Aggregate Provider Agreement

Document Name: GENI Aggregate Provider Agreement
Version: 0.4.0 (Draft)
Date: Nov. 1, 2011

Introduction

GENI is a federated network testbed designed to allow researchers to experiment with network applications and services that benefit from distribution across a wide geographic area. All uses of GENI should be consistent with this high-level goal.

Aggregate Authorities (AAs), providing aggregates and components operating as a part of GENI, are well-served by having a common set of principles to establish an expected level of service, and methods of cooperation. Such principles, presented in this agreement, benefit the security and stability of the entire GENI suite of infrastructures.

While AAs can operate and protect their resources however they see fit, to acquire the status of "GENI-approved", they are expected to follow the high-level principles described in this agreement. This agreement, like all other GENI federation agreements, is made with the GENI Clearinghouse to reach a common set of expectations between all GENI actors (e.g., experimenters, aggregate authorities, slice owners, identity portals, etc). This agreement does not preclude any bilateral agreements between entities operating in the GENI Federation, but it provides a common framework for cooperation in regards to security incidents and defines the criteria for the label of a "GENI-approved" aggregate, i.e. one listed in the registry at the clearinghouse.

There must be benefits to the Aggregate Authorities if they are expected to seek the "GENI-approved" label for their aggregates. There are three primary reasons why signing should appeal to an AA.

1. An AA knows what to expect of their peers if they interoperate only with other "GENI-approved" aggregates or experimenters who have likewise entered into agreements with the Clearinghouse.
2. "GENI-approved" aggregates could receive official GENI operational services that may be provided in the future (e.g., from the GMOC, the security team, or help desk).
3. AAs agreeing to these principles of operation will be listed in the GENI Clearinghouse.

For an AA to have its aggregates labeled "GENI-approved", they must agree to the Principles of Operation in the following section by signature. The GENI Clearinghouse operator may regularly check that these principles are being followed, but the ultimate arbitrator of any conflicts, resulting either from complaints by other AAs or the Clearinghouse, will be the GENI Governance Group. The full conflict resolution process is described in the GENI Clearinghouse Policy.

Principles of Operation

An Aggregate Authority that agrees to follow the Principles of Operation in this section will face limitations on the degree to which it can control aggregate components and collect information about them. These limitations will vary by aggregate. For example, aggregates that make heavy use of resources from opt-in users may have little or no control of resources being shared by the opt-in user, except to disconnect or allow user's access to GENI. This agreement cannot define principles for every conceivable aggregate, but it is expected that participating AAs will document and share important limitations on their ability to follow the principles in this section.

1. Aggregate administrators agree to advertise their services and status as accurately *as possible*, represent their capabilities fairly, and make their requirements and limitations known.
2. Aggregate administrators agree to maintain the security and stability of the aggregate resources being provided (if under their control), keeping up-to-date on security patches and maintaining audit logs with accurate timestamps so they can better assist the GENI security team or other MAs with investigations. Operators are strongly encouraged to use any hardening guidelines published through the GENI working groups.
3. All services that hold credentials for another party are in a position of trust. Aggregate administrators agree to broker these credentials honestly and not to abuse that trust. It is expected that aggregate operators will take reasonable precautions to protect the security of those credentials and to investigate all reports of compromise of the security of those credentials. The precautions to protect the security of any non-local GENI credentials should be compliant with community recognized best practices and in no event should be less than those applied to similar credentials at the AA's institution.
4. Logs should be maintained for as long as allowed by the AA's institution's retention policies, but the aggregate administrators are not expected to share raw logs. The GENI-CSIRT (Computer Security & Incident Response Team) can provide an aggregate operator with tools to anonymize logs should they desire to share them during the course of an investigation. At a minimum, logs must be detailed enough to map problematic behaviors of an experiment to the correct slice on a component.
5. Aggregate operators agree not to knowingly interfere with the normal operation of any GENI resource under the control of another AA. It is expected that if an aggregate operator is informed that some aspect of their aggregate's presence is creating a problems for other aggregates, then the operator will investigate and make their best effort to promptly resolve the complaint.
6. The GENI community relies upon each AA to stop unacceptable activity originating from resources they provide to GENI. Therefore,

aggregate administrators agree to support the execution of the GENI AUP with regard to the actions of local users on any GENI component. This implies that aggregate operators agree to participate in investigations of GENI security incidents that involve resources under their control.

7. Components in GENI aggregates may be hosted by organizations which do not own or manage the aggregate. For example, a campus may install a shared compute resource from a GENI AA in order to give students at the campus access to that resource. A host organization may receive third party complaints or intrusion alerts about the GENI component that require action on the part of the AA. The AA agrees to provide the group(s) responsible for infrastructure and security at the host organization with a point of contact to assist the host organization in responding to reported problems.
8. Aggregate operators agree to *privately* notify the GENI-CSIRT of all security-related complaints about their aggregate so that trends and new attacks can be detected more quickly. This does not preclude AAs from responding directly to such complaints about their aggregates in any way.
9. As it is necessary to respond to incidents in a timely fashion, there must be clear channels of communication. Therefore, aggregate operators agree to keep accurate and up-to-date contact information with the GMOC (GENI Meta-Operations Center). This contact information must be for someone who is responsive, knowledgeable of the aggregate's operation, and able to shutdown that aggregate or block the offending component in an emergency.
10. Aggregate operators should inform the Clearinghouse of any planned or unplanned outages lasting more than 24 hours, and will inform the Clearinghouse of any permanently retired components.
11. Aggregates will inform the Clearinghouse of resource allocations granted to GENI slices (those registered with the clearinghouse) through a method provided by the Clearinghouse so that federation-level allocation policies can be verified.
12. Aggregate operators will provide to the GMOC a list of public IPs that may be used by slices running on their components. This so the LLR representative can rule out supposed complaints about GENI resources as early as possible in the process and not trouble aggregate operators needlessly.

Glossary

- **Aggregate**: is a system containing a collection of resources (i.e. components) under common administration running an aggregate manager service (defined in the GENI Software Framework Architecture).
- **Aggregate Administrator:** is one who has been delegated the responsibility, by the aggregate authority, to set local resource allocation policy for an aggregate and its components.
- **Aggregate Authority (AA):** is responsible for the management of the aggregate, but can delegate selected functions to other actors. The aggregate authority is the one who can enter into agreements for the aggregate.
- **Aggregate Manager:** a service that exports a well-defined remotely accessible control framework interface to an aggregate.
- **Aggregate Operator:** is appointed by the Aggregate Authority to operate the Aggregate Manager and any components of the aggregate. This may be a the AA itself, or someone from another organization operating on its behalf.
- **Component:** encapsulates a collection of resources, including physical resources (e.g., CPU, memory, disk, bandwidth) logical resources (e.g., file descriptors, port numbers), and synthetic resources (e.g., packet forwarding fast paths).