA), to allow you to generate, and manage certificates. The first time you log into the Frontend as root you will be prompted for the passphrase for your newly installed CA. This passphrase should be secure, and different from your root account password.

```
Enter CA passphrase:
Enter CA passphrase (again):
Installing Globus CA (takes a few minutes)
Done.
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
Stopping MDS                                               [  OK  ]
Starting MDS                                               [  OK  ]
```

You must configure the Simple CA, even if you wish to use an different CA system. After providing a passphrase, you may modify your Globus configuration to use your preferred CA system. The Simple CA is

provided as a starting point, for users to setup there own grid testbeds quickly as possible. Production grids may require a different CA configuration.

2.3. Globus Usage Statistics

The Globus Team has a policy[1] of collecting usage statistics from all installations of Globus. The version of Globus on this roll is configured by default to opt-in for this reporting from your system. If you wish to opt-out of this you must reconfigure the firewall rules on your frontend. Edit the file **`/etc/sysconfig/iptable`** and a new **`DROP`** in the following section of the file.

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
# Preamble
-A FORWARD -i eth1 -o eth0 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -j ACCEPT
-A INPUT -i eth0 -j ACCEPT
-A INPUT -i lo -j ACCEPT

# Disable Globus Usage Statistics Reporting from this host
-A OUTPUT -d usage-stats.globus.org -j DROP
```

Notes

1. http://www-unix.globus.org/toolkit/docs/4.0/Usage_Stats.html

Chapter 3. Using the Grid Roll

3.1. Managing Certificates

This section discusses how to use the Globus Simple CA, and Rocks software to manage user certificates. If you plan to use a different CA system please refer to the documentation for that CA.

Creating a Globus User Certificate, regardless of the CA system, involves the following steps:

1. User creates a certificate request.
2. Certificate Request is sent to the CA system. The Grid Roll skips this step, and the root account directly reads the Certificate Request out of the user's home directories.
3. The CA system creates a Globus User Certificate and returns it to the user.

The advantage of using the Simple CA (and the Rocks Grid Roll) to provide CA services is that these steps can be completed in minutes, rather than the standard practice of waiting hours to days for a certificate.

3.1.1. Requesting a Certificate

Users may request certificates using the Globus command **grid-cert-request**. In the following sample output a certificate request is generated for the user with a Common Name (CN) of "Spaceman Spiff". The rest of the DN is picked up from the configuration of the CA, which was done at installation time.

Although the **grid-cert-request** command instructs that you email you certificate request this step is not necessary when using the Grid Roll.

```
$ grid-cert-request
Enter your name, e.g., John Smith: Spaceman Spiff
A certificate request and private key is being created.
You will be asked to enter a PEM pass phrase.
This pass phrase is akin to your account password,
and is used to protect your key file.
If you forget your pass phrase, you will need to
obtain a new certificate.

Using configuration from /etc/grid-security/globus-user-ssl.conf
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to '/home/gridboy/.globus/userkey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```

```
-----
you are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Level 0 Organization [Grid]:Level 0 Organizational Unit [San Diego Supercomputer Center]:Level 1 Org

A private key and a certificate request has been generated with the subject:

/O=Grid/OU=San Diego Supercomputer Center/OU=rocks12.sdsc.edu/OU=sdsc.edu/CN=Spaceman Spiff

If the CN=Spaceman Spiff is not appropriate, rerun this
script with the -force -cn "Common Name" options.

Your private key is stored in /home/gridboy/.globus/userkey.pem
Your request is stored in /home/gridboy/.globus/usercert_request.pem

Please e-mail the request to the Globus Simple CA root
You may use a command similar to the following:

cat /home/gridboy/.globus/usercert_request.pem | mail root

Only use the above if this machine can send AND receive e-mail. if not, please
mail using some other method.

Your certificate will be mailed to you within two working days.
If you receive no response, contact Globus Simple CA at root
```

3.1.2. Creating User Certificates

Only the root account is permitted to issue user certificates using the locally installed Simple CA. After one, or more, users have run **grid-cert-request**, the root use must log in and run **local-ca-sign**. In the following example, a certificate request is found, a certificate issued, and the grid-mapfile populated with an entry for the user.

```
# local-ca-sign
Enter CA passphrase:

Enter password for the CA key:

The new signed certificate is at: /root/.globus/simpleCA//newcerts/03.pem

/etc/grid-security/grid-mapfile does not exist... Attempting to create /etc/grid-security/grid-mapfi
(1) entry added
```

3.2. Using Certificates

You can verify Globus is correctly installed by running a few simple Globus commands from your Frontend. Although this is only a simple loopback-grid this will verify the installation. The following will run grid-hostname over loopback on your Frontend node.

1. Create a proxy certificate.

```
$ grid-proxy-init
Your identity: /O=Grid/OU=San Diego Supercomputer Center/OU=rocks12.sdsc.edu/OU=sdsc.edu/CN=Space
Enter GRID pass phrase for this identity:
Creating proxy ............................................ Done
Your proxy is valid until: Tue Sep  9 10:53:51 2003
```

2. Run hostname over Globus

```
$ globus-job-run localhost /bin/hostname
rocks12.sdsc.edu
```

To start building a grid you will need to exchange certificate and grid-mapfile information with other hosts and users. Please visit the Globus site documentation[1] to learn how to do this.

3.3. Testing the Grid Roll

1. Login to the frontend as a non-root user and create a certificate for that user by executing:

```
$ grid-cert-request
```

2. Now you'll sign the certificate. Logout as the user and login back in as root and execute:

```
# local-ca-sign
```

3. Now you'll need to log back in as a non-root user in order to run the following test job:

```
$ grid-proxy-init
$ globus-job-run localhost /bin/hostname
```

   This should output the hostname for the frontend.

   If you installed the SGE roll, then you can test the SGE/Grid roll integration by using Globus to submit an interactive job to SGE:

```
$ globus-job-run localhost/jobmanager-sge /bin/hostname
```

   This should return the name of one of the compute nodes.

Notes

1. http://www-unix.globus.org/toolkit/documentation.html