

Aug 16, 2012

GENI - Emergency Stop Procedure Workflow (Spiral 4)

1. Issue Reported

GPO, GENI LLR (Legal Law-Enforcement Representative) or a GENI Experimenter will contact the GMOC to request an Emergency Stop

1.1 Create an Emergency Stop ticket

GPO or other entity will contact the Service Desk requesting an Emergency Stop. GMOC Service Desk will create an Emergency Stop ticket via Quick Ticket template in the GMOC ticketing system. Collect all pertinent information (check for contact information in the GMOC Database):

- Requestor Organization
- Requestor Name
- Requestor Phone Number
- Requestor Email
- Requestor Location*Optional
- Slice Name or a portion of the experiment

Assign GMOC Service Desk for tracking the issue until final resolution; paying close attention to the Escalation Times. Assign GMOC Network Engineering to the ticket and contact the engineer immediately by phone.

1.2 Verify Identity/Callback

In each case, GMOC will verify rights and identity of the requester (authentication and authorization via GMOC DB look-up and callback)

- If the request comes in to GMOC via email, GMOC Service Desk will look up the email in the GMOC DB and call the person back to verify identity
- If the requestor calls in, GMOC Service Desk will gather the contact information and cross-reference the GMOC DB to verify identity

1.3 Is there good reason to initiate an emergency stop?

There are two primary reasons for initiating an emergency stop procedure.

- a. An experimenter's experiment not responding or negatively affecting other experiments.
- b. Flooding of traffic is the second reason, whether that comes from a bad experiment or more likely a loop causing broadcast storms.

2. Investigate/Respond

2.1. Isolation?

If the decision is made to perform isolation, the method of least disruption will be considered and implemented whenever possible.

2.2. Identify Source Aggregate

The ingress of the offending traffic can be identified most likely in two ways;

- a. Identified by network observation, unexpected (high) utilization on links facing GENI participants.
- b. Experimenter or GPO identifies which traffic should be stopped.

The offending ingress port is fairly easy to find, simply observing the input counters of the switches will lead you back to the source. The GPO is always helpful in identifying the source and may even have the traffic isolated before an engineer investigates.

3. GMOC Engineers Isolate

3.1. If Isolation is approved

GMOC will try and isolate the experiment without disruption to the Backbone. If successful then GMOC will proceed to Step 6.

4. If GMOC unable to isolate

4.1. Contact Appropriate Experimenters and Aggregate(s) GENI - Emergency Stop Procedure Workflow (Spiral 4)

4.2. Find and Contact Appropriate Experimenter and Aggregate(s)

GMOC will use the Operational data-set in the GMOC DB to find contact information for contacting both the appropriate Experimenter and Aggregate Operator.

NOTE:If an Experimenter or Aggregate Operator would like to authenticate GMOC for stop requests, they should use a callback procedure. After being contacted by someone claiming to be the GMOC, the Aggregate Operator may call the GMOC back using the published GMOC phone number, and ask to speak to the requester who made the initial contact. Using a callback process for GMOC authentication is optional, left to each aggregate operator to decide.

4.3. One Hour Acknowledgement?

Appropriately notified parties should provide acknowledgement of an Emergency Stop request (but not necessary issue resolution) within one hour. - If no acknowledgment is received, GMOC will send a request to the escalation contact for the Organization in question.

4.4. Escalation Contact

After one hour, if there's no response from the Primary contact for an Experimenter or Aggregate Operator, contact the Escalation Contact for the Organization that is documented in the GMOC Database.

-If no acknowledgement is received after one hour of 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 directly contain the aggregate from the backbone. For Spiral 4, GMOC will make these decisions based on the severity of the situation and the anticipated side effects of the isolation on the Backbone. These decisions can be reviewed and improved.

5. Implement

5.1. Stop Offending Traffic/Experiment

The identified traffic can be excluded the following ways;

- a. Aggregate Operator stops the experiment
- b. Shutdown the ingress port on the GENI Openflow Backbone
- c. In the case of shared infrastructure, remove the associated VLAN from the ingress port
- d. Participant shuts down their egress port to the GENI OpenFlow Network

5.2. Perform Isolation

The identified traffic can be excluded the following ways;

- a. Shutdown the ingress port on the GENI Openflow Backbone
- b. In the case of shared infrastructure, remove the associated VLAN from the ingress port.
- c. Participant shuts down their egress port to the GENI Openflow Network.

6. Consensus/Resolution

6.1. Document and Update GMOC

Aggregate Operator should document the issue and contact the GMOC and/or GPO with resolution to verify success of the Emergency Stop.

6.2. Facilitate Discussion

GMOC can help facilitate discussion between Aggregate(s), GPO and Experimenter(s). GMOC (gmoc@gnoc.iu.edu) should be included and stay in the loop on any developments so they can serve as the single place of contact for latest information about an ongoing issue.

6.3. Verify Resolution

Anytime ingress traffic is removed the network, the engineer acting upon the request should verify with GPO the success or failure of the actions taken.

GMOC Service Desk can help facilitate communication between Aggregate Operator, GMOC Engineering team(s) and GPO. It is best to keep GMOC (gmoc@grnoc.iu.edu) in the loop on all communication so this can be tracked in the ticketing system and that there's always a central place of information availability in case of questions/concerns.

6.4. Safe to Restore

Initially GPO should confirm whether the isolation actions performed by Aggregate Operator or GMOC on the OpenFlow Backbone fixed the problem. Eventually as tools/workflows improve GMOC should have this responsibility.

7. Complete

7.1. Restore All Connections

Once the source of the offending traffic is identified and removed, the emergency stop should be reversed and traffic allowed to ingress the GENI Openflow Backbone.

7.2. Document Issue / Close Ticket

GMOC will document the events and evaluate results or the Emergency Stop:

- note any down-times and affected elements on the GENI OpenFlow Backbone
- Update GMOC DB with any missing information for requester or Operator.
- evaluate criteria for isolation (say, we didn't isolate something that we should in the future)
- send any final notifications of resolution
- close the ticket

GENI - Emergency Stop Procedure Workflow (Spiral 4)06272012 Updated - Last modified on Aug 16, 2012 9:58 AM

