Managing Disaster Response through On-Demand Resource Federation

Dr. Craig A. Lee, Senior Scientist, lee@aero.org
Dr. Nehal Desai, Senior Engineering Specialist
Andrew Brethorst, Member Technical Staff

The Aerospace Corporation
(a California nonprofit corporation that operates a federally funded research and development center)
The GeoINT Community Cloud Demo
What Did We Learn From All This?

• While managing the sharing access to storage containers is a good first step, it was inadequate to facilitate the secure federation of arbitrary tools, i.e., arbitrary services
  • Managing federated access to *databases* and *RSS feeds* could have been used by GCC participants

• Federation management needed to be generalized to manage any type of service endpoint
  • Cloud infrastructure services (VMs, storage, SDNs) are just services, just like application-level services

• *How can the VO concept be generalized to manage general federations?*
Virtual Organization Abstract Concepts

• A VO is a security and collaboration context not exclusively associated with any one physical organization or site
  – *Participating partners agree upon structure, rules and processes*
  – *A VO partner can be a single person, a group or an entire organization*

• A VO has members that are assigned roles and/or attributes
  – *Membership roles or attributes grant specific capabilities within a given VO as determined by each resource/service provider*

• Partners participating in a VO contribute resources, i.e., data and services
  – *They retain complete control over their own resources!*
  – *Access by VO members can be modified or revoked at any time by both the VO administrator and the resource administrator*

• A VO Management System (VOMS):
  – * Maintains member identity attributes and authorization attributes*
  – *Enables resource (service) discovery*
  – *Enables validation of VO member authz credentials on service invocation*

• Many implementation options and choices necessary
  – *Centralized (third-party) and Distributed (P2P) implementations possible*
General AuthN/Z
AuthN/Z in a Distributed Env

Is it possible to request to SP_B with IdP_A credentials?
Federated AuthN/Z Using a VOMS
General Federation Mgmt Design Requirements

• Client-Side: *Federated Authentication & Service Discovery*
• Server-Side: *Federated Credential Validation & Authorization*
• Centralized, Trusted, Third-Party VOMS
• Proxy VOMS
• Distributed, Trusted, P2P VOMS
• Trust Federations

Diagram illustrates an external, third-party VOMS.
KeyVOMS: A Keystone-based VOMS

- KeyVOMS is a centralized, third-party VOMS
- Re-purposed instance of the OpenStack Keystone v3 service
- Keystone maintains a Service Catalog
  - Used in KeyVOMS as the VO Services Catalog for service discovery
- Keystone v3 Object Model very close to what’s needed
Current Keystone v3 Object Model
with representative object associations (assignments)