Secure Federated Light-weight Web Portals for FusionGrid

By: D. Aswath, M. Thompson, M. Goode, X. Lee, N. Y. Kim

Presented by: Dipti Aswath

GCE Workshop 2006
Second International Workshop on Grid Computing Environments

Tampa, Florida
Nov 12-13, 2006
Acknowledgements

• The National Fusion Collaboratory Project (FusionGrid)

• The DOE Web Portals Project

• The Staff of the DIII-D National Fusion Facility

• Work is supported by the USDOE Department of Energy
  - SciDAC: Office of Advanced Scientific Computing Research
  - Significant leveraging: Office of Fusion Energy Sciences
Presentation Key Points

• **FusionGrid**
  - Highly-distributed collaborative virtual environment (VO)
  - Supports scientific needs of the US Fusion community

• **Fusion web sites dispersed across the US**
  - Light-weight single purpose portals

• **Federate these disparate web sites**
  - Integrate Pubcookie and MyProxy technology with FusionGrid credentials
  - Provide code portals for easy client usage of FusionGrid service from any web browser

• **Extend our Federated Portal architecture to meet future needs**
  - FusionGrid credentials with DIII-D’s Media-Wiki pages and Bugzilla
  - Visualizations of FusionGrid codes (input and output stages) with web portals
FusionGrid created for better use of resources

- **Resources shared between sites**
  - Reduces duplication of effort
  - Secures resources with a security model

- **Identifies FusionGrid users on separate administrative domains**
  - Authentications with X.509 (based on PKI infrastructure)
  - Provides single sign-on with Credential Delegation

- **Allows resource owners to control access to their resources**
  - Authorization with ROAM
  - Resource queries ROAM and makes authorization decisions
Fusion Research Web sites dispersed across US

- **Serve FusionGrid functionality**
  - Authentication
  - Monitoring
  - Authorization
  - Working documents
  - Several potential job submission sites

- **Function as light-weight single purpose portals**
FusionGrid services launched with client software

- **Client programs depend on**
  - Globus Security Infrastructure (GSI) for secure data access and remote job submissions
  - Interactive Data Language (IDL) - a commonly used software analysis and programming language in the experimental fusion community

- **Gives rise to two problems**
  - Globus Toolkit not available on Windows and has fairly complicated installation procedure on Unix
  - IDL needs commercial license and is not available on every client system
Easy Client Usage of FusionGrid services

• Single general purpose portals did not quite meet our needs
  − Did not correspond to the realities of a highly distributed virtual organization with its significant amount of legacy web sites

• What was desirable?
  − Simple web interfaces with easy client usage from any web browser capable system
  − Web interfaces to facilitate data marshalling and remote job submissions
  − Web interfaces enabled to leverage off a single sign-on authentication scheme to get a proxy certificate for the user
Secure Federated Web Portals

- **Single purpose portals to help users**
  - Data preparation stages
  - Setting input parameters,
  - Recording inputs for future reference
  - Invoking the computational service on the FusionGrid
  - Monitoring the service
  - Making results available to the user

- **Challenges for such portals**
  - Provide single sign-on across all other portals a user requires
  - Obtain necessary grid credentials to enable client web browser to make GSI calls to FusionGrid services
  - Provide access to Globus from within the portal
Federated Portal Architecture

ADS
- Credential Manager
  - Pubcookie login server
  - MyProxy servers

Web portal (1)
- Pubcookie login

Web portal (2)
- Login cookie

ROAM (AuthZ)

ADS: Authorization & Delegation Server

ROAM: Resource Oriented Authorization Manager

secure connection
mutually authenticated, trusted connection

gridID
User de/Cred

FusionGrid service
User CN
Credential Manager (CM)

- Web based interface for handling registration of users and management of their X.509 user certificates

- FusionGrid accepts new users via request to the CM for new certificate
  - Requires user name, password, contact information, purpose to join FusionGrid
  - Needs to be approved by a sponsor and issued by an RA

- Long term credentials issued are stored in collocated MyProxy server

- User gets proxy certificates authenticated by user name, password via a myproxy-logon call
  - Keys are password encrypted with passwords not stored on CM host
  - Removes need for credential to be stored on machine from where Globus jobs are submitted
Single sign-on with Pubcookie

- Open source package providing a multi-site/single sign-on ability for web sites in the same domain (e.g. fusiongrid.org)

- Framework consists of an Apache module deployed on all of the trusted web portals and a central login server

- Single sign-on process:
  - First time FusionGrid user accesses a page hosted by Web Portal(1), they are redirected to the login server to get a cookie
    - Login server presents a login page to the user to enter his gridID and password
    - Login server then authenticates the user returning two cookies - a granting cookie scoped to reach the web portal and a login cookie scoped to be returned to it
  - WebPortal(1) creates a site-specific signed cookie (session cookie) containing user’s gridID for subsequent requests for web pages hosted by it
  - Login cookie used for user’s subsequent access to other web portals (e.g. WebPortal(2))
MyProxy Server with Pubcookie

- **Two MyProxy servers**
  - **MyProxy Credential Store** to store end-entity certificates with encrypted keys and to provide a flexible user oriented delegation policy
    - Anonymous delegation with password
  - **MyProxy Proxy Store** to store short-term proxies with unencrypted keys and to allow for delegations by only a set of known web services
    - Retriever must authenticate by certificate and be listed as an allowed retriever for the specific certificate

- **Pubcookie uses MyProxy**
  - Authenticates a FusionGrid user with the gridID and password supplied
  - Stores the resulting proxy in the MyProxy proxy store

- **Web Portal requiring a proxy certificate**
  - Authenticates itself with its own X.509 certificate registered with the ADS
  - Retrieves the short term proxy for an authenticated user from the MyProxy store to submit Globus jobs on their behalf
Web Portal Use Case

• **OneTwo**
  - FusionGrid computational service

• **AutoOneTwo and PreOneTwo**
  - IDL-based client side GUI
  - Help scientists prepare OneTwo inputs and launch runs remotely on FusionGrid

• **OneTwo portal enables FusionGrid users to launch OneTwo runs**

---

1. Sign on with FusionGrid credentials
2. Load inputs into database
3. Run code on Run ONETWO on a Linux cluster hosted at GA
4. Read ONETWO inputs
5. Status messages to the FusionGrid monitor monitoring the ONETWO run
6. Write ONETWO o/p/s
7. Visualize ONETWO i/po
Web Portal to launch OneTwo runs on the FusionGrid

FusionGrid Web Portal

Run FusionGrid computational codes:

- ONETWO
- TRANSP
- GATO

about the fusion grid | fusiongrid research

Web Page for OneTwo inputs preparation
### Web Page (FGM) to monitor a OneTwo run

![FusionGrid Logo]

**FGM (Fusion Grid Monitor) - RunID 9**

<table>
<thead>
<tr>
<th>RunID</th>
<th>CODE</th>
<th>COMPLETED</th>
<th>Tokamak</th>
<th>DATE</th>
<th>2006-09-22</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Slot</th>
<th>State</th>
<th>Contact</th>
<th>Queue</th>
<th>Start at</th>
<th>Stop at</th>
<th>Wall Time</th>
<th>CPU Time</th>
<th>Priority</th>
<th>Host</th>
<th>Fcat Code</th>
<th>Logfile</th>
<th>Data Monitor</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Sep 22 17:54:19 PDT 2006</td>
<td>1190</td>
<td>Completed</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Completed OK</td>
</tr>
<tr>
<td>Fri Sep 22 17:54:19 PDT 2006</td>
<td>1190</td>
<td>Writing Outputs</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Data written to AOT06</td>
</tr>
<tr>
<td>Fri Sep 22 17:54:06 EDT 2006</td>
<td>1190</td>
<td>Writing Outputs</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Writing to MDSplus</td>
</tr>
<tr>
<td>Fri Sep 22 17:54:08 EDT 2006</td>
<td>1190</td>
<td>Running</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Run completed OK</td>
</tr>
<tr>
<td>Fri Sep 22 17:53:12 PDT 2006</td>
<td>1190</td>
<td>Running</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Running</td>
</tr>
<tr>
<td>Fri Sep 22 17:53:14 PDT 2006</td>
<td>1190</td>
<td>Fetching Inputs</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Directory prep OK</td>
</tr>
<tr>
<td>Fri Sep 22 17:53:10 PDT 2006</td>
<td>1190</td>
<td>Fetching Inputs</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Preparing directory</td>
</tr>
<tr>
<td>Fri Sep 22 17:53:10 PDT 2006</td>
<td>1190</td>
<td>Authorization</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Authorization OK</td>
</tr>
<tr>
<td>Fri Sep 22 17:53:09 EDT 2006</td>
<td>1190</td>
<td>Authorization</td>
<td><a href="mailto:leesia@fusion.gat.com">leesia@fusion.gat.com</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>star12.gat.com</td>
<td>autoonetwo.sh</td>
<td>View Log</td>
<td>-</td>
<td>Checking</td>
</tr>
</tbody>
</table>

---

**DIII-D**

![General Atomics Logo]
Lessons Learned

- **Limitations**
  - Web Portals are required to have a fusiongrid.org alias in addition to their primary name
  - Portals require presence of an SSL-enabled Apache webserver and host X.509 certificates listed with the ADS

- **Preliminary phase shows**
  - Codes with intensive visualizations during input preparation not suited for access with our portal framework
  - Codes without extended graphics (such as OneTwo) are better suited for use
Next Steps

- **Enable visualization of FusionGrid code-run outputs with web browsers**
  - Elvis ~ a java based scientific visualization tool allows users to view graphs in a browser window

- **DIII-D’s fusion facility makes use of a Media-Wiki based web site and Bugzilla system to track software updates and bugs**
  - FusionGrid credentials for the login scheme on Media-Wiki and Bugzilla
  - Pubcookie authentication model to secure the Wiki pages and eliminate need for users to have a separate set of logins for both
Conclusion

- **Straight-forward implementation to authenticate, authorize and provide a proxy credential for the user**
  - Federated disparate web sites with single sign-on authentications with FusionGrid credentials
  - OneTwo Portal securely launched OneTwo as a FusionGrid service
  - Presented a convenient and intuitive web interface for input preparations of FusionGrid code runs

- **Scientists have commenced usage of the portals**
  - Need to determine types of physics codes that can be ported to our portal framework
  - Duration of six months to decide best usage of this technology