MAGIC Meeting Minutes
January 8, 2014

Attendees

Mark Berman	GENI
Marshall Brinn	GENI
Janet Brown	
Rich Carlson	DOE/SC
Bob Cowles	Indiana U.
Chip Elliott	BBN/GENI
Dan Gunter	LBL
Ken Klingenstein	Internet2
Bryan Lyles	NSF
David Martin	Northwestern U.
Grant Miller	NCO
Von Welch	Indiana U.
Steve Zoppi	Internet2

Action Items

Proceedings

This MAGIC Meeting was chaired by Rich Carlson of DOE/SC. Chip Elliott and Marshall Brinn discussed Identity Management for the GENI program.

GENI Background: Chip Elliott

GENI is building large-scale infrastructure at universities throughout the U.S. to support computer science experiments. GENI currently has over 1000 unique users creating GENI slivers. It provides infrastructure for at-scale experiments in networking, distributed systems, security and novel applications. It supports leading-edge research and enables rapid innovation.

GENI enables slices of the network where a user can implement the software he wants throughout the slice including firewalls, routers, clouds, … Each slice is isolated from other slices so multiple internet architectures can be run at the same time on different slices. GENI provides prototype equipment on campuses with students as early adopters and enabling inter-campus applications. The GENI infrastructure provides:

- Flexible network/cloud infrastructure
- Hybrid circuit models including OpenFlow
- Distributed cloud (racks) for content, caching, acceleration…

GENI enables rapid instantiation of network slices for networks on demand. This enables fast spin new protocols, switching strategies, and virtual machines.

GENI and Federated Identity, Authorization, and Resource Management: Marshall Brinn

Federation is cooperation among resource owners and experimenters to provide federations that enable them to share resources confidently. GENI provides software services to facilitate the interactions between the resource providers and experimenters. GENI services include, aggregate managers, GENI Meta-Operations Center, tools, and federation services (Federation API). GENI recognizes two classes of identity:

- GENI-internal: between GENI services they authenticate service invocations via PKI
- GENI-external: For federating with other trusted identity providers, GENI provides tools that bridge external identities to GENI-internal credentials.

The GENI portal is an InCommon Research and Scholarship (R&S) Category service provider. It provides automatic access for users of InCommon Identity Providers that implement the R&S category. User identity is supplemented with GENI-managed attributes, e.g., Project Lead privileges. For InCommon users, they arrive and have immediate access which dramatically reduces the management effort for GENI. For Non-InCommon users GENI manages its own IdP and can add new accounts which are the same as InCommon to the GENI Portal. The GENI Portal has 1071 registered users currently. GENI is also currently federated with café in Brazil.

The GENI federation is facilitated by establishing common trust roots (I accept credentials signed by these entities). A federation also establishes common policies for resource allocation and authorities provide credentials based on the common policies. GENI seeks to assure that all actions on resources are authorized and accountable.

Policy representations in GENI include:

- RBAC: Role Based Access Control, which provides a fixed set of permissions to a given user (slice)
- ABAC: Attribute Based Access Control which provides a dynamic set of permissions based on matching attributes of the user to policy requirements, e.g.,
- - Anyone who is a lead of a slice can add members to that slice
- Attribute assertions: Joe is the lead of slice 'TEST2014'

Some policy statements require additional characteristics:

- Quantity based: Quotas of specific projects, slices, individual, groups
- Time-based: Statements that change with time: e.g., Project A can have 50% of our VMs for 3 weeks and 75% of our VMs after that.

GENI users need tools to speak to the Authority and Aggregate Manager APIs on their behalf: If you give the tools the user's cert/private-key, the tool can 'speak-as' the user but passing keys is bad practice and accountability is difficult... GENI can also 'speak-for' a user if the user authorizes a tool to act on its behalf in some context. The tool provides its own cert/key to authorities and aggregates.

GENI provides the authentication, authorization, allocation, and accountability for resources and users. The resources include:

- Bare metal and virtual machines
- Storage
- Services
- Cross-domain network connections
- Resources for allocation of SDNs

GENI is collaborating with Fed4Fire (EU), and Emulab for standard federation and resource interfaces. GENI is talking to Jim Brothers of Clemson about applying GENI concepts to

support ad hoc VOs. Discussions are ongoing to discuss cross-domain monitoring, forensics and 'manager-of-manager' with limited visibility into individual federations.

For the complete briefings, please see the MAGIC Website for the January 8, 2014 meeting at: http://www.nitrd.gov/nitrdgroups/index.php?title=Middleware_And_Grid_Interagency_Coordination_(MAGIC)#title

Discussion among the MAGIC members identified that:

- InCommon is pushing for additional institutions to release their R&S attributes
- Social identities to SAML interface exists in InCommon
- ABAC attributes do not exist reliably on campuses currently
- InCommon is initiating interfederation with café
- Most of the GENI data is being stored in relational data bases but is moving toward metadata storage.
- Up front efforts to establish Identity Management and federation has provided a basis for easy authentication and authorization in the complex environments we will be using in the longer run.
- GENI identity management is a success but GENI descriptions of resources needs work.

Upcoming Meetings:

February 20-21, perfSONAR Workshop, NSF: By invitation only
Feb 28-29: Operating Innovative Networks (OIN) Workshop Hands-on Training in SDN, Science DMZ, DTNs and perfSONAR: LBL, Berkeley California, **http://www.oinworkshop.com**
April 30-May 1, CCNIE PI meeting at the NSF

Next MAGIC Meetings:

February 5, 2014, 2:00-4:00 EST, NSF
March 5, 2014, 2:00-4:00 EST, NSF