gMOC
GENI META-OPERATIONS CENTER

Spiral 2 Emergency Stop

(Draft V4)

Summary

One of the essential early operational requirements for the GENI facility is the need to manage and coordinate the stop and/or containment of GENI resources among all GENI projects in the case of an urgent request. Emergency stop is the system used to respond to incidents of interference or resource exhaustion caused either unintentionally (misconfiguration), or intentionally (malware). This is intended to protect GENI aggregates when they begin to integrate with other aggregates, and when GENI begins to interconnect with outside networks.

For Spiral 2, GENI aggregates will have active experimentation and increased integration and interconnection with other aggregates or non-GENI networks. This document will provide an approach for an early emergency stop service in Spiral 2, as well as a potential evolution for emergency stop for future spirals.

Spiral 2 Emergency Stop Model

In Spiral 2, the GENI Meta-Operations Center is tasked with developing, prototyping, and providing an early emergency stop process for GENI. This service prototype is expected to present the basic functionality needed by the early active experimenters on GENI while remaining lightweight and simple.

Overview

The early emergency stop system has 3 main goals:

1. To give experimenters and other GENI stakeholders a single place to go for notification of emergency stop issues
2. To facilitate emergency stop with GENI aggregates for the most severe issues on behalf of authorized users
3. To provide a basic, functional model, easily understood by GENI stakeholders and which can be extended for the future as requirements evolve.

The Early Emergency Stop system will accomplish these goals through two mechanisms:

1. An initial coordination process to identify related GENI aggregates and/or slices for a given stop request, notify appropriate GENI aggregate managers, facilitate communication among GENI users and GENI aggregate managers, verify ultimate resolution of the issue, and reporting of emergency stop issues to the GENI operational community.
2. A last resort isolation mechanism using the existing Internet2 and NLR GENI donations to effectively quarantine aggregates with issues from the rest of the GENI infrastructure.

This early emergency stop system will be coarse, time intensive, and potentially drastic, if isolation is required. Nevertheless, it will provide a basic operational safety net to ensure overall stability of the GENI facility and will give experimenters the ability to request action from a single GENI contact and ensure that the right GENI parties are notified.

Emergency Stop Participants & Stakeholders

GMOC – GMOC will provide the "front door", communication (internal and external to GENI), coordination, tracking, and reporting for emergency stop issues. GMOC will also directly operate the interconnections among aggregates, to isolate issues as a last resort.

Aggregate Managers – Aggregate Managers bear operational responsibility for their aggregates and thus will be responsible for timely response to emergency stop requests. Response will include investigation of the issue, and intervention/shutdown of the source of the issue, if the aggregate manager confirms the issue. Aggregate managers will also be responsible for reporting their findings and results back to GMOC for tracking & reporting purposes.

GENI-Interconnected Networks & Experimenters – Spiral 2 experimenters and GENI-interconnect networks will be responsible only for reporting problems that may require emergency stop to GMOC, and for providing as much information about the issue as possible.

Emergency Stop Triggers

In Spiral 2, emergency stop should be limited to the cases that would most likely require it in the near term. In Spiral 2, no direct detection of emergency stop triggers is anticipated. There are 3 main types of stop triggers, reported by GENI aggregate managers, users, or other outside parties:

1.) reported cases in which an aggregate's resources are being exhausted or in which an aggregate is being otherwise adversely affected by traffic from another aggregate
2.) reported cases from external networks, such as campus operators, production research & education networks, or international peers in which these networks are being improperly affected by GENI resources
3.) cases of requested legal action (e.g. Cease & Desist, subpoena, AUP violations) based on the content or actions within a GENI slice.

In these cases, these parties should request emergency stop action through a well-known GENI stop contact (phone and email). If such a request comes to aggregates, aggregates should redirect these requests to this GENI stop contact, unless the requests are limited to the aggregate and so are unrelated to the GENI facility as a whole.

If it is necessary to limit the parties who may request stop action, the appropriate policies must be developed.

The GENI Operational Contact List

To serve as a coordinator for emergency stop, GMOC will require a contact list for contacting the appropriate GENI aggregates for these issues.

The GENI operational contact list should consist of 2 contacts for each GENI aggregate: an initial contact or list to receive notification of an emergency stop request and a contact or list to receive escalation notifications of emergency stop requests. Contacts will need to have both an email and phone number.

In the long-term, the data for this list could exist at the GMOC, in each participating project, at the GPO, or kept in some type of distributed system. The list must meet two requirements: it must have a mechanism to ensure the data is accurate and it must be available whenever it's needed. In order to keep it highly available to the GMOC, the initial list of contacts should be kept within the GMOC's database. If another system comes about which can meet these requirements in a different way, this may change in the future.

Stop escalation contact emails may also be provided using designated GENI aliases, (e.g. stop-gpeni@geni.net). This would allow each project to directly manage the alias while allowing a consistent contact email for GMOC.

Depending on the requirements or policy for limiting emergency stop requests, a contact list of authorized parties would also be required.

Security Implications for Emergency Stop

In Spiral 2, the emergency stop system will require a basic system to ensure authentication of the manual contacts among the GENI parties. This will consist of a simple callback mechanism for the contact between GMOC and aggregate managers. As contacts for authorized

Correlation of Requests to Aggregates

One of the challenges for this prototype will be connecting a stop request to the appropriate related projects, in the absence of a unique GENI identifier for a slice that GMOC could use to identify the projects providing resources.

This is one of the reasons to limit emergency stop in Spiral 2 to the most severe, facility-affecting and legal-action cases.

In Spiral 2, GMOC will still be working to gather the rich operational data from the GENI projects that will provide the mapping of slivers and slices to aggregates. So, during this period, appropriate contact will be made on a best effort, erring on the side of too much contact rather than too little. As GMOC begins to gather more data relating slices to components, and as GENI identifier issues begin to mature, GMOC will be able to make these connections in an increasingly more accurate and precise way.

Response Time Expectations & Escalation Path

Response Expectations - early emergency stop will be limited to the most severe and urgent cases, so timely response by aggregate managers will be crucial. Because of this, appropriately notified parties should provide acknowledgement of an emergency stop request (but not necessarily issue resolution) within one business hour.

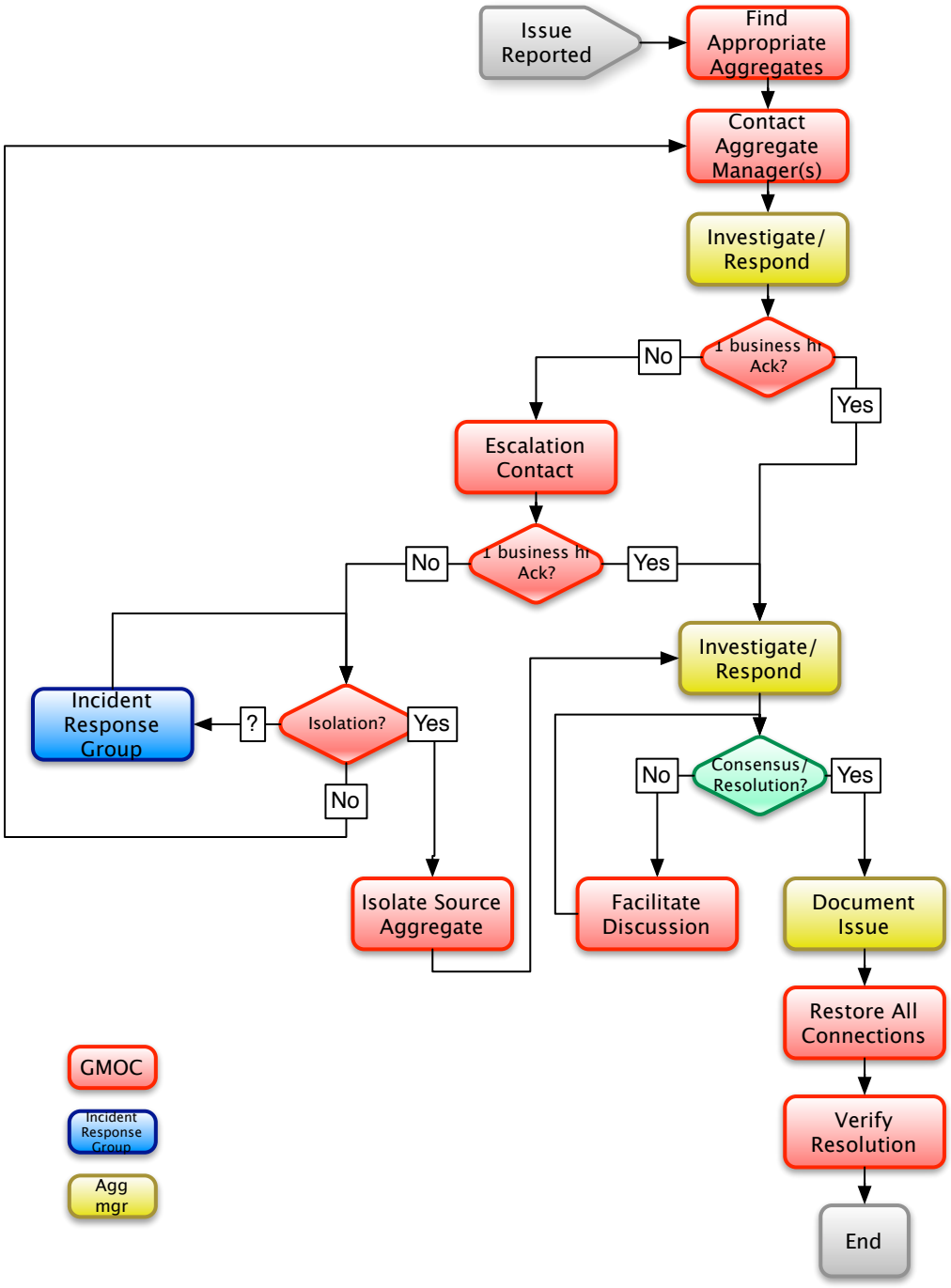
Initial Escalation - If GMOC receives no acknowledgement from notified parties in the appropriate time frame, GMOC will escalate to the escalation contact for that project (or its PI). GMOC will then wait another business hour for the response for the project.

Quarantine - If no acknowledgement is received after initial escalation, a decision will need to be made about whether to contain the aggregate that is the suspected source of the issue. If it is decided that containment is proper and feasible, GMOC will either directly contain the aggregate or request that containment.

This decision will require a set of policies defined by the GENI community used to make the decision. In cases where the policies are not well defined, a small incident response group made up of representative GENI stakeholders should be tasked with making the judgment about that particular case. This group's participants and expectations must also be well defined.

User Expectations - This means that issue reporters should expect some issue acknowledgment or response by two business hours from the reported time for emergency stop request. Timeframes for the actual resolution of issues is not guaranteed and users must be aware of this.

A figure of this process can be seen here:



The effectiveness of this process will depend on 3 things:

1. The quality of contact information and data to relate contacts to the aggregate or slice data provided by those reporting issues.
2. Widespread understanding among GENI projects and users of the overall process and use cases.
3. Understanding within the GENI community about expectations and roles

Post Spiral 2 Emergency Stop

Evolution of the Spiral 2 emergency stop system will depend largely how GENI as a whole evolves. However, five areas of improvement seem likely:

1. *Isolation on Slice Level vs Aggregate Level* – significant interactions between GMOC and project operations teams will help to give better information to make stop actions less intrusive
2. *Better correlation of requests to the appropriate related projects and components* – as GENI evolves, GMOC will make use of better and more consistent data to make faster more accurate correlation between Emergency stop requests and the related projects
3. *Some development of automated interactions* – interact with interested projects in better ways to automate the process of issue tracking and resolution, exploring the issues surrounding automated control plane access for emergency stop.
4. *Improved security (authentication and authorization)* – better integrated and fully featured mechanisms to verify requests, so that users can be authenticated in some way.
5. *Expanded Triggers for Emergency Stop* – Additional cases for emergency stop may be added as needed.