

Emergency Shutdown

Early Implementation and Potential Evolution

Summary

One of the essential early operational requirements for the GENI facility is the need to manage and coordinate the shutdown and/or isolation of GENI resources among all GENI projects in the case of an urgent request. This emergency shutdown is needed for any system that could might adversely impact other systems on the GENI facility or interfere in an unintended way with any slices on GENI. For interconnected networks/systems this is even more important as these complex systems can be potentially misbehave unintentionally (misconfiguration, unexpected effects) or intentionally (malware), causing a negative impact on other interconnected systems.

As of July 2009, many GENI cluster/services are just starting to make resources available to experimenters. This document will explain how GENI should approach emergency shutdown at this early prototyping period, as well as how it should likely evolve as the GENI facility evolves.

Early Emergency Shutdown Model

By November 2009, the GENI Meta Operations Center will start providing an early Emergency Shutdown 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.

The Early Emergency Shutdown system has 3 main goals:

1. To give experimenters and other GENI stakeholders a single place to go for notification of emergency shutdown issues
2. To be able to facilitate shutdown with GENI federates for the most severe issues on behalf of authorized users;
3. To provide a basic, function model that will be easily understood by GENI stakeholders and which can be extended for the future if requirements evolve.



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

1. A process to identify related federates for a given shutdown request, notify appropriate GENI federates of any urgent intrusive issues, facilitate communication among GENI users and GENI federates, and verify the ultimate satisfaction of the GENI users requesting a shutdown.
2. An isolation mechanism using the existing Internet2 and NLR GENI donations to effectively separate projects with issues from the rest of the GENI infrastructure as a last resort.

This early Emergency Shutdown process will be fairly 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 shutdown Cases

In the first year, GMOC expects three emergency shutdown cases: Emergency shutdown of a project, emergency shutdown of the GENI Internet2 interconnect, and emergency shutdown of a node within a project. However, given the limited capabilities of the current GENI control plane, GMOC's only controlled actuator would be the disconnection of the GENI Internet2/NLR interconnects. For all other cases GMOC would serve as a facilitator for the involved individuals and/or institutions.

The GENI Operational Contact List

The GENI operational contact list will consist of 2 contacts for each GENI project: an initial contact or list who will receive notification of an emergency shutdown request and a contact or list which will receive escalation notifications of emergency shutdown requests. Initially, each contact will need to have both an email and phone number associated with it.

In the long-term, the data for this list could exist at the GMOC, in each participating project, at the GPO. Two challenges exist for this list: how to keep the data accurate and how to make it easily available from GMOC's perspective. In order to keep it highly available to the GMOC, initially the database and/or an



automatically updatable copy should be kept at the GMOC. Shutdown and shutdown escalation contact emails may also be provided using designated GENI aliases, (e.g. shutdown-gpeni@geni.net). This would allow each project to directly manage the alias while allowing a consistent contact email for GMOC.

Correlation of requests to appropriate projects

One of the challenges for this early prototype will be connecting a shutdown 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 initially limit Early Emergency Shutdown to the most severe facility-affecting cases.

To start, GMOC will make a best effort to contact the appropriate projects, 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 develop, GMOC will be able to make these connections in an increasingly more accurate and precise way.

Response Time, Expectations and Escalation

In the case of GENI we initially expect to limit Emergency shutdown to the most severe and most urgent cases, so timely response will be crucial. Because of this, appropriately notified parties should provide acknowledgement of an emergency shutdown request (but not necessarily issue resolution) within one business hour.

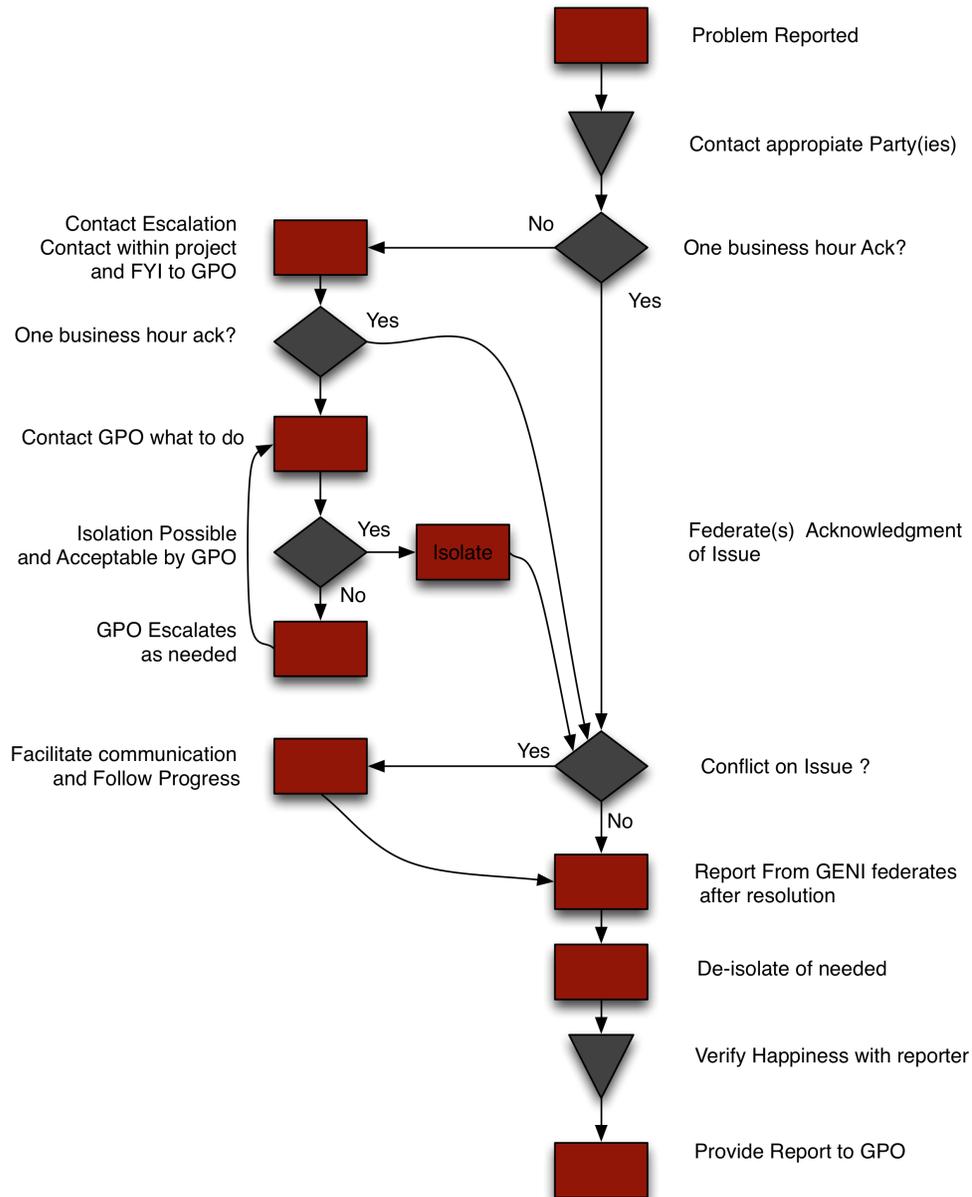
If GMOC receives no acknowledgement from notified parties in the appropriate time frame, GMOC will escalate to the escalation contact for that project (or its PI) and notify the GPO of that such escalation took place. GMOC will then wait another time frame for the response for the project.

If no acknowledgement is received after escalation, GMOC will escalate directly to the GPO and if isolation of the project is a reasonable option will also ask the GPO if GMOC should isolate the project. GMOC will wait for the GPO and/or the appropriate project contacts to proceed with the issue. There will be no isolation without GPO permission.

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

If there are conflicts or question about whether an issue warrants a shutdown, GMOC will facilitate communication between the involved entities.

A figure of this process can be seen in figure 2:



The success of this process will depend on 3 things:

1. The quality of contact information and data to relate contacts to slices
2. The widespread understanding among GENI projects and users of the process.

3. A clear understanding among GENI projects and users of what constitutes a legitimate case to trigger the Emergency Shutdown process

Future Emergency Shutdown Model

Evolution of the Early Emergency Shutdown system would largely be based on how GENI as a whole evolves, and the requested services as users begin to use GENI. However, five areas of improvement seem likely:

1. **More granularity in what gets shutdown** – significant interactions between GMOC and project operations teams will help to give better information to make shutdowns 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 shutdown 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 fully automated control plane access for shutdown.
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 Cases for Emergency Shutdown** – Additional cases for shutdown may be added as requested.