MyProxy: An Online Credential Repository for the Grid

Jim Basney
jbasney@ncsa.uiuc.edu
http://www.ncsa.uiuc.edu/~jbasney/
Grid Portals

• **Allow users to access Grid services using standard web browsers**

• **Need credentials to act on user’s behalf**
  – Standard web browsers don’t support credential delegation
  – The user’s credentials may not be available on the web browser machine
  – Install credentials on each portal in advance?
    – Each portal must be trusted to manage credentials securely
MyProxy

- Secured MyProxy server manages user’s credentials
  - Allows secure access to credentials from anywhere on the Grid
  - Delegates credentials to resources (like web portals) that don’t already support delegation
  - Limits credential exposure with short-lived proxy credentials
• User delegates credential to MyProxy server using MyProxy client program
• User chooses username and pass phrase for credential to protect against unauthorized retrieval
• User specifies lifetime of credential on MyProxy server and lifetime of credentials delegated to Grid Portals
• User connects to the Web Portal at a later time using a standard web browser from any machine
• User provides MyProxy username and pass phrase to the Portal
MyProxy Architecture

• Web Portal contacts MyProxy server and provides user’s username and pass phrase
• MyProxy delegates short-term proxy credentials to Web Portal
MyProxy Architecture

- Web Portal uses the short-term proxy credential to access Grid resources on the user’s behalf

Diagram:
- User
- MyProxy Server
- Grid Portal
- Grid

**Diagram Notes:**
- Arrows indicate the flow of access:
  - From User to MyProxy Server
  - From MyProxy Server to Grid Portal
  - From Grid Portal to Grid
  - From Grid to User
MyProxy Implementations

• C implementation of client and server

• Java Community Grid (CoG) toolkit client implementation
  – http://www.globus.org/cog/

• Grid Portal Development Kit
  – http://dast.nlanr.net/Projects/GridPortal/
MyProxy Deployments

- NCSA (Alliance User Portal, Gaussian portal, Chemical Engineering)
- NASA IPG (Launchpad user portal)
- University of Lecce, Italy (Grid Resource Broker)
- Poznan Supercomputing Center (Web-based resource broker)
- NPACI/SDSC (HotPage)
- UK HPC center
• Convenient, secure access to credentials from multiple sites
  – Without copying credential files by hand
• Unattended proxy credential renewal
  – Submit job to CondorG with pointer to MyProxy server to use for proxy renewal
  – CondorG authenticates to MyProxy server using the current user proxy before it expires
  – MyProxy delegates a new user proxy to CondorG
• **Additional authentication mechanisms**
  – Kerberos (and others?)

• **More control over managed credentials**
  – Restricted delegation
  – Credential access control
    – Which identities can download credentials?
    – What authentication methods are trusted?

• **Multiple credentials per user**
  – Download the credential needed for the current task

• **Standardization**
  – Global Grid Forum and IETF
• **CAS: Community Authorization Service**
  – Allows community members to access community owned/allocated resources
  – Users authenticate to CAS to obtain a “community credential” valid on a resource
  – Interface for community administrators to add/remove users, etc.
• **Alliance User Portal**
  – Built with Grid Portal Development Kit
  – http://aup.ncsa.uiuc.edu

• **NCSA MyProxy server**
  – myproxy.ncsa.uiuc.edu