Installing and managing GUMS

http://fermigrid.fnal.gov

Steven C. Timm

FermiGrid Services Group, Fermilab

with significant contributions from

Dan Yocum and Keith Chadwick

OSG Site Admins

August 10, 2010 @Vanderbilt

GUMS Install Introduction

- The bare steps to install GUMS are in the Twiki at https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GUMSHandsOn
- In the next hour our goal is to get you to have a single working GUMS server.
- We will go through the steps in the Twiki one by one and explain why.
- Then we will go over a few of the finer points of managing a GUMS server.
-

What is GUMS

- Grid User Management System
- Given a Distinguished Name (DN) from a certificate and an optional FQAN (Fully Qualified Attribute Name) it returns a username—usually a unix username.
- Also produces the osg-user-vo-map.txt which maps username to VO.
- Can be used to produce grid-mapfiles.
- GUMS is a web service, runs under Tomcat.
- Developed mostly at Brookhaven National Laboratory
- GUMS developer documentation: https://www.racf.bnl.gov/Facility/GUMS/1.3/index.html
- Required by most big VO's that use roles
- Faster than a grid-mapfile
- If you are not running GUMS you should be.
- GUMS can map to group accounts or pool accounts
- Pool accounts by default are never recycled.

Planning a GUMS server

- CPU load depends on rate of jobs through the gatekeeper, 1 call per job.
- Small cluster--60 core cluster * 2 hrs/job means 720 calls/day
- Big cluster (FermiGrid) average 289K calls/day, all-time record is 3M calls/day.
- Glexec can make 50-100Hz of calls.

FermiGrid GUMS-HA
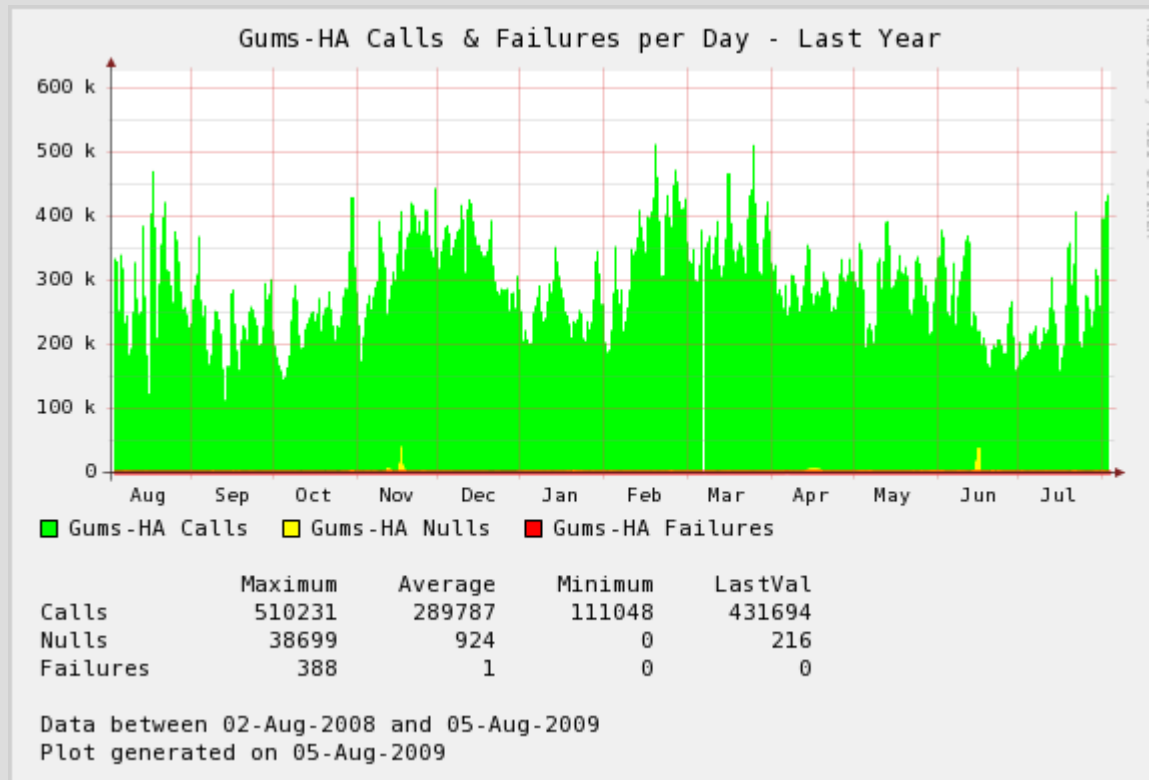
2 Virtual servers

1 core each of Xeon E5430 (Dell Poweredge 2950)

2GB RAM

Mean load >0.1
Since GUMS 1.3 upgrade. RSS ~350MB

Get pacman

- Note, we are following the steps in
- https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GUMSHandsOn
- Cd /usr/local
- wget http://atlas.bu.edu/~youssef/pacman/sample_cache/tarballs/pacman-latest.tar.gz
- tar xvfz pacman-latest.tar.gz
- cd pacman-3.29
- . setup.sh
- cd ..
- mkdir vdt-2.0.0
- Ln -s vdt-2.0.0 vdt
- cd vdt-2.0.0
- Notes—keep your pacman outside of your vdt dir
- Check for a clean PATH, watch out for old perl, java
- Use a versioned vdt directory, make a symlink.

Get a host and http certificate

- See https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GetGridCertificates
- That will give you instructions on how to request host and http certs from the command line using the cert-request tool.
- If you've got several of these it is worth becoming a GridAdmin for your site.
- See https://twiki.grid.iu.edu/bin/view/Security/OsgRaOperations, the GridAdmins section, for info on how to become a grid-admin
- There are a couple of OSG Registration Agents in the building who should be able to approve your request on the spot.
- You should make a host cert and an http cert.
- Only the http cert is actually used by the GUMS server.
- Make sure http cert is in /etc/grid-security/http, and directory and files are owned by daemon.
- It is OK to go ahead and do the rest of the GUMS install while waiting for the cert.

Pacman -get

- pacman -get http://software.grid.iu.edu/osg-1.2:gums
- Answer yes to the trusted caches questions
- Wait about 10 minutes.
- source setup.sh
- Vdt-post-install
- vdt-ca-manage setupCA --location local --url osg
- ln -s /usr/local/vdt-2.0.0/globus/TRUSTED_CA /etc/grid-security/certificates
- vdt-control --enable fetch-crl vdt-rotate-logs mysql5 apache tomcat-55 vdt-update-certs
- vdt-control –on
- Congratulations, GUMS is up!
- Check with browser https://yourgums.yourdomain:8443/gums
- Now we have to make it work.
- **Note** if anything goes wrong with pacman, you can always remove everything in the top level directory and start from scratch.

GUMS post-configuration

- Define a GUMS admin or admins:
  - cd tomcat/v55/webapps/gums/WEB-INF/scripts
  - ./gums-add-mysql-admin "YOUR DN"
  - Once this is done, you should be able to look at persistence factories on the web ui menu.
- Import the OSG template
  - ./gums-create-config –osg-template
  - Once this is done you should be able to generate a grid-mapfile
- Or bring your old gums config along from previous version of GUMS.
- GUMS will automatically upgrade it to the later version the first time you make a change from the Web UI

Using the Web UI

- Important—use the Web UI to make changes!
- One missed XML bracket in gums.config can break everything!
- Nifty features
  - Merge button—merge the latest OSG GUMS template with your current configuration.
  - "Shortcut" for adding a VO
    - In one form gives you all you need to add a new VO
  - Long way for adding a VO:
    - VOMS server
    - Account mapper
      - Manual, pool, group, ldap
      - Most common in OSG is group, CMS uses pool.
    - User Group
      - Sets of users from a VOMS server with group and role
    - Group to account mappings
      - Binds User Group above, with account mapper above
    - Host to group mappings
      - Order is important here
      - Can define different mappings for different hosts.

Troubleshooting

- Logs will be in $VDT_LOCATION/tomcat/v55/logs
- Look at catalina.out and gums-service-admin.log
- Some logs from my production server today:

10 Aug 2010 06:17:37,719 [WARN]: Automatic group update had failures - Some user groups weren't up
dated correctly:
dosar-admin - Couldn't retrieve users: (404)Not Found
icecubeadmin - Couldn't retrieve users: org.glite.security.voms.admin.common.VOMSSyntaxException: S
yntax error in container name: icecube/Role=icecubeadmin
icecubepro - Couldn't retrieve users: org.glite.security.voms.admin.common.VOMSSyntaxException: Syn
tax error in container name: icecube/Role=Production

Troubleshooting continued

- Open voms-admin of the relevant VO
- https://grid-voms.desy.de:8443/voms/icecube
- Browse the VO
- Look—in this case a group name is misspelled, I have icecubeadmin where it should be lcgadmin
- Also I have /Role=Production where it should be /Role=production
-

Troubleshooting--Null Mappings

- Null mappings—can fail to map for 3 reasons
  - VO requires a voms-qualified proxy and user doesn't have one
  - User is not in any VO.
  - The voms is malformed and the grid-mapfile or gums server is not picking up the user even though he is there

NO VOMS PROXY:

08 Aug 2010 05:42:44,298 [INFO]: GridID[/DC=org/DC=doegrids/OU=Services/CN=fnpcosg1.fnal.gov] - Mapped on host '/DC=org/DC=doegrids/OU=Services/CN=fnpcosg1.fnal.gov' the user '/DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Timothy Ma/CN=UID:timothym' / 'null' to 'null'

User not in VO YET:

02 Aug 2010 14:04:14,840 [INFO]: GridID[/DC=org/DC=doegrids/OU=Services/CN=fermigridosg1.fnal.gov] - Mapped

on host '/DC=org/DC=doegrids/OU=Services/CN=fermigridosg1.fnal.gov' the user

'/DC=org/DC=doegrids/OU=People/CN=Steven Cox 318595' / '/Engage/Role=NULL/Capability=NULL' to 'null'

 Browse a VOMS-ADMIN

•https://voms.fnal.gov:8443/voms/cdf/services/VOMSAdmin?
method=listUsersWithRole&container=/cdf/glidecaf&role=Role%3dnamcaf

Manual mapping

- Common usage—
  - Map one DOEGrids cert to a personal account
  - Map one cert to the rsvuser account.
- See https://twiki.grid.iu.edu/bin/view/MonitoringInformation/MapServiceCert