GUMS
(Grid User Management System)

"GUMS maps users' grid credentials to site-specific identities in accordance with the site's grid resource usage policy"

by Igor Sfiligoi

Purpose

- Map grid certificates/credentials to site-specific identities/credentials (like UNIX accounts)
  - Handle extended attributes (FQANs)
  - Can generate both static and dynamic mappings
  - Most often used as a replacement for Globus grid-mapfile
- A site-wide Policy Decision Point (PDP)
  - Implemented as a Web Service
  - Using SAML as the interface
  - Every Policy Enforcement Point (PEP) will call it
- Mappings configured in several ways
  - Manually in the local database
  - retrieved from external sources (like VOMS or LDAP)

Operation modes

- Two modes of operation
  - generate a node-specific grid-mapfile
  - map a single user
- Three types of mapping
  - personal accounts (manual or from LDAP)
  - group accounts (multiple DNs to a single UID, like VO->UID)
  - pool accounts (dynamically generated)
    - Guarantee that the same UID can be used by only one DN/FQAN at any given time
    - Currently, the pool account is created when a DN/FQAN is first seen, and never released

Flexible mappings

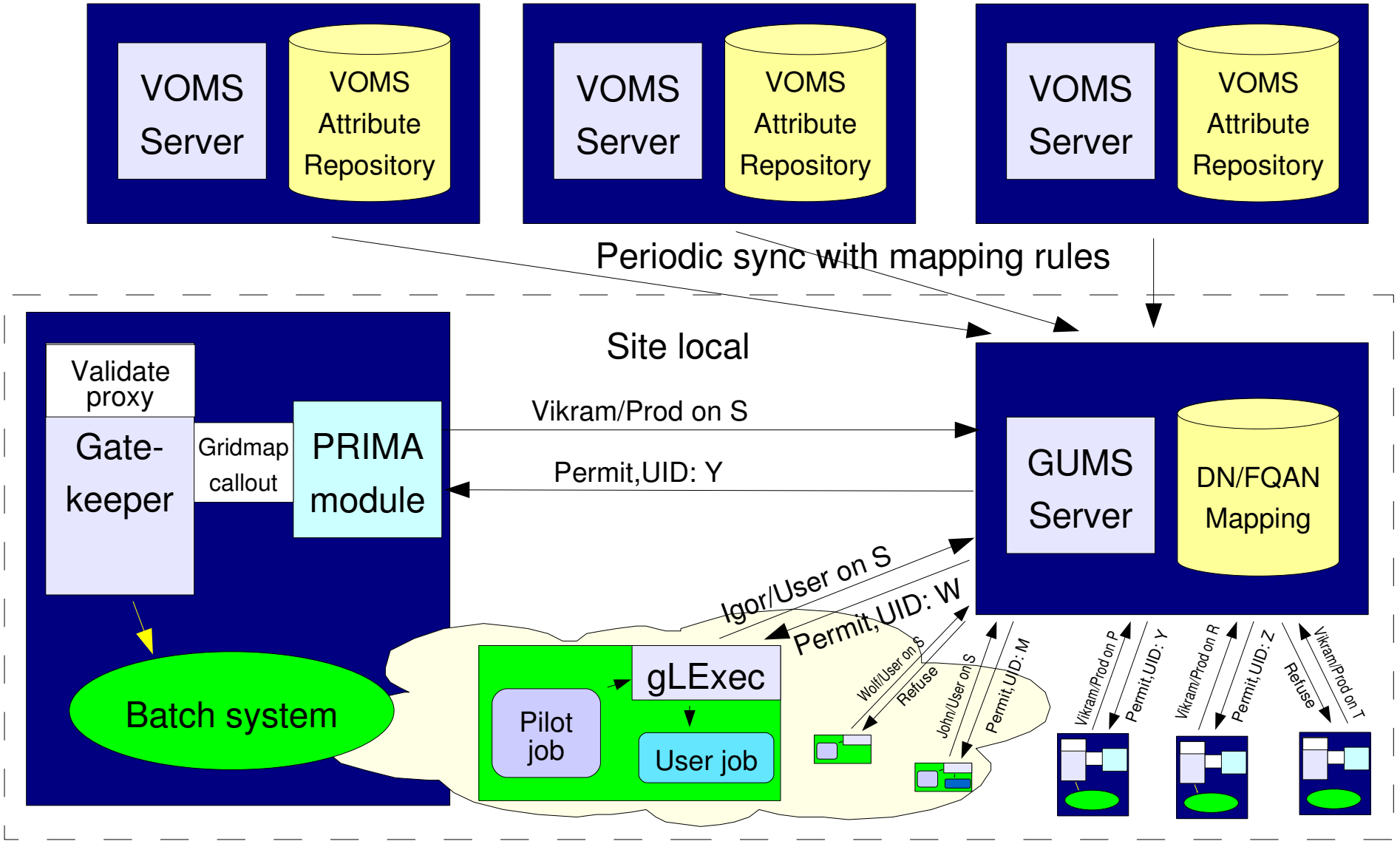
- Two kinds of grouping
  - By user
  - By host
- User groups
  - Map (DN,FQAN) to (uid,gid)
  - Mapping generated as described in previous slide
- Host groups
  - Connect host with user groups
  - A M x N configuration

    A single host group can be used for
    - Multiple hosts (like "*.usatlas.bnl.gov")
    - Multiple user groups (like “usatlasGroup,atlas,dial")

Integration with PEPs

- GUMS used inside Globus Gatekeeper via Prima AuthZ callouts
  - Both pre-WS and WS interface exists
- GUMS used by gLite gLExec via a dedicated LCMAPS plugin
  - Allows UID switching on the worker nodes
  - Needed for the Pull model

An example


VOMS Server
VOMS Attribute Repository
VOMS Server
VOMS Attribute Repository
VOMS Server
VOMS Attribute Repository
Periodic sync with mapping rules
Site local
Validate proxy
Gate-keeper
Gridmap callout
PRIMA module
Vikram/Prod on S
Permit,UID: Y
GUMS Server
DN/FQAN Mapping
Igor/User on S
Permit,UID: W
Batch system
gLExec
Pilot job
User job
Wolf/User on S
Refuse
John/User on S
Permit,UID: M
Vikram/Prod on P
Permit,UID: Y
Vikram/Prod on R
Permit,UID: Z
Refuse
Vikram/Prod on T