Report for the GGF 15 Community Activity: Leveraging Site Infrastructure for Multi-Site Grids

Copyright © Open Grid Forum (2006-2007). All Rights Reserved.

Abstract

This document summarizes the Community Activity "Leveraging Site Infrastructure for Multi-Site Grids" held at GGF 15 on October 3rd in Boston.

Table of Contents

1 Speakers and Talks

This document summarizes the Community Activity “Leveraging Site Infrastructure for Multi-Site Grids” held at GGF 15 on October 3rd in Boston. The list of speakers and talks follows.
Speakers and talk titles:

- Ken Klingstein, I2 "Overview of Campus IT"
- Arnie Miles, Georgetown "Exposing Computational Resources Across Administrative Domains: Condor Shibboleth Integration"
- Jim Basney, NCSA "Integrating MyProxy with Site Authentication"
- Marty Humphrey, U. Virginia "MyProxy integration with Pubcookie"
- Von Welch, NCSA "GridShib: Campus/Grid RBAC Integration"
- David Chadwick, U. Kent "X.509 Privilege Management Infrastructures for Dynamic Delegation of Authority between Sites"
- Abhishek Rana, UCSD "Multi-Site VOs and Multi-VO Sites in Open Science Grid"
- Tom Barton, U. Chicago "Signet and Grouper for Distributed Attribute Administration"
- Dane Skow, FNAL "Experiences with Kerberos-Issued Certificates at Fermilab "

The activity was concluded with a 45-minute discussion session.
A brief summary of the talks follows. Slides are available online at
http://www.ogf.org/GGF15/ggf_events_schedule_MultiSite.htm

1.1 Ken Klingstein

Ken Klingstein kicked off the activity. He gave a overview of virtual organizations and their relevant components. He presented a model for virtual organizations, which included components of users, enterprises, virtual organizations and a virtual organization service center.
Ken also introduced the Shibboleth architecture, project and code base. He noted the original project was web-centric, but is now expanding beyond this space. He discussed current plans for interoperability between Shibboleth and emerging WS-Federation specifications from Microsoft. The inCommon federation built on the Shibboleth technology was also described, including its management and trust models.

1.2 Arnie Miles

Arnie Miles gave a presentation on work to integrate Shibboleth with Condor by allowing Condor to use Shibboleth attributes for access control. He described initial work on a web browser-based client with future plans to enable command-line clients.

1.3 Jim Basney

Jim Basney described recent work to enhance MyProxy with programmable authentication mechanism (PAM) and on-line CA functionality, as well as the successful

application of this to integrate MyProxy with existing site authentication mechanisms in the LTERGrid prototype project and the TeraGrid user portal.

1.4 Marty Humphrey

Marty Humphrey described work to integrate Myproxy with campus authentication through the PubCookie web-based single sign-on mechanisms.

1.5 Von Welch

Von Welch described work to integrate Shibboleth with the X.509 authentication mechanism used in the Globus Toolkit and in most Grid deployments. A beta version of this work is completed and development continues to integrate it with MyProxy to provide a transparent bridge from site authentication mechanisms to X.509 credentials.

1.6 David Chadwick

David Chadwick presented work on a system for managing the delegation of authority for attribute assignment in an X.509 infrastructure based on his PERMIS work.

1.7 Abhishek Rana

Abhishek Rana provided a presentation on the OSG authorization and RBAC infrastructure to support multi-site virtual organizations. This infrastructure utilizes a number of components including GUMS, PRIMA, gPLAZMA, VOMS, SAZ, and authorization callouts from SRM-dCache and the Globus Toolkits.

1.8 Tom Barton

Tom Barton provided a presentation on the Signet and Grouper projects. These tools work together to allow for the administration of groups and their privileges and can be configured to allow for administratively distributed authorities.

1.9 Dane Skow

Dane Skow gave a presentation on the deployment of a Kerberos-based certification authority (CA) at FermiLab and its application for Grid users. He reports that it has proved to be a reliable solution for their needs.

2 Identified Success Stories, Tools and Issues for Leveraging Campus Infrastructure

2.1 Success Stories

The presenters described a number of success stories involving the leveraging of site infrastructure to support multi-site virtual organizations:

- Ken Klingstein showed the inCommon federation with approximately 20 members and the standardization of the eduPerson schema for attribute exchange.
- Jim Basney mentioned the use of MyProxy and PAM to leveraging existing authentication services for the LTER Grid pilot and the TeraGrid user portal.

- Abhishek Rana described OSG's use of RBAC in storage elements and compute elements, pluggable security architectures such as gPLAZMA and the possible integration of the SAZ service at Fermilab.
- Dane Skow described Fermilab's leveraging of their existing Kerberos domain to bridge into Grid X509 authentication system.

2.2 Available Tools, Standards and Technologies

All the presentations had some discussion of a particular tool or tools. We highlight those here.

- Ken Klingenstein described the Shibboleth cross-site identity federaion system and SAML standard that it utilizes.
- Arnie Miles' presentation included a discussion of Condor for high throughput computing and raised the notion of both portals and command-line clients for users.
- Jim Basney described MyProxy as a means of federating between different security domains. Marty Humphrey described work to add support for Pubcookie, a web single sign-on package, to Myproxy.
- Von Welch described the Globus Toolkit and the work by the GridShib project to allow for interoperability between Shibboleth and the Globus Toolkit.
- David Chadwick described PERMIS, an X509-based policy decision engine with dynamic delegation capabilities.
- Abhishek Rana's talk described a number of tools in use in the OSG RBAC architecture, including GUMS, PRIMA, gPLAZMA, VOMS, VOMRS, authorization callouts in the pre-web services version of the Globus Toolkit, authorization callouts in SRM-dCache, and SAZ.
- Tom Barton presented Signet and Grouper, tools for managing and creating policies expressing groups of users and their privileges.
- Dane Skow described KCA/KX509 as the basis for Kerberos-to-X509 bridging at Fermilab.

2.3 Issues and Key Discussion Points

This section lists issues and key discussion points from the activity.

- Privacy: Ken Klingstein mentioned that IBM sees privacy for virtual organizations as a absolute requirement.
- Web Browser versus commandline users: these are very different communities with very different needs. Some systems work well for one, but not for the other.
- Site versus virtual organization authorization: Abhishek Rana raised the issue where do authorization decisions fall between the site and the virtual organization, and the trade-offs involved in this decision.
- VO admin of attribute space: even if sites run services which issue attributes for authorization, virtual organizations will need the ability to administer those

attributes. It may even be the case that sites may not understand the attributes they serve as they are only meaningful to the virtual organization.

- Chadwick mentioned usability issues in crafting security polices in that the use of terminology in GUIs for crafting policies that was clear to non-security personnel often confused security personnel, due to the it being different from what they expected (and it differed from what appeared in the resulting policy).
- Current Grid deployment and implementations don't deal with hierarchies of CAs well.
- Current Grid CA key distributions methods are labor intensive.
- Dane Skow noted that the leveraging of existing names at sites can cause unexpected problems. For example if a user's name changes (e.g. if they get married) this can change their identity in their Grid credentials which will cause identity-based authorization systems to not recognize the user.
- Dane Skow mentioned an issue that services such as an online CA (for which KCA is an example) can be seen as an attractive target since their compromise could allow to the compromise of many user accounts, however in Fermilab's experience over the past ten years without a compromise of this class of tightly secure system indicates this risk is worth taking
- Ken Klingenstein mentioned that science VOs is high benefit communities to campuses.
- Legal entanglements are unavoidable once someone mentions indemnification, then everyone needs lawyers. This should be avoided as long as possible.
- A hypothetical scenario was mentioned of CMS being authoritative for attributes, which are served by a service hosted at U. of Chicago and consumer by Fermilab to make decisions. Where do responsibilities lie in this scenario?
- The question was raised of when we need to define standard for interoperability. Von Welch raised the opinion that these standards are needed when multiple implementations exist that either overlap or complement each other (e.g. a PEP and a PDP). There may also be a need to develop more rigorous trust models addressing liabilities and risks involved in federated security.
- Ken Klingstein mentioned that one implication of the direction of federated identity means all information about a user is not readily available to an application, since it is not in a local DB (the site not autonomous). He also noted that HIPPA and privacy may drive this since it also forces information not to be freely available.

3 Security Considerations

Many of the presentations at the community activity focused on security, however the presentations in this document should be taken as opinions of the presenter and are not recommendations of any OGF working group.

4 Acknowledgements

Tom Barton, Jim Basney, Steven Carmody, Ken Klingensten, Frank Siebenlist, and Von Welch organized the activity.
The editor wishes to thank all the presenters and audience participants for making the activity an interesting and stimulating event.

5 Author Information

Von Welch, Editor
NCSA
vwelch@ncsa.uiuc.edu

6 Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.
The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this recommendation. Please address the information to the OGF Executive Director.

7 Full Copyright Notice

Copyright (C) Open Grid Forum (2006-2007). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the OGF or other organizations, except as needed for the purpose of developing Grid Recommendations in which case the procedures for copyrights defined in the OGF Document process must be followed, or as required to translate it into languages other than English.
The limited permissions granted above are perpetual and will not be revoked by the OGF or its successors or assigns.
This document and the information contained herein is provided on an "AS IS" basis and THE OPEN GRID FORUM DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."