Grid User Management Service
GUMS
Tutorial

Carlos Fernando Gamboa

Brookhaven National Laboratory

Grid Colombia 2010, Bucaramaga, Colombia March 1-5 2010.

Tutorial Goal

With the aim of introducing system administrators to GUMS software the following presentation was intended to demonstrate it's installation procedure.

Introduction

What is GUMS?

It is a Grid Identity Mapping Service.

Maps a GRID credential to a Site's UNIX account.

GUMS service mapping is composed by web services, web Pages for GUMS administration, and command-line tools Which interact with the web services.

GUMS service is **transparently** provided to users.

GUMS installation overview

GUMS installation consists off:

1. Obtaining GRID service credentials and GUMS software

A package management tool PACMAN is used to:

Obtain/install GUMS software

https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/PacmanInstall

Requesting/retrieving/installing the host and service (HTTP) certificates.

https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GetGridCertificates

2. Deployment and Configuration of the GUMS software

Specific instructions for this tutorial can be found at:

https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GridColombiaInstallGUMS

GUMS installation overview (cont.)

3. Post-configuration GUMS

- Create a GUMS administrator
- Replace default configuration with OSG configuration
- Test configuration

4. Site Customization

- Depending on the Site policy for internal account management

General information about this demo

Pre-requisites:

- **Operative System:** Red Hat Enterprise Linux Client release 5.4
- **HOSTNAME :** grid07.racf.bnl.gov
- **Host Certificates** (hostcert.pem, hostkey.pem)

  located under /etc/grid-security/

  Service Certificates (httpcert.pem,httpkey.pem)

  located under /etc/grid-security/http/, the files should be owned by daemon and belong to the daemon group

  (chown -R daemon:daemon http)

Note: If **PRIMA** will be used please follow the instructions to setup the service certificates at the end of the documentation see,

https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/InstallConfigureAndManageGUMS

1. Installing GUMS software:

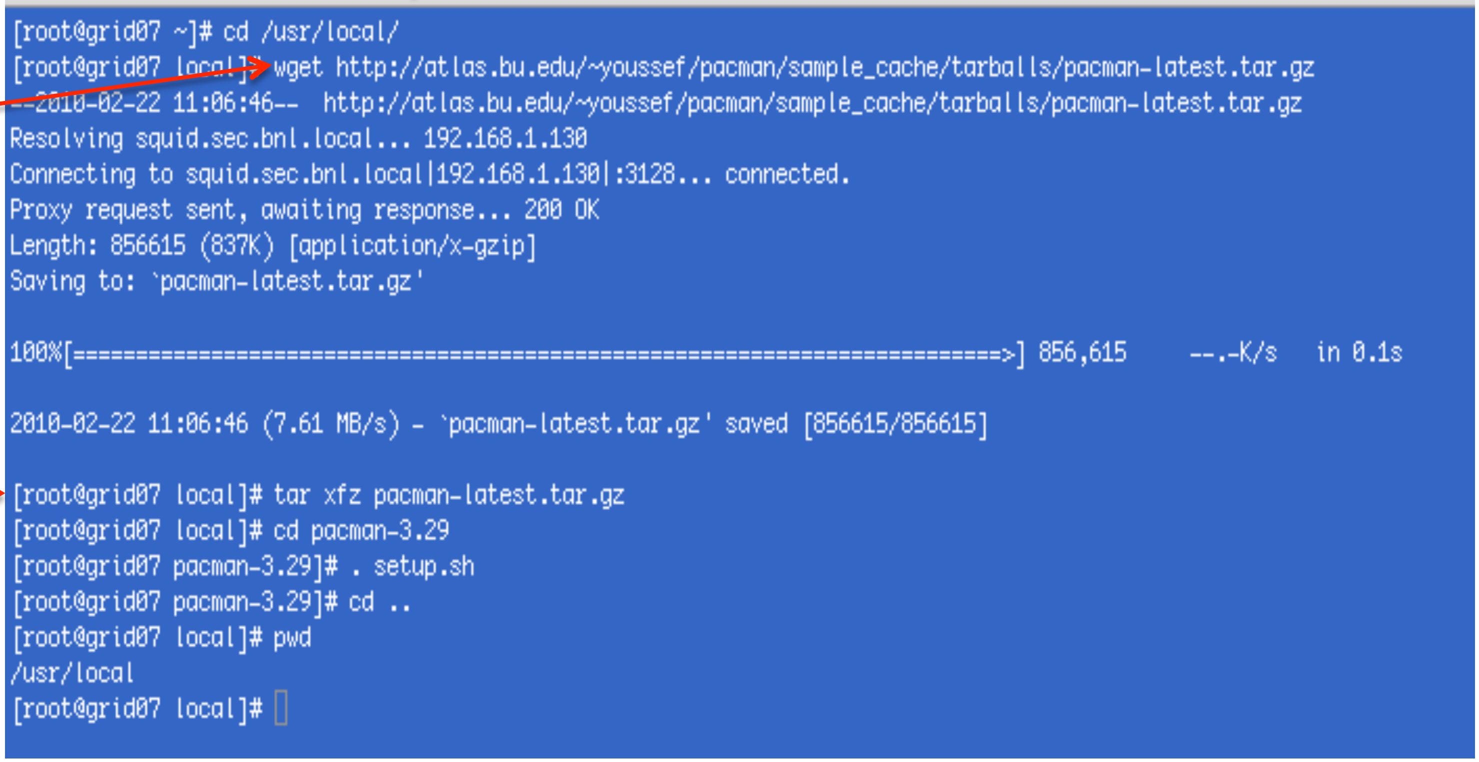
Installing PACMAN https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/PacmanInstall

Choosing a location different that the OSG software packages

Downloading the software

Uncompressing the software recently

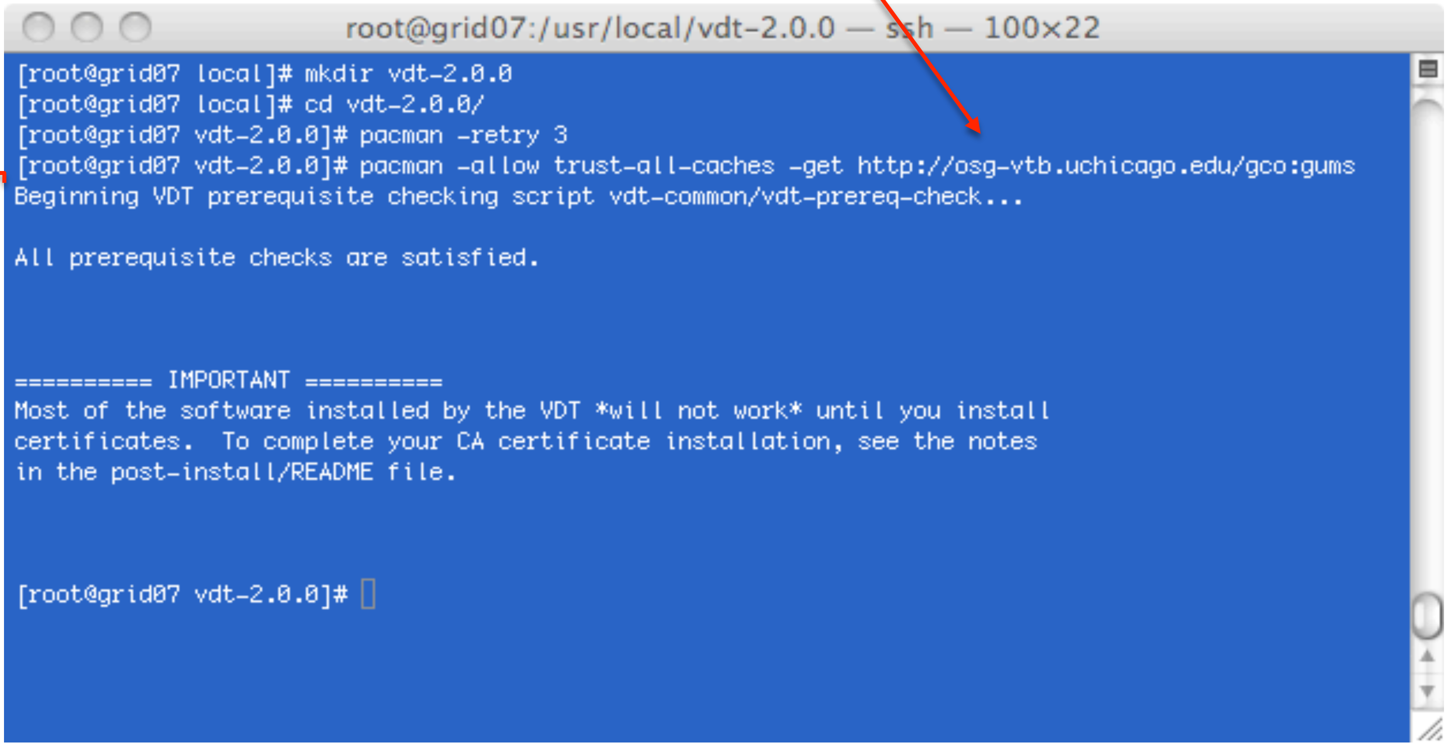
Setting up the Environment for PACMAN



```
[root@grid07 ~]# cd /usr/local/
[root@grid07 local]# wget http://atlas.bu.edu/~youssef/pacman/sample_cache/tarballs/pacman-latest.tar.gz
--2010-02-22 11:06:46--  http://atlas.bu.edu/~youssef/pacman/sample_cache/tarballs/pacman-latest.tar.gz
Resolving squid.sec.bnl.local... 192.168.1.130
Connecting to squid.sec.bnl.local|192.168.1.130|:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 856615 (837K) [application/x-gzip]
Saving to: `pacman-latest.tar.gz'

100%[=========================================================================>] 856,615     --.-K/s   in 0.1s

2010-02-22 11:06:46 (7.61 MB/s) - `pacman-latest.tar.gz' saved [856615/856615]

[root@grid07 local]# tar xfz pacman-latest.tar.gz
[root@grid07 local]# cd pacman-3.29
[root@grid07 pacman-3.29]# . setup.sh
[root@grid07 pacman-3.29]# cd ..
[root@grid07 local]# pwd
/usr/local
[root@grid07 local]# 
```

Obtain/install GUMS software

Software repository location



```
[root@grid07 local]# mkdir vdt-2.0.0
[root@grid07 local]# cd vdt-2.0.0/
[root@grid07 vdt-2.0.0]# pacman -retry 3
[root@grid07 vdt-2.0.0]# pacman -allow trust-all-caches -get http://osg-vtb.uchicago.edu/gco:gums
Beginning VDT prerequisite checking script vdt-common/vdt-prereq-check...

All prerequisite checks are satisfied.



========== IMPORTANT ==========
Most of the software installed by the VDT *will not work* until you install
certificates.  To complete your CA certificate installation, see the notes
in the post-install/README file.



[root@grid07 vdt-2.0.0]#
```

Use the following systanx if you want to use your local squid cache

pacman -allow trust-all-caches **-http-proxy** http://192.168.109.130:3128 -get http://osg-vtb.uchicago.edu/gco:gums

2. Deployment and Configuration of the GUMS software

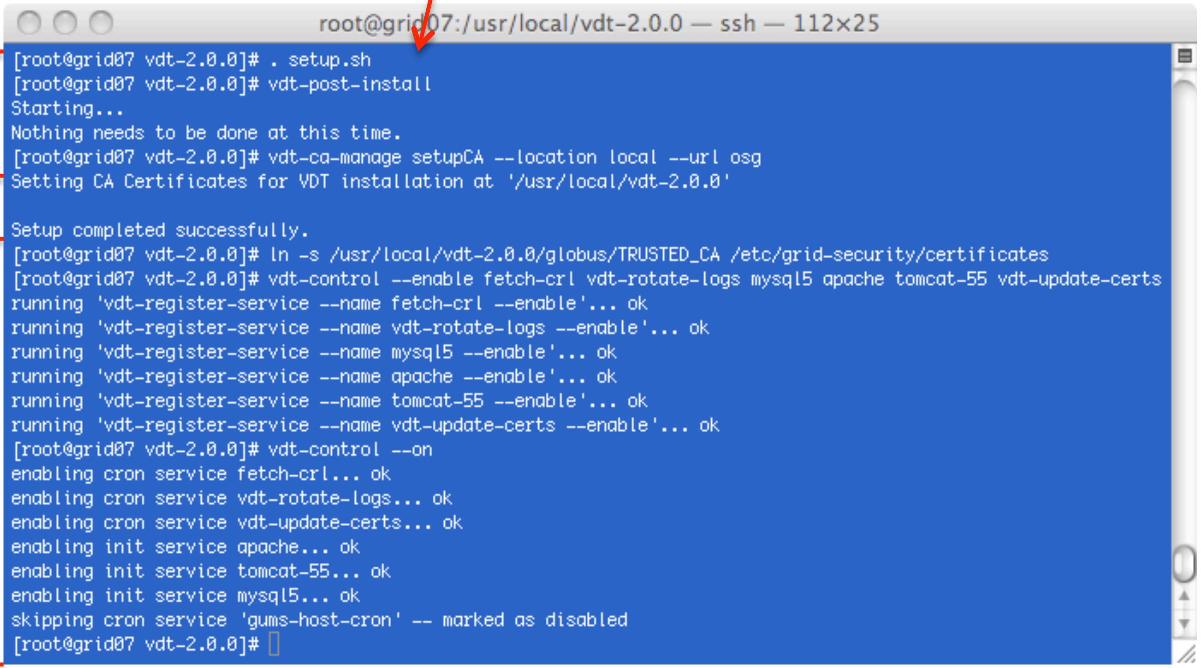
This installs both the GUMS server and the GUMS client.

certificate authority
certificates
installation

Enabling services and starting

Service vdt-update-certs : insures that future certificate updates are fetched automatically.

Service fetch-crl : Cron service that retrieves the latest certificate revocation lists (CRLs) for each CA.

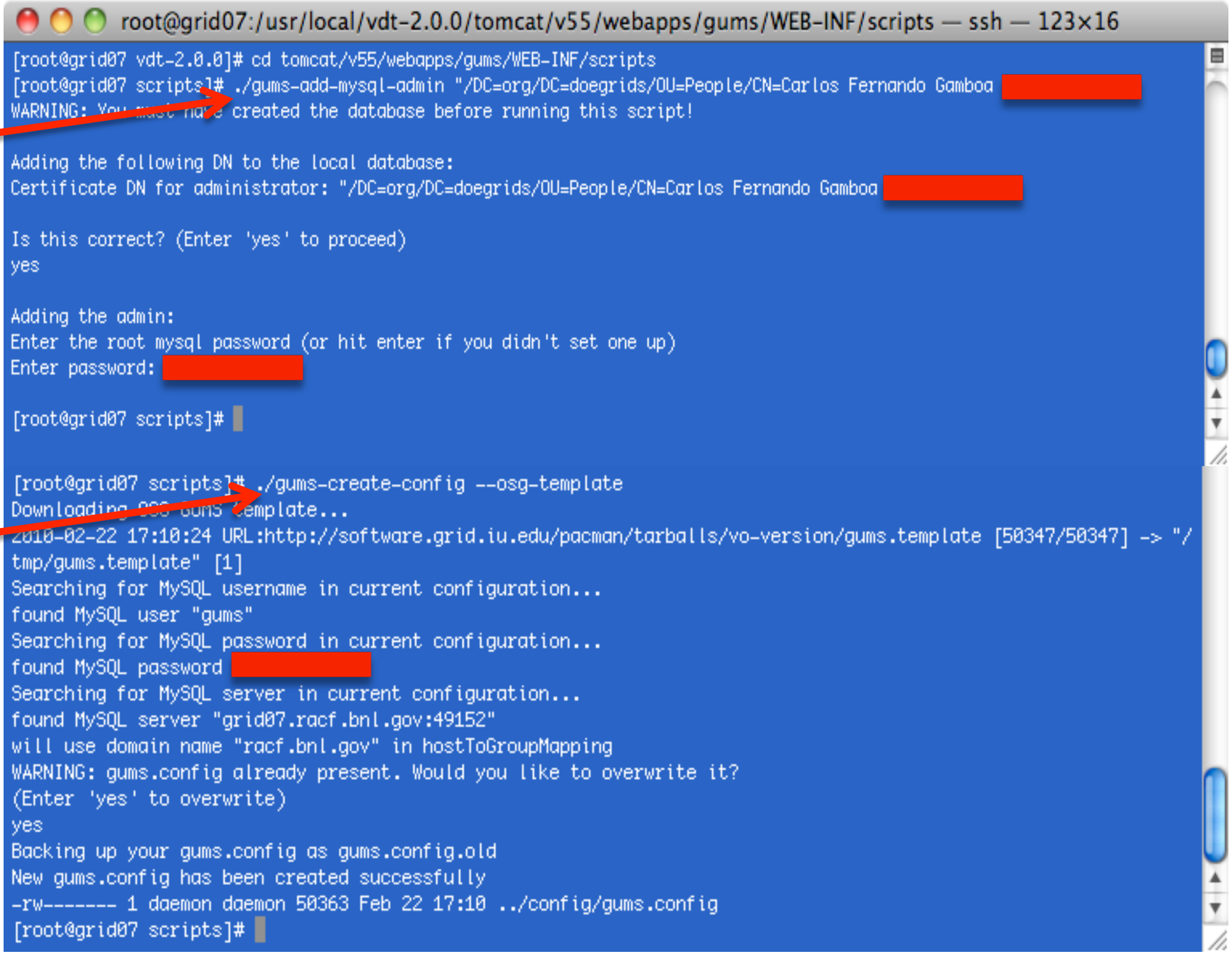


```
[root@grid07 vdt-2.0.0]# . setup.sh
[root@grid07 vdt-2.0.0]# vdt-post-install
Starting...
Nothing needs to be done at this time.
[root@grid07 vdt-2.0.0]# vdt-ca-manage setupCA --location local --url osg
Setting CA Certificates for VDT installation at '/usr/local/vdt-2.0.0'

Setup completed successfully.
[root@grid07 vdt-2.0.0]# ln -s /usr/local/vdt-2.0.0/globus/TRUSTED_CA /etc/grid-security/certificates
[root@grid07 vdt-2.0.0]# vdt-control --enable fetch-crl vdt-rotate-logs mysql5 apache tomcat-55 vdt-update-certs
running 'vdt-register-service --name fetch-crl --enable'... ok
running 'vdt-register-service --name vdt-rotate-logs --enable'... ok
running 'vdt-register-service --name mysql5 --enable'... ok
running 'vdt-register-service --name apache --enable'... ok
running 'vdt-register-service --name tomcat-55 --enable'... ok
running 'vdt-register-service --name vdt-update-certs --enable'... ok
[root@grid07 vdt-2.0.0]# vdt-control --on
enabling cron service fetch-crl... ok
enabling cron service vdt-rotate-logs... ok
enabling cron service vdt-update-certs... ok
enabling init service apache... ok
enabling init service tomcat-55... ok
enabling init service mysql5... ok
skipping cron service 'gums-host-cron' -- marked as disabled
[root@grid07 vdt-2.0.0]# 
```

3. Post-configuration GUMS

Setting up the DN of the GUMS administrator

Replacing the current gums.config file with the OSG template while preserving original database configuration


root@grid07:/usr/local/vdt-2.0.0/tomcat/v55/webapps/gums/WEB-INF/scripts — ssh — 123×16

```
[root@grid07 vdt-2.0.0]# cd tomcat/v55/webapps/gums/WEB-INF/scripts
[root@grid07 scripts]# ./gums-add-mysql-admin "/DC=org/DC=doegrids/OU=People/CN=Carlos Fernando Gamboa [redacted]
WARNING: You must have created the database before running this script!

Adding the following DN to the local database:
Certificate DN for administrator: "/DC=org/DC=doegrids/OU=People/CN=Carlos Fernando Gamboa [redacted]

Is this correct? (Enter 'yes' to proceed)
yes

Adding the admin:
Enter the root mysql password (or hit enter if you didn't set one up)
Enter password: [redacted]

[root@grid07 scripts]#
```

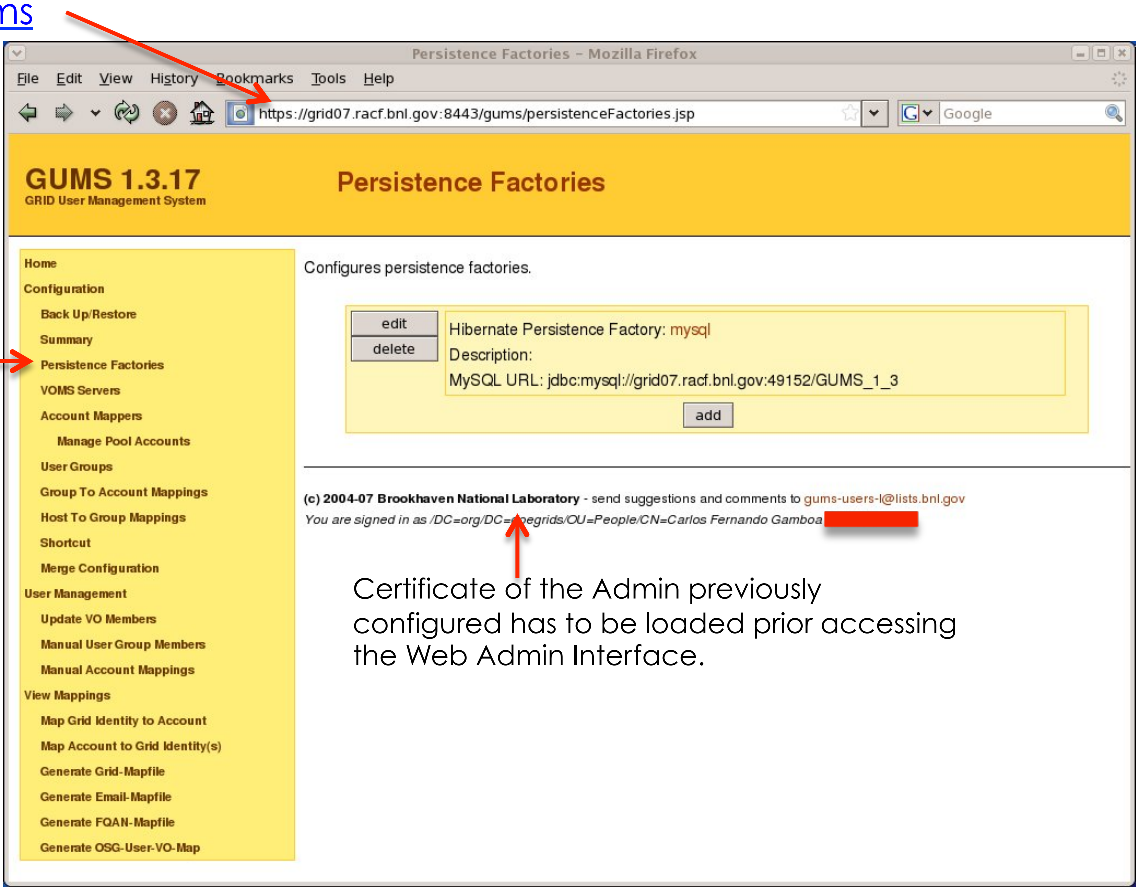
```
[root@grid07 scripts]# ./gums-create-config --osg-template
Downloading OSG GUMS template...
2010-02-22 17:10:24 URL:http://software.grid.iu.edu/pacman/tarballs/vo-version/gums.template [50347/50347] -> "/
tmp/gums.template" [1]
Searching for MySQL username in current configuration...
found MySQL user "gums"
Searching for MySQL password in current configuration...
found MySQL password [redacted]
Searching for MySQL server in current configuration...
found MySQL server "grid07.racf.bnl.gov:49152"
will use domain name "racf.bnl.gov" in hostToGroupMapping
WARNING: gums.config already present. Would you like to overwrite it?
(Enter 'yes' to overwrite)
yes
Backing up your gums.config as gums.config.old
New gums.config has been created successfully
-rw------- 1 daemon daemon 50363 Feb 22 17:10 ../config/gums.config
[root@grid07 scripts]#
```

3. Post-configuration GUMS

Test configuration

At this point the GUMS service is up and can be administrated through:
https://grid07.racf.bnl.gov:8443/gums

This plot showed the result of selecting the link **Persistence Factory**



Configures persistence factories.

Hibernate Persistence Factory: mysql
Description:
MySQL URL: jdbc:mysql://grid07.racf.bnl.gov:49152/GUMS_1_3

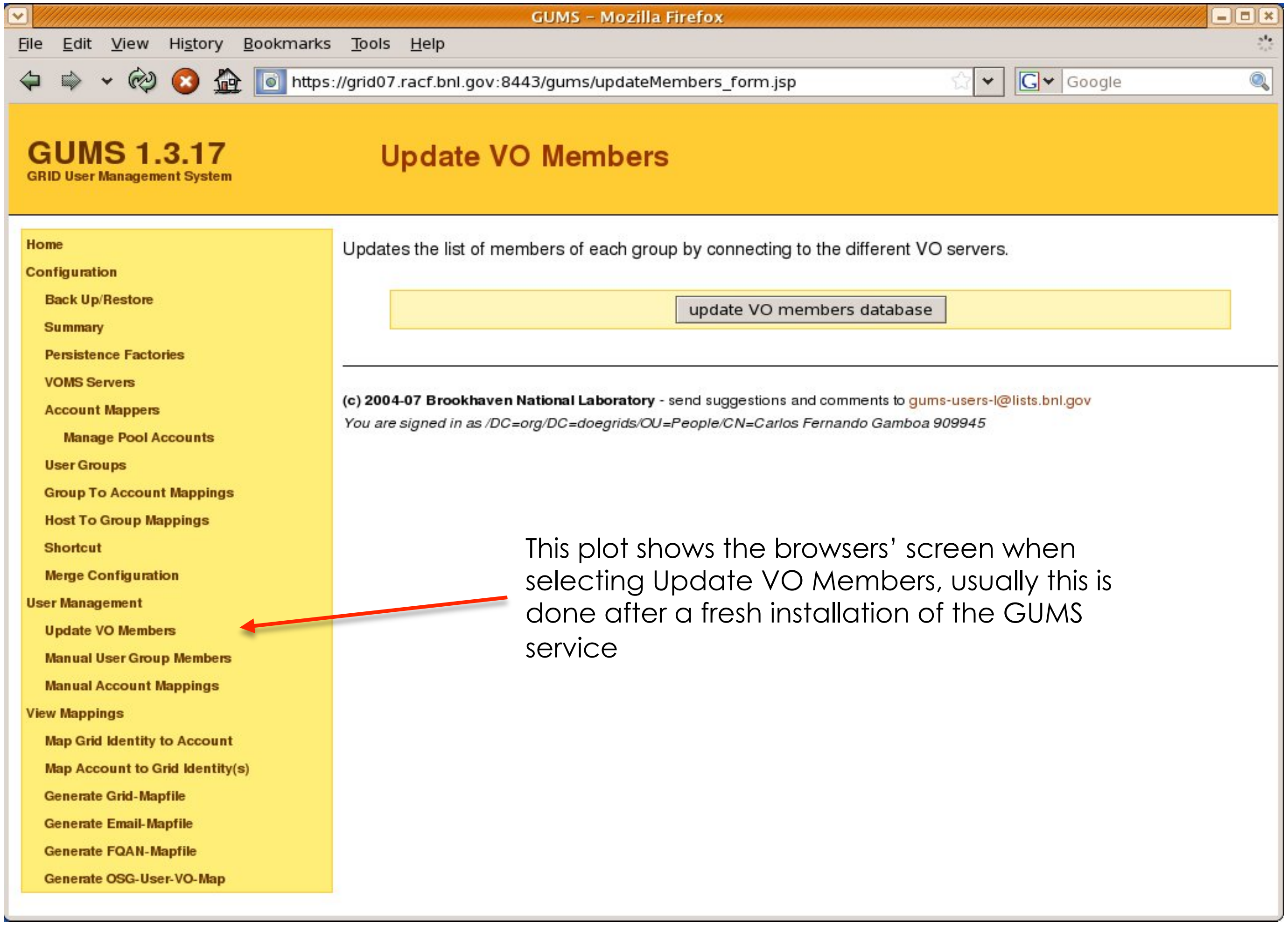
(c) 2004-07 Brookhaven National Laboratory - send suggestions and comments to gums-users-l@lists.bnl.gov

You are signed in as /DC=org/DC=doegrids/OU=People/CN=Carlos Fernando Gamboa [redacted]

Certificate of the Admin previously configured has to be loaded prior accessing the Web Admin Interface.

3. Post-configuration GUMS

Updating Virtual Organization Members



Updates the list of members of each group by connecting to the different VO servers.

(c) 2004-07 Brookhaven National Laboratory - send suggestions and comments to gums-users-l@lists.bnl.gov

You are signed in as /DC=org/DC=doegrids/OU=People/CN=Carlos Fernando Gamboa 909945

Configure the elements involved in mapping a user to an account

Add individual users to user groups and account mappers, or force an member update for each user group

View mappings to see if the output of GUMS mappings is as expected.

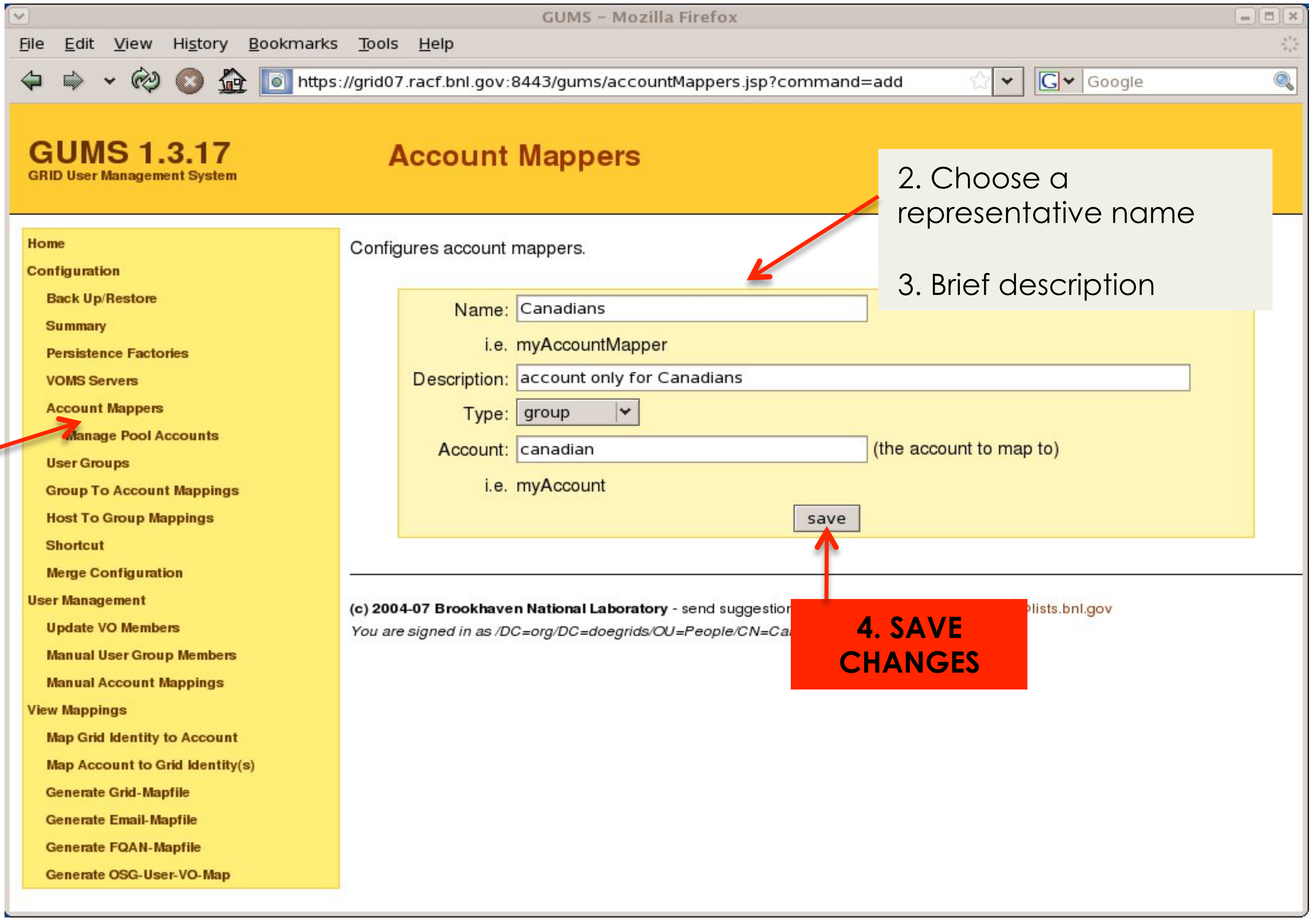
This plot shows the browsers' screen when selecting Update VO Members, usually this is done after a fresh installation of the GUMS service

4. Site Customization

The following example for creation of account to be mapped,

The users belonging to the /atlas/ca VO will be mapped to the following unix account **canadian.** Only requests coming from Host that are part of the following domains *.racf.bnl.gov, usatlas.bnl.gov will be mapped.

1. Select Account Mappers



Configures account mappers.

Name: Canadians

i.e. myAccountMapper

Description: account only for Canadians

Type: group

Account: canadian (the account to map to)

i.e. myAccount

(c) 2004-07 Brookhaven National Laboratory - send suggestion … lists.bnl.gov

You are signed in as /DC=org/DC=doegrids/OU=People/CN=Ca

2. Choose a representative name

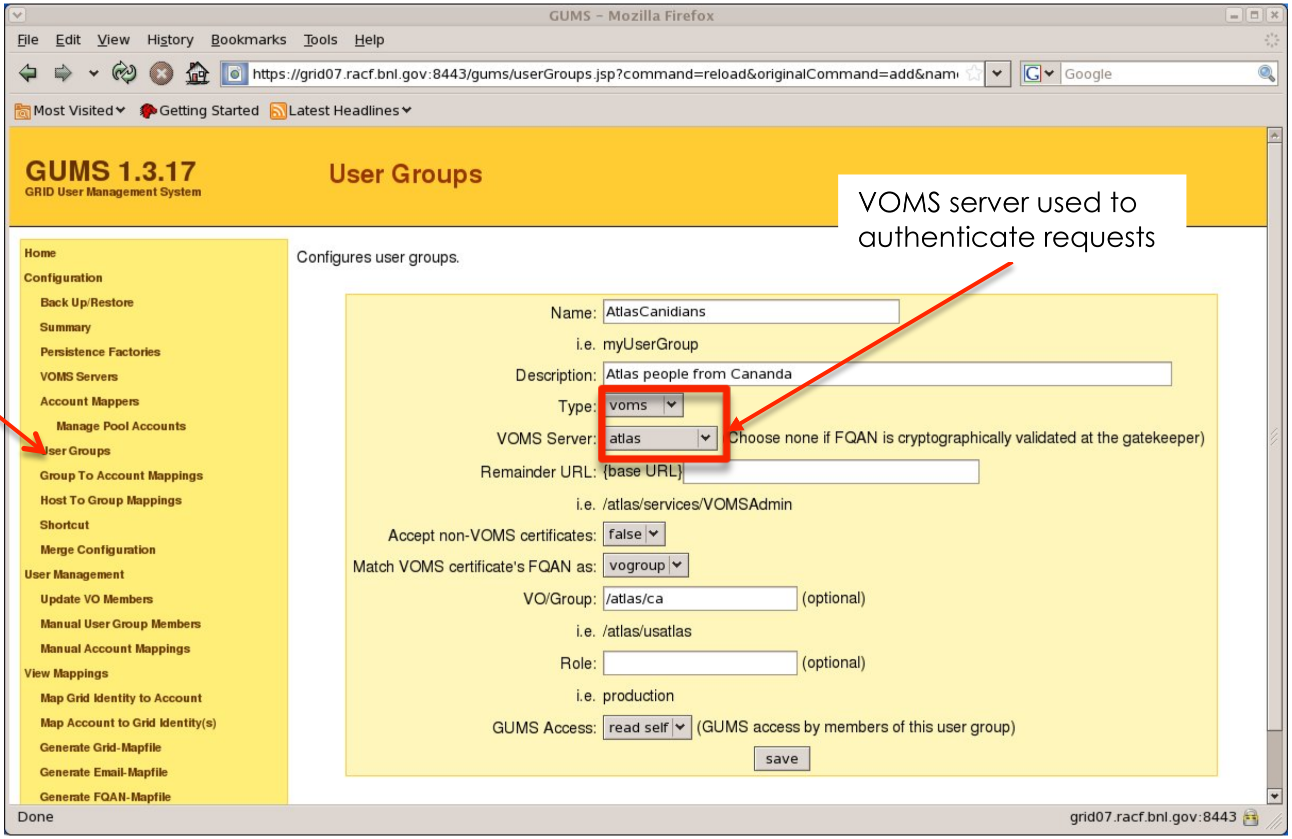
3. Brief description

4. SAVE CHANGES

4. Site Customization

Defines groups of users that share common associations (such as belonging to the same project)

In this case the group **AtlasCanadians**



https://grid07.racf.bnl.gov:8443/gums/userGroups.jsp?command=reload&originalCommand=add&nam

User Groups

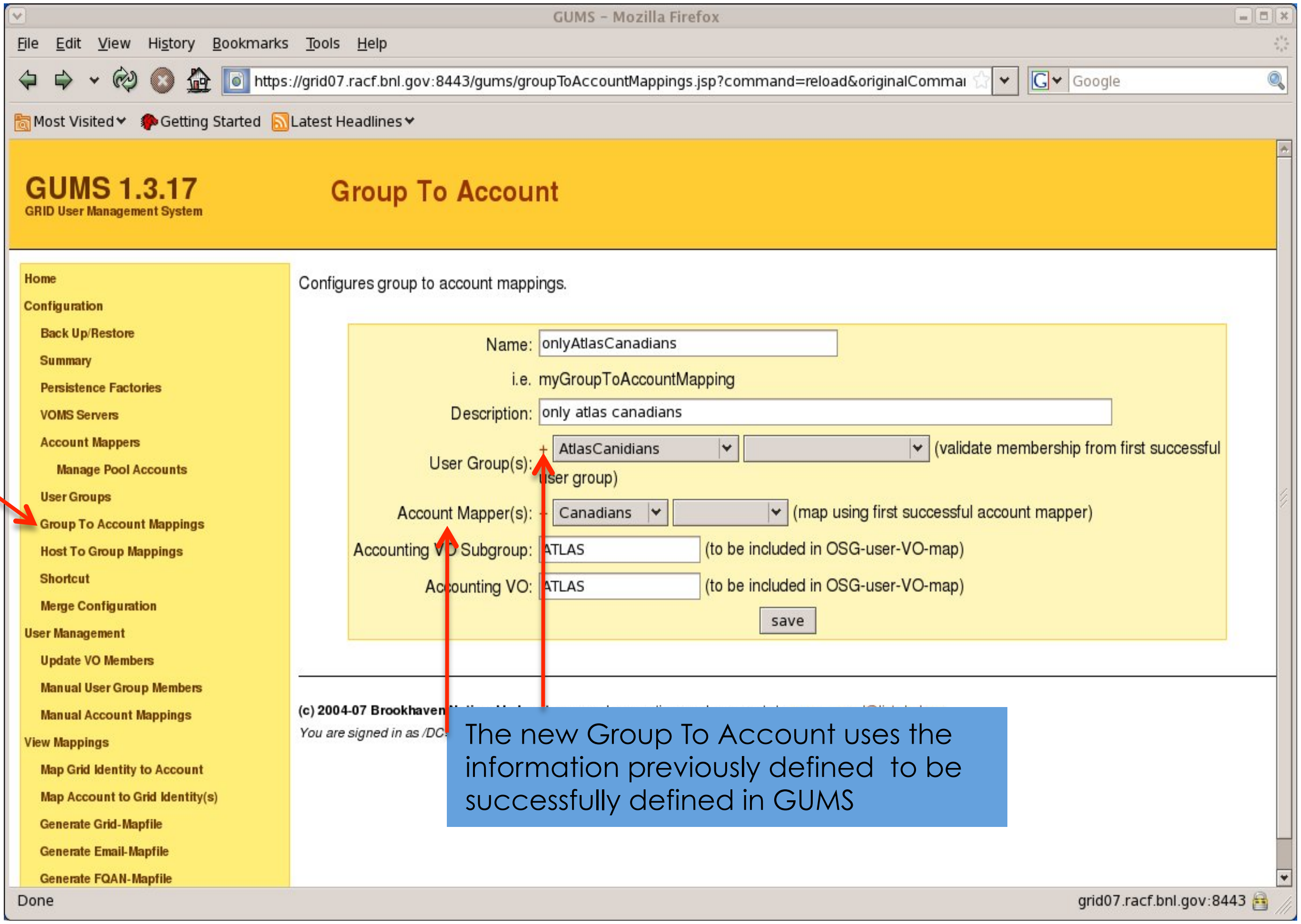
Configures user groups.

Name:	AtlasCanidians
i.e.	myUserGroup
Description:	Atlas people from Cananda
Type:	voms
VOMS Server:	atlas (Choose none if FQAN is cryptographically validated at the gatekeeper)
Remainder URL:	{base URL}
i.e.	/atlas/services/VOMSAdmin
Accept non-VOMS certificates:	false
Match VOMS certificate's FQAN as:	vogroup
VO/Group:	/atlas/ca (optional)
i.e.	/atlas/usatlas
Role:	(optional)
i.e.	production
GUMS Access:	read self (GUMS access by members of this user group)

VOMS server used to authenticate requests

4. Site Customization

Bundles a set of userGroups and a set of accountMappers together



Configures group to account mappings.

Name: onlyAtlasCanadians

i.e. myGroupToAccountMapping

Description: only atlas canadians

User Group(s): AtlasCanidians (validate membership from first successful user group)

Account Mapper(s): Canadians (map using first successful account mapper)

Accounting VO Subgroup: ATLAS (to be included in OSG-user-VO-map)

Accounting VO: ATLAS (to be included in OSG-user-VO-map)

(c) 2004-07 Brookhaven

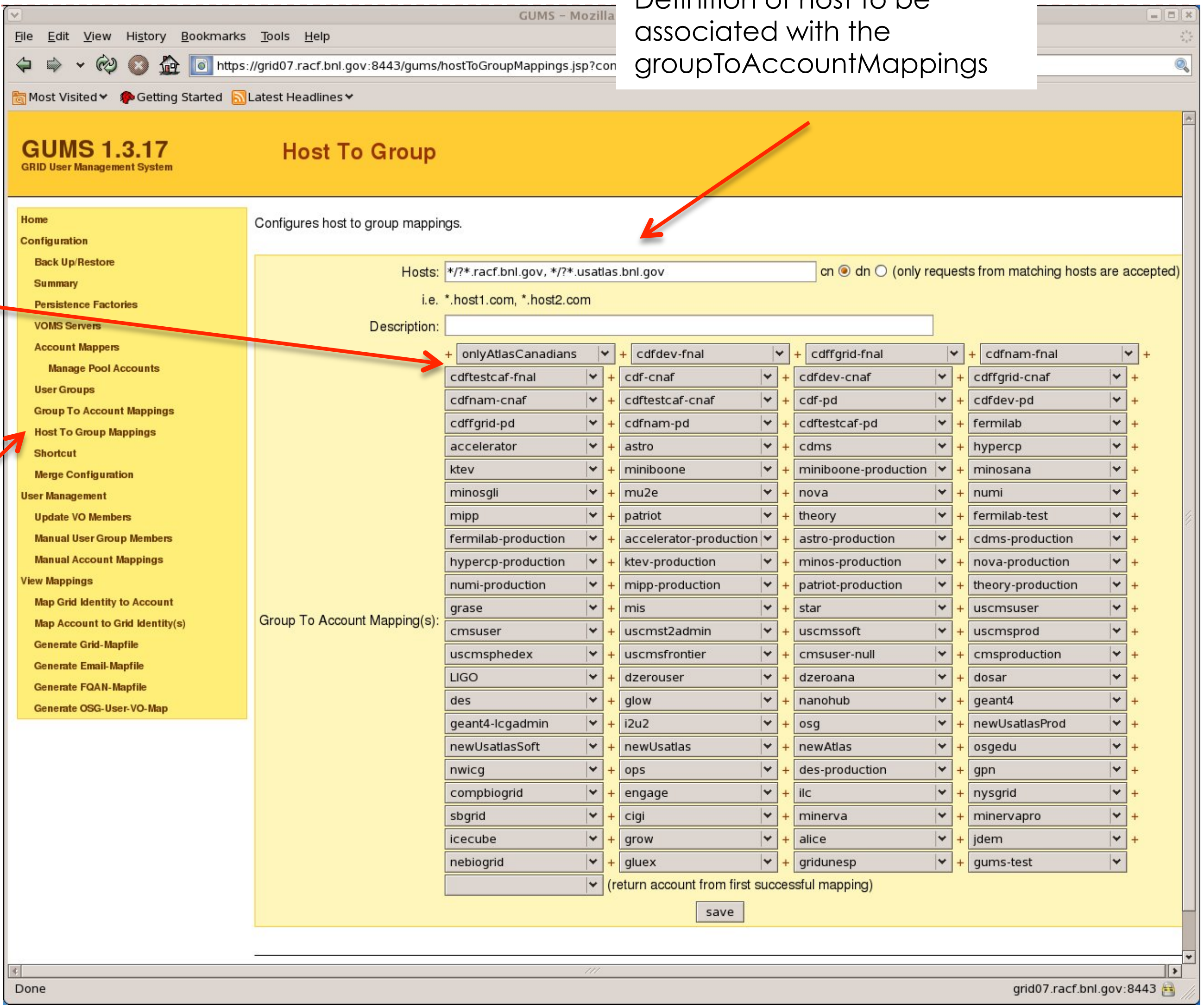
You are signed in as /DC

The new Group To Account uses the information previously defined to be successfully defined in GUMS

4. Site Customization

The order of the groupToAccountMappings is relevant, in this example the The request will be evaluating starting with **onlyAtlasCanadians.**

Defines which groupToAccountMappings are used for different hosts.



Host To Group

Configures host to group mappings.

Hosts: */?*.racf.bnl.gov, */?*.usatlas.bnl.gov cn ● dn ○ (only requests from matching hosts are accepted)

i.e. *.host1.com, *.host2.com

Description:

Group To Account Mapping(s):

onlyAtlasCanadians	cdfdev-fnal	cdffgrid-fnal	cdfnam-fnal
cdftestcaf-fnal	cdf-cnaf	cdfdev-cnaf	cdffgrid-cnaf
cdfnam-cnaf	cdftestcaf-cnaf	cdf-pd	cdfdev-pd
cdffgrid-pd	cdfnam-pd	cdftestcaf-pd	fermilab
accelerator	astro	cdms	hypercp
ktev	miniboone	miniboone-production	minosana
minosgli	mu2e	nova	numi
mipp	patriot	theory	fermilab-test
fermilab-production	accelerator-production	astro-production	cdms-production
hypercp-production	ktev-production	minos-production	nova-production
numi-production	mipp-production	patriot-production	theory-production
grase	mis	star	uscmsuser
cmsuser	uscmst2admin	uscmssoft	uscmsprod
uscmsphedex	uscmsfrontier	cmsuser-null	cmsproduction
LIGO	dzerouser	dzeroana	dosar
des	glow	nanohub	geant4
geant4-lcgadmin	i2u2	osg	newUsatlasProd
newUsatlasSoft	newUsatlas	newAtlas	osgedu
nwicg	ops	des-production	gpn
compbiogrid	engage	ilc	nysgrid
sbgrid	cigi	minerva	minervapro
icecube	grow	alice	jdem
nebiogrid	gluex	gridunesp	gums-test

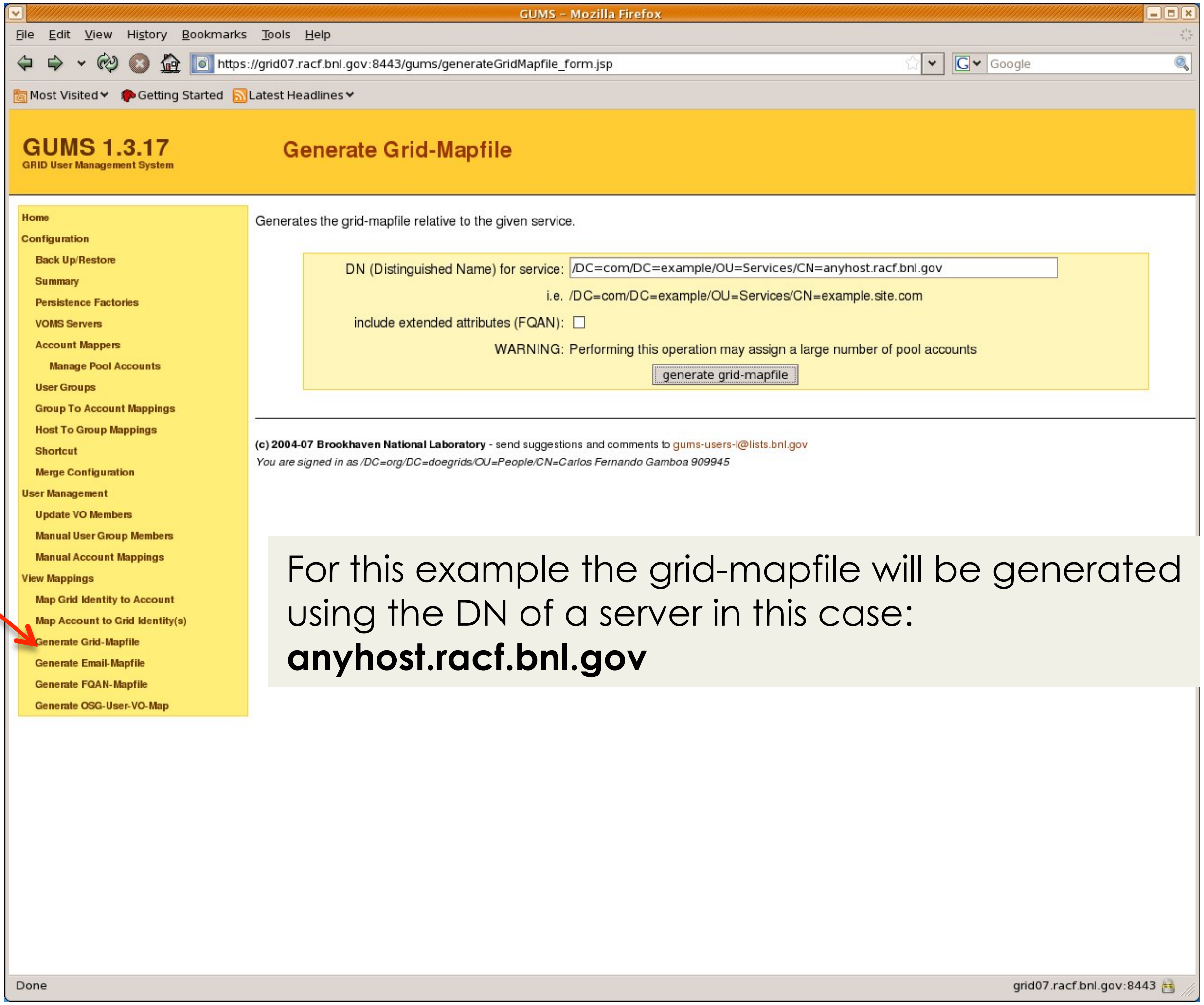
(return account from first successful mapping)

save

Definition of host to be associated with the groupToAccountMappings

4. Site Customization

Finally generate the grid-mapfile



Generate Grid-Mapfile

Generates the grid-mapfile relative to the given service.

DN (Distinguished Name) for service: /DC=com/DC=example/OU=Services/CN=anyhost.racf.bnl.gov

i.e. /DC=com/DC=example/OU=Services/CN=example.site.com

include extended attributes (FQAN): □

WARNING: Performing this operation may assign a large number of pool accounts

generate grid-mapfile

(c) 2004-07 **Brookhaven National Laboratory** - send suggestions and comments to gums-users-l@lists.bnl.gov

You are signed in as /DC=org/DC=doegrids/OU=People/CN=Carlos Fernando Gamboa 909945

For this example the grid-mapfile will be generated using the DN of a server in this case: **anyhost.racf.bnl.gov**

Acknowledgments

Many thanks to John Hover,
Brookhaven National Laboratory.

References

General GUMS installation notes

https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/InstallConfigureAndManageGUMS

Developer documentation

https://www.racf.bnl.gov/Facility/GUMS/1.3/index.html

GUMS Hands on by Steven Timm

https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GUMSHandsOn