SVOPME
A Scalable Virtual Organization Privileges Management Environment

Nanbor Wang <nanbor@txcorp.com>
Tech-X Corporation
Gabriele Garzoglio <garzoglio@fnal.gov>
Fermi National Accelerator Laboratory

ISGC 2009, Taipei, Taiwan
April 21, 2009
Funded by US DOE OASCR
Grant #DE-FG02-07ER84733
Outlines

• **Project overview**
  – What SVOPME tries to address

• **Proof of concept**
  – Design and capability of the prototype tools

• **Outlook and planning**
  – Plans for a production quality tool
What are VO Privileges?

Virtual Organizations:
- VOs use resources
- VOs wish to define usage policies for various resources for different users within the VOs
  - Example 1: Production team members submit jobs with higher priority
  - Example 2: Software team members can write to disk area for software installations
- VOs define user privileges at different resources to comply with the expressed usage policies
- However, VOs do not manage/configure all Grid sites

Grid Sites:
- Grid sites provide resources
- Grid sites may want to provide different services to different VOs
  - Example 3: site X has a special agreement with VO Y; therefore, jobs from VO Y might have higher priority than others
- Grid sites help VOs to enforce their usage policies by managing user privileges
- Grid sites don’t define VOs’ usage policies

Site and VO Challenge: Enforcing heterogeneous VO privileges on multiple Grid sites to provide uniform VO Policies across the Grid (ad hoc solution: verbal communication)
Motivations of SVOPME

Address scalability

With the growth in Grid usage, both the numbers of **VOs** and **Grid-sites** increase.

Serious scalability problems in propagating VO privilege policies.

SVOPME:

- Provide the tools and infrastructure to help
  - VOs express their policies
  - Sites support a VO
- Reuse proven administrative solutions – we adopt common system configuration patterns currently in use in major grid sites.
Modern User Privilege Management

- Moving away from the use of gridmap files to VOMS/GUMS role-based privilege management
  - Eliminate the need for multiple user certificates
  - Similar trend can be observed in EGEE (LCAS/LCMAPS + SCAS and VOMS)
- Managing requests priority for both SE and CE
Proof of Concept: Prototype Implementation

- Provide validation of the overall approach
- Design suitable XML schemas for describing policies
  - This project adopts XACML
  - Allows aggregation of policies
  - XACML is also used by AuthZ Interoperability project
- Determine the information needed in VO and site policies
  - Compiled a list of resources and policies

- A prototype environment for synthesizing administrative directives and verifying VO policies
Survey of Resources and Policies Managed on the Grid

• Resources
  – OS protection (account types: group or pool)
  – Batch system
  – File system
  – External storage (SRM/dCache)
  – Network access (inbound/outbound)
  – Edge services

• Policies expressed by the Site
  – Timed availability (execution time slots for certain VO users)

• Policies expressed by both
  – Disk quota
  – File retention period
  – Account type
  – Network (inbound/outbound) access control

Highlighted policies are supported

SVOPME focuses on VO policies

ISGC09– SVOPME: A Scalable Virtual Organization Privileges Management Environment
SVOPME Prototype Architecture

A report on which VO policies are implemented by Grid Site

If response is permit, this VO policy is honored. Otherwise not.

Grid Site

Policy Advisor
- Produces
- Compares
- Grid Admin uses these instructions and configures CE and SE accordingly

Site Instructions

Compute Element
- Outputs site policies
- Outputs site resources

Storage Element

Policy Comparer
- Same query sent to the Grid Policy
- Policy Advisor
- Compares

VO Policies with supporting attributes/Verification Queries
- VO Policies
- Edits VO Policies
- VOMS Client
- Provides info from VOMS server

XACML VO Policy Editor

VO

Grid Probe

Std Grid Service

Output Directive

Output Data

Legend

Middleware Component

Domain

Action
The VO Tool – Used by VO-Admin

VO Policies with supporting attributes/Verification Queries

Executes test queries for every policy such that the response is always a permit.

If response is permit, this VO policy is honored. Otherwise not.

Legend

- Middleware Component
- Output Data
- Output Directive
- Action
- Std Grid Service
- Domain

A report on which VO policies are implemented by Grid Site

If response is permit, this VO policy is honored. Otherwise not.
XACML VO Policy Editor (Domain Specific)

- **XACML** is a generic XML-based language for specifying access control policies
  - Not very human readable
  - Suitable for machine processing
- **The VO Policy Editor**, therefore, allows VO administrators to edit a set of pre-defined VO policies in simple readable forms
  - For example: Account Mapping Policy
    - Group _____ should run with pool/group account
- The VOMS client obtains information about all the Group/Role and the number of users from the VOMS server. This information is passed to the VO Policy Editor to avoid operator errors
- The Editor stores the policies and test queries for verification in XACML format to enable automation
- Support for new policy types can be added as “Policy Template” plug-in’s
- We also plan to develop command-line policy editing tools to convert between a text-based policy specification and XACML documents
Prototype VO Policy Editor Screen Shot 1
Select Policy Type to Add

Select Policy

VO Policy Description
Prototype VO Policy Editor Screen Shot 2
Edit Policy Attributes

VOMS Client assists in setting attributes for the policy
Prototype VO Policy Editor Screen Shot 3
Allow XACML view

Policy is then converted into XACML template
Three Grid Site Tools – Used by Site-Admin

- **VOXACML VO Policy Editor**: A report on which VO policies are implemented by Grid Site. Executes test queries for every policy such that the response is always a permit. If response is permit, this VO policy is honored. Otherwise, not.

- **VOMS Client**: Provides info from VOMS server, compares VO Policies with supporting attributes/Verification Queries.

- **Policy Comparer**: Compares VO Policies. Edits VO Policies.

---

**Grid Site**

- **Grid Probe**: Outputs site policies.
- **Storage Element**: Probe site resources.
- **Compute Element**: Outputs site policies.
- **Site Instructions**: Grid Admin uses these instructions and configures CE and SE accordingly.

**Legend**

- **Middleware Component**
- **Output Data**
- **Output Directive**
- **Action**
- **Std Grid Service**
- **Domain**
Grid Probe

- Probes the Grid site local configurations

- For Phase-I we probe the settings of the GUMS and Condor systems
  - GUMS provides info on account mapping from VO user/role to local UID
  - Condor provides priorities of accounts

- Generates the equivalent Grid side policies (in XACML)
Vo/Grid Policies Advisor

- Verify that the Grid site configurations support the VO policies by running the verification queries generated by VO Policy Editor for each VO policy.
- Provide advice for the Grid site administrator on what amendments need to be done on the Site; such that the Grid site complies with the VO policies.
- Example output:
  - VO requested 3 accounts for VISITORS role via VO policies.
  - Site-policies derived from GUMS do not match.

```java
VO/Grid Grid Accounts Policy Advices

No matching Grid Accounts Policy was found for /TECHXVISITORS on the Grid site. Create a mapping in GUMS config such that /TECHXVISITORS be mapped to at least 3 account(s).
```

```java
TECHX/Role=VO-Admin mapped to 1 account(s) (techxVOadmin) on the Grid site, is not sufficient enough. Needs to be mapped to at least 3 accounts.
```
VO/Grid Policies Comparer

- Verify that the Grid site configurations support the VO policies by running the verification queries generated by VO Policy Editor for each VO policy
- Produces a report for the **VO admin** on which VO policies are honored by the Grid site and which are not
- Example output:

```java
VO/Grid Grid Accounts Policy Comparison
---------------------------------------
/TECHX/Role=User is mapped to 1 account(s) on the Grid site. Passed!
No Account Mapping Policies for /TECHX/VISITORS were found on the Grid site.
/TECHX/Role=Software-Admin is mapped to 1 account(s) on the Grid site. Passed!
/TECHX/Role=VO-Admin does not have sufficient accounts on Grid Site. Failed! (Needs to be mapped to at least 3 accounts.)
/TECHX is mapped to 1 account(s) on the Grid site. Passed!
```
Advantages for VOs and Sites

Advantages for the VOs

• No need to run ad-hoc jobs to figure out what policies are enforced and what not
• Provides templates to define commonly used policies
• Automates most of the communication with Sites that support the VO
• Provides the basis for the negotiation of privileges at sites that provide opportunistic access

Advantages for the Sites

• Sites can advertise and prove that a VO is supported
• Sites that want to support a VO have a semi-automated mechanism to enforce the VO policies
• Privilege enforcement remains responsibility of the Site, informed by formal VO policy assertions
Future Workplan

- **Objective 1: Usability**
  - Support a more comprehensive set of VO policies
    - Add support for remaining policies collected in Phase I
      - Not sure if we want to incorporate site-specified policies or not
    - Collaborate with VOs and key OSG grid sites to gather VO policies needed and how sites could support these policies
  - Command-line scripting tools
    - Derive a set of policy statements
    - Embed policy statements in generated XACML
Future Workplan (Cont.)

- **Completing Features and Hardening of prototype tools**
  - Overall Feature enhancements
    - Change to use PolicySets for VOs and grid sites
      - Allows us to aggregate policies
      - Supports the semantics of a whole VO or site
    - Modularize components
      - Support new policies
      - Support new grid environments and configurations
    - Support customized policies and queries
  - VO Policy Editor
    - Merge VOMS Client with the Editor
    - Allow opening/editing/saving of existing PolicySet
    - Support browsing of PolicySet
    - Support consistency check of overall VO PolicySet
    - What to do when there’s a mismatch between VO and PolicySet
  - Grid Probe
    - Support probing of more resources / configurations
Future Workplan (Cont.)

- VO/Grid Policy Comparator/Advisor
  - Currently, we only check for supported policies but not redundant site policies
  - Address security concerns (of site configurations and policy inconsistency, etc.)
- Services for VOs and Grid sites to exchange/verify policies

- **Objective 2: Flexibility and Robustness**
  - Modularize system aspects such as Grid configurations and tool stacks
  - Migrate toward a common Grid XACML profile (Authorization Interoperability Profile)
  - Identify and implement more privilege policies
    - Site-specific policies
    - Service contracts between sites and VOs?
Future Workplan (Cont.)

- **Objective 3: Demo the Effectiveness**
  - Integrate with OSG distribution
  - Develop recommendation for running/using SVOPME tools
  - Deployment, documentation and customer service
Conclusions

- SVOPME ensure uniform access to resources by providing an infrastructure to propagate, verify, and enforce VO policies at Grid sites.
- SVOPME integrates with the OSG Authorization Infrastructure.
- We are extending and adjusting the scope of the project based on feedback and comments on the prototype tools.
- We plan to comparing the policy work in EGEE.
- We love to hear your comments and suggestions.

https://ice.txcorp.com/support/wiki/MidSys/SVOPME