Status of GUMS (Grid User Management System)

John R. Hover
Grid Group
RHIC/ATLAS Computing Facility
Brookhaven National Laboratory
OSG Users Meeting 2008

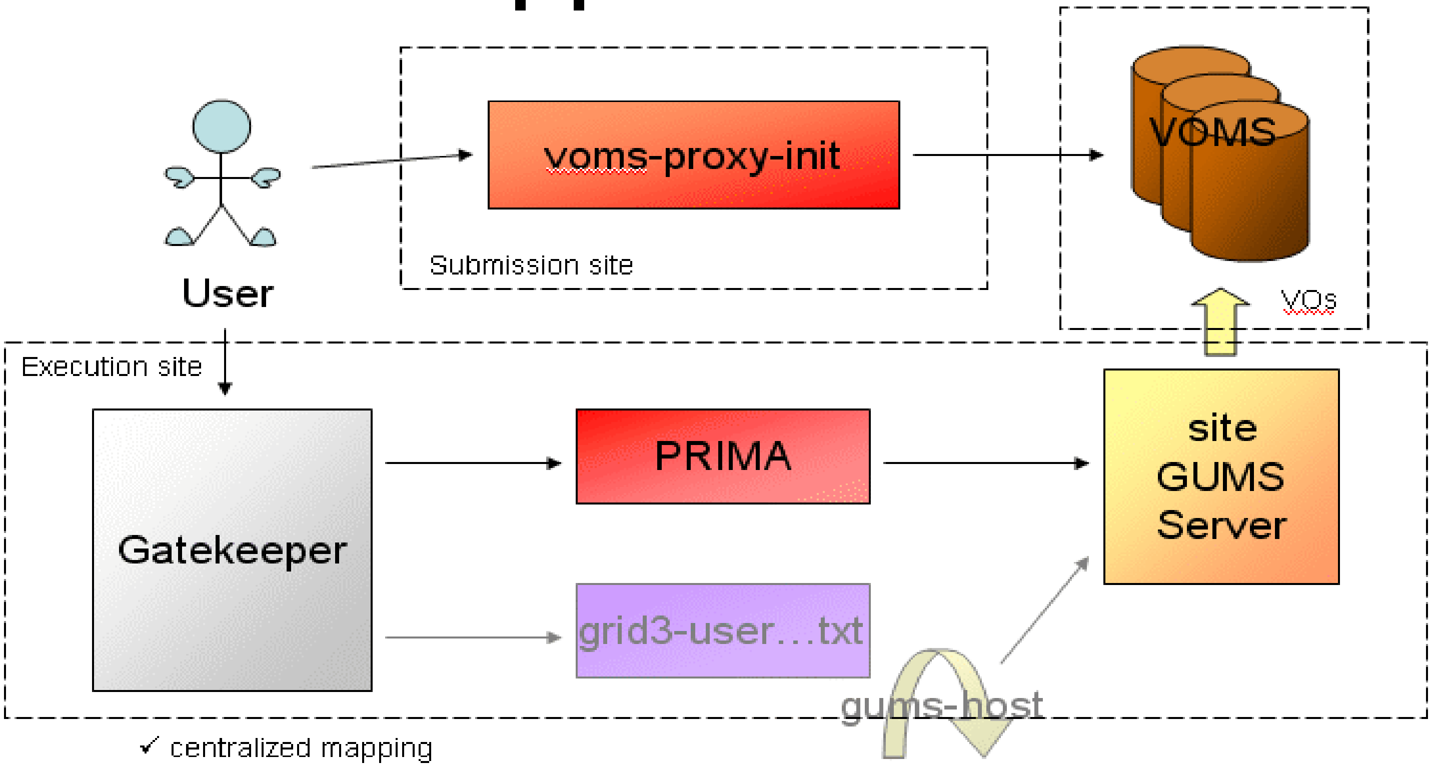
Brief History and Context

- Apache/Tomcat Web Service. In VDT/OSG.
- Periodically caches VOMS contents.
- Provides mapping from X.509 proxy DN (Distinguished Name) to a UNIX user account. e.g. '/DC=org/DC=doegrids/OU=People/CN=John R. Hover 47116' -> agrd1234
- Mappings can be flexibly specified by host, VO, group, and Role.
- Clients: Globus gatekeeper, glExec, dCache gPlazma

GUMS in Action.

Open Science Grid

Full support scenario



- ✓ centralized mapping
- ✓ account pool
- ✓/✗ dynamic mappings (broken by accounting)
- ✓ role/group based mappings

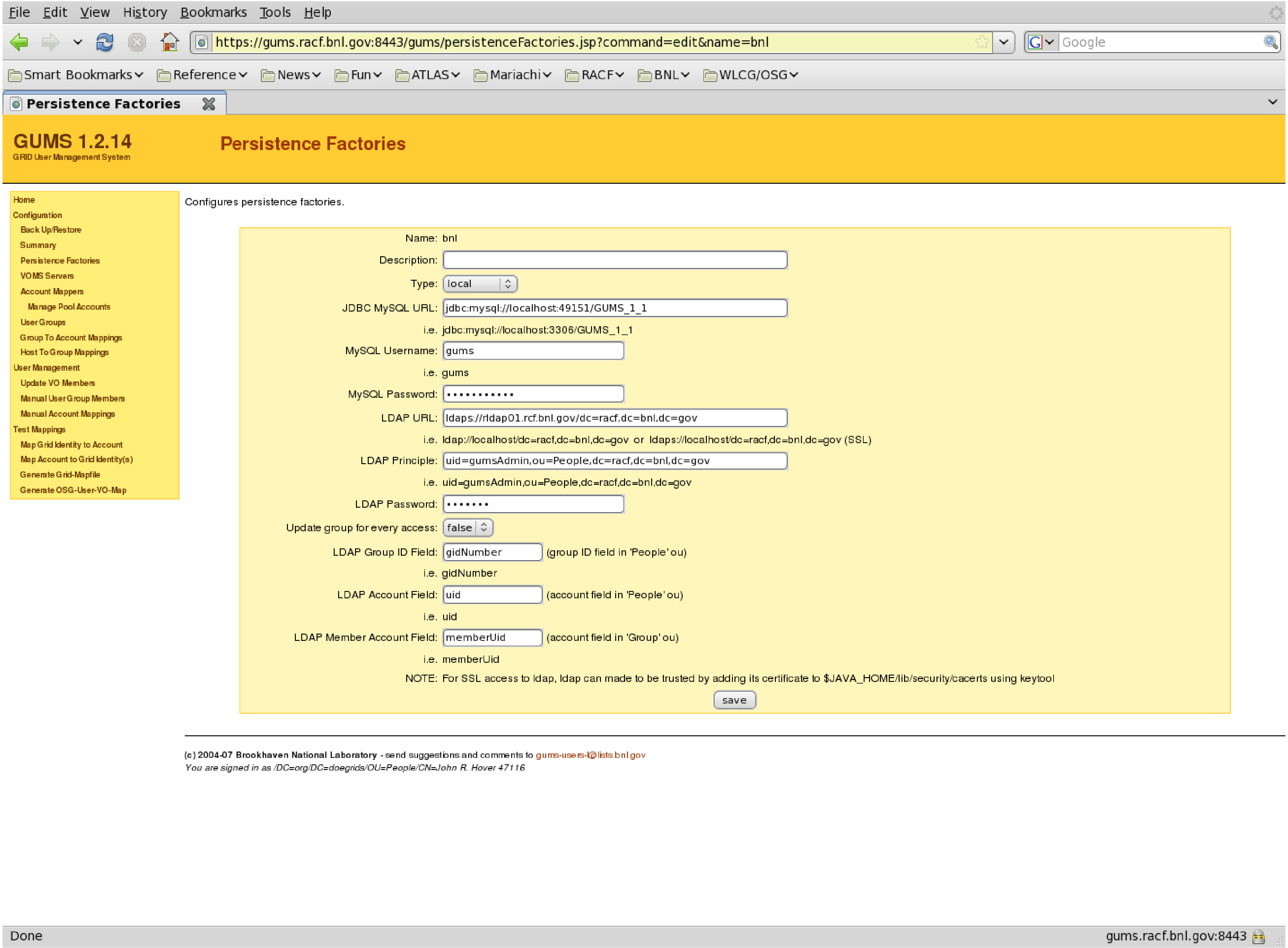
Notable Features

Current version is 1.2.14

- Fully flexible mapping definitions.
- Flexible User list sources (VOMS, LDAP, Manual).
- Support for *pool accounts*—UNIX accounts mapped on demand, with group(s) set in LDAP.
- Enterprise-grade: full unit and functional test coverage, Maven project management, nightly integration builds, automated deployment.

Most Recent Feature Additions

- Complete configuration via web-based graphic user interface—no more editing XML! (Which also required restructuring of internal configuration representation.)
- Detailed configuration summary in GUI.
- Configuration backup and restore via GUI.
- dCache-specific gridmap file type.
- More fine-grained read-access based on request host and user DN.
- Addition of LDAP as back-end 'database'.



GUMS 1.2.14
GRID User Management System

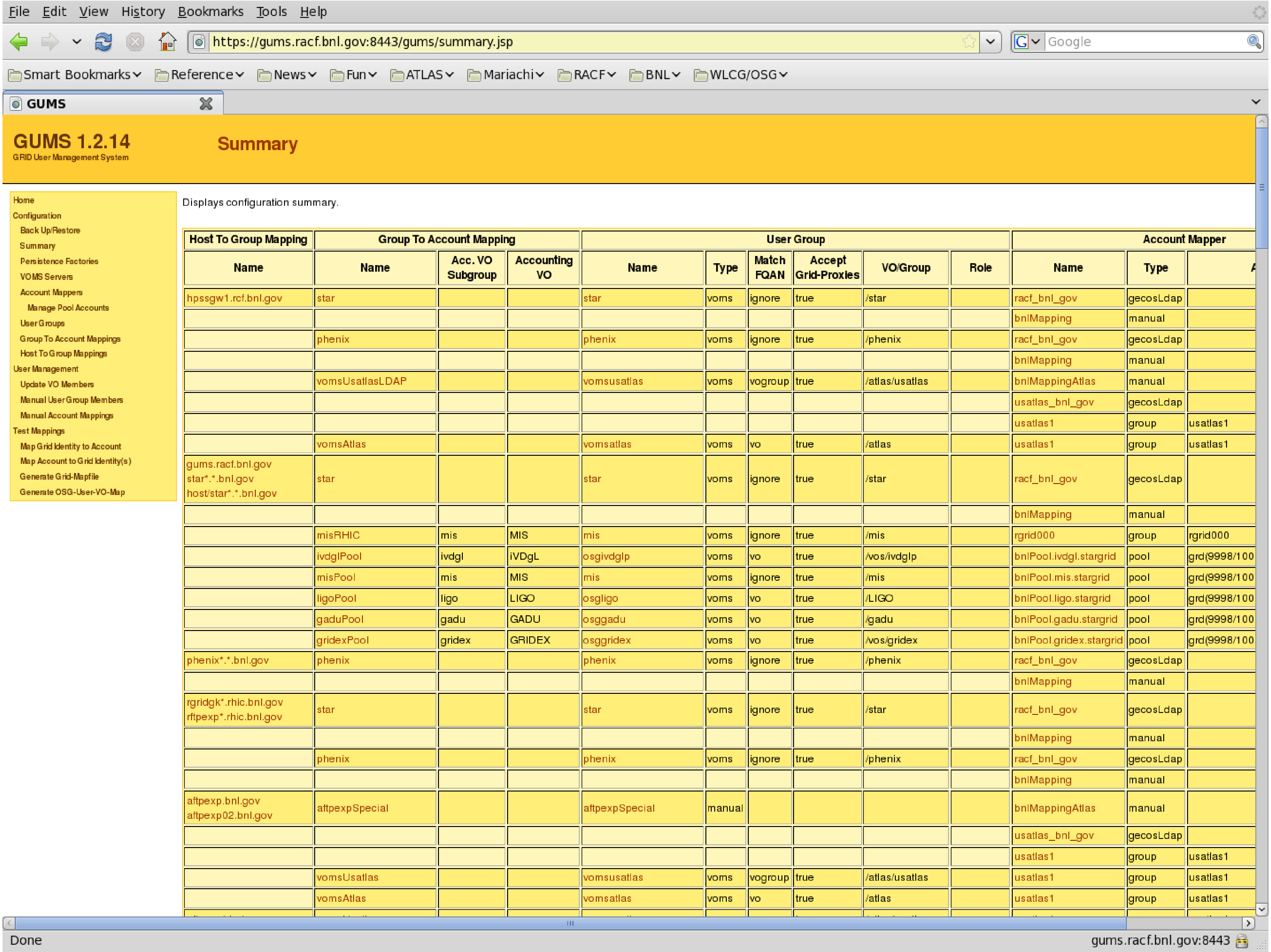
Persistence Factories

Configures persistence factories.

Name:	bnl
Description:	
Type:	local
JDBC MySQL URL:	jdbc:mysql://localhost:49151/GUMS_1_1
i.e.	jdbc:mysql://localhost:3306/GUMS_1_1
MySQL Username:	gums
i.e.	gums
MySQL Password:	•••••••••••
LDAP URL:	ldaps://rldap01.rcf.bnl.gov/dc=racf,dc=bnl,dc=gov
i.e.	ldap://localhost/dc=racf,dc=bnl,dc=gov or ldaps://localhost/dc=racf,dc=bnl,dc=gov (SSL)
LDAP Principle:	uid=gumsAdmin,ou=People,dc=racf,dc=bnl,dc=gov
i.e.	uid=gumsAdmin,ou=People,dc=racf,dc=bnl,dc=gov
LDAP Password:	•••••••
Update group for every access:	false
LDAP Group ID Field:	gidNumber (group ID field in 'People' ou)
i.e.	gidNumber
LDAP Account Field:	uid (account field in 'People' ou)
i.e.	uid
LDAP Member Account Field:	memberUid (account field in 'Group' ou)
i.e.	memberUid
NOTE:	For SSL access to ldap, ldap can made to be trusted by adding its certificate to $JAVA_HOME/lib/security/cacerts using keytool

(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=John R. Hover 47116



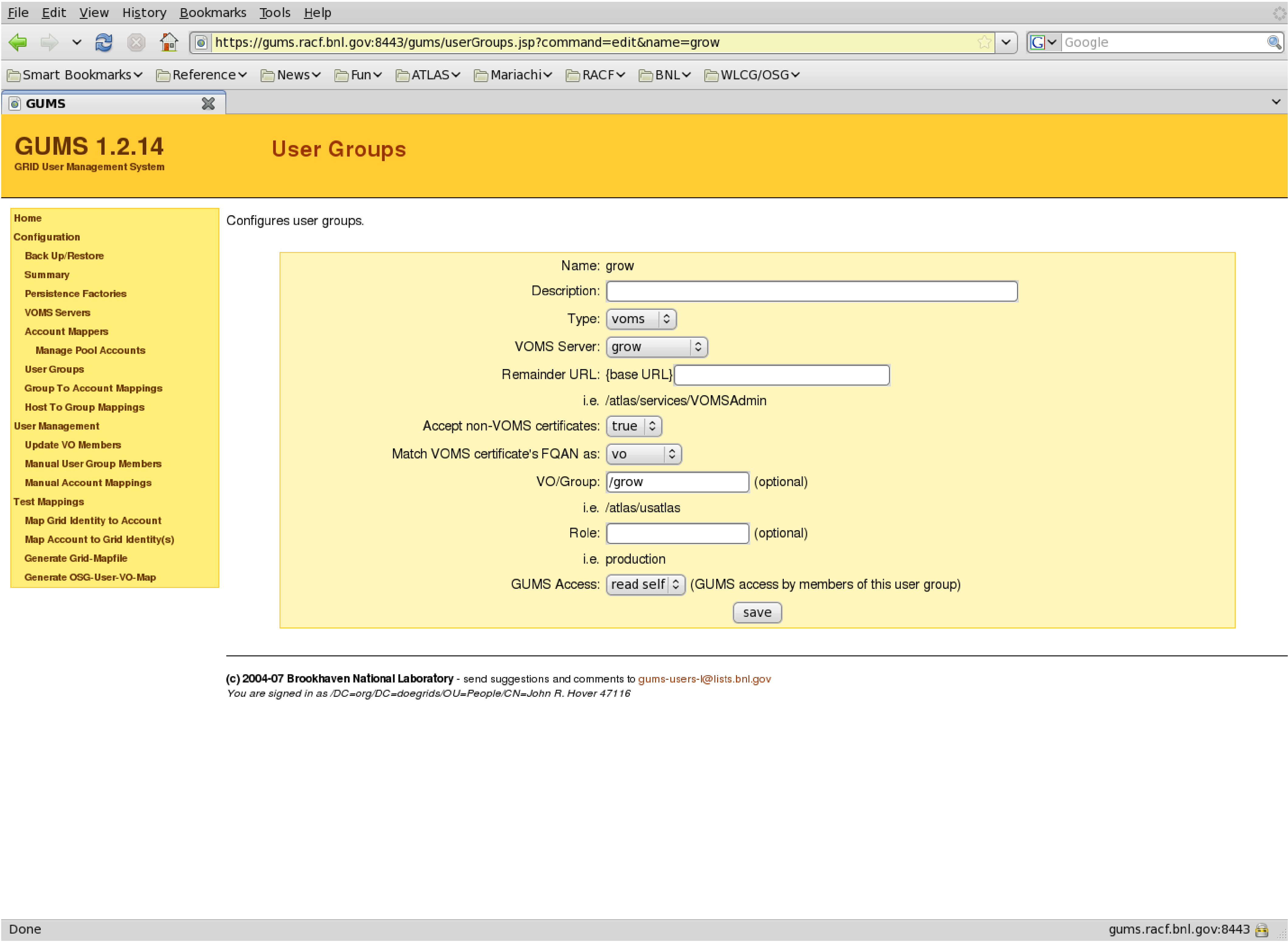
GUMS 1.2.14

GRID User Management System

Summary

Displays configuration summary.

Host To Group Mapping	Group To Account Mapping			User Group						Account Mapper		
Name	Name	Acc. VO Subgroup	Accounting VO	Name	Type	Match FQAN	Accept Grid-Proxies	VO/Group	Role	Name	Type	A
hpssgw1.rcf.bnl.gov	star			star	voms	ignore	true	/star		racf_bnl_gov	gecosLdap	
										bnlMapping	manual	
	phenix			phenix	voms	ignore	true	/phenix		racf_bnl_gov	gecosLdap	
										bnlMapping	manual	
	vomsUsatlasLDAP			vomsusatlas	voms	vogroup	true	/atlas/usatlas		bnlMappingAtlas	manual	
										usatlas_bnl_gov	gecosLdap	
										usatlas1	group	usatlas1
	vomsAtlas			vomsatlas	voms	vo	true	/atlas		usatlas1	group	usatlas1
gums.racf.bnl.gov star*.*.bnl.gov host/star*.*.bnl.gov	star			star	voms	ignore	true	/star		racf_bnl_gov	gecosLdap	
										bnlMapping	manual	
	misRHIC	mis	MIS	mis	voms	ignore	true	/mis		rgrid000	group	rgrid000
	ivdglPool	ivdgl	iVDgL	osgivdglp	voms	vo	true	/vos/ivdglp		bnlPool.ivdgl.stargrid	pool	grd(9998/100
	misPool	mis	MIS	mis	voms	ignore	true	/mis		bnlPool.mis.stargrid	pool	grd(9998/100
	ligoPool	ligo	LIGO	osgligo	voms	vo	true	/LIGO		bnlPool.ligo.stargrid	pool	grd(9998/100
	gaduPool	gadu	GADU	osggadu	voms	vo	true	/gadu		bnlPool.gadu.stargrid	pool	grd(9998/100
	gridexPool	gridex	GRIDEX	osggridex	voms	vo	true	/vos/gridex		bnlPool.gridex.stargrid	pool	grd(9998/100
phenix*.*.bnl.gov	phenix			phenix	voms	ignore	true	/phenix		racf_bnl_gov	gecosLdap	
										bnlMapping	manual	
rgridgk*.rhic.bnl.gov rftpexp*.rhic.bnl.gov	star			star	voms	ignore	true	/star		racf_bnl_gov	gecosLdap	
										bnlMapping	manual	
	phenix			phenix	voms	ignore	true	/phenix		racf_bnl_gov	gecosLdap	
										bnlMapping	manual	
aftpexp.bnl.gov aftpexp02.bnl.gov	aftpexpSpecial			aftpexpSpecial	manual					bnlMappingAtlas	manual	
										usatlas_bnl_gov	gecosLdap	
										usatlas1	group	usatlas1
	vomsUsatlas			vomsusatlas	voms	vogroup	true	/atlas/usatlas		usatlas1	group	usatlas1
	vomsAtlas			vomsatlas	voms	vo	true	/atlas		usatlas1	group	usatlas1



GUMS 1.2.14
GRID User Management System

User Groups

Configures user groups.

Name:	grow
Description:	
Type:	voms
VOMS Server:	grow
Remainder URL:	{base URL}
i.e.	/atlas/services/VOMSAdmin
Accept non-VOMS certificates:	true
Match VOMS certificate's FQAN as:	vo
VO/Group:	/grow (optional)
i.e.	/atlas/usatlas
Role:	(optional)
i.e.	production
GUMS Access:	read self (GUMS access by members of this user group)

(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=John R. Hover 47116

Current Work/Future Directions

- Convert LDAP (and other) interactions to a plugin architecture, allowing more flexibility and user-written plugins. Use LDAP as a UserGroup source (rather than VOMS). (LIGO request)
- Recycleable pool accounts (if user community desires).
- Clustered GUMS (2 GUMS servers sharing back-end database), behind DNS round-robin or virtual IP.

People and Sites

- Original design and development: Gabrielle Carcassi
- Current lead developer: Jay Packard <jpackard@bnl.gov>
- Current lead designer: John Hover <jhover@bnl.gov>
- Maven-generated web site: https://www.racf.bnl.gov/Facility/GUMS/1.2/