

The Careful Puppet Master

Reducing risk and fortifying acceptance testing with the
Jenkins Continuous Integration system

Jason A. Smith
RHIC & ATLAS Computing Facility
Brookhaven National Lab

Old Way: Manual Testing

- Approval system shows only Git branch history & diff.
 - Manual review to ensure things look OK before merge.
 - Mandatory 5 minute delay to review & approve changes
- Rely on people manually testing production changes, and asking others to test large or core changes.
 - Delays waiting for people to manually test changes.
 - Not reliable since people might not test every variation.
- Last summer we recruited a student from the DOE SULI (Science Undergraduate Laboratory Internship) program to work on an automated testing system.
 - Successful prototype established during the 10 weeks. ²

Manual Production Approval

Main Production Approvals

Date	Age	User	Environment	Changes	Changelog	Approve	Reject
Fri Feb 6 15:00:10 2015	1 month	John DeStefano	production	diff	pending-production-13e8e80-20150206T200010UTC	merge	delete
Fri Mar 13 16:10:13 2015	1 week	Zhenping Liu	production	diff	pending-production-13e8e80-20150313T201013UTC	merge	delete
Tue Mar 17 11:11:46 2015	1 week	Jason A. Smith	production	diff	pending-production-13e8e80-20150317T151146UTC	merge	delete
Tue Mar 24 16:06:26 2015	2 minutes	Jason A. Smith	production	diff	pending-production-13e8e80-20150324T200626UTC	merge	delete

Instructions:

- The table above lists all changes to puppet's production environment that are currently pending approval.
- The diff link in the Changes column uses the cgit interface to display the detailed changes to all files contained in that pending update.
- The branch link in the Changelog column uses the cgit interface to display the commit history of that branch since it diverged from production.
- Use the merge link in the Approve column to accept the changes and merge them into production.
- Note: You must wait at least 5 minutes before you are allowed to approve your own changes, or you can ask someone else to approve them immediately.
- Use the delete link in the Reject column to delete the branch if you do not want it merged into production.
- Email notifications are sent after confirmation of the chosen action.
- A side effect of this approval process is that you might see a lot of these old temporary pending branches accumulate in your locally cloned git repo. You can clean these up by using the "git remote prune origin" command.

If you think that one of puppet's environments is out of date, you can force a resync from git:

You can also view the complete difference between the **production** and the branch:

Approval Committee

User	Name	Email	Authorization	Dynamic Production
[redacted]	Carlos Gamboa	[redacted]	^storage/.*	None
[redacted]	Hironori Ito	[redacted]	^storage/.*	None
[redacted]	Christopher H. Hollowell	[redacted]	All	farm
[redacted]	John DeStefano	[redacted]	All	None
[redacted]	Tejas Rao	[redacted]	^gce/.*/ ^hpss/.*	None

Manual Review & Merge

Are you sure you want to merge your own pending changes for the production environment shown below Jason A. Smith?

Please review the changes below, you must scroll to the bottom before you can confirm (javascript required).

File(s) touched by this merge request:

```
4 files changed, 279 insertions(+), 187 deletions(-)
M    gce/dovecot/files/10-ssl.conf
M    gce/dovecot/manifests/init.pp
M    gce/email/manifests/init.pp
M    gce/postfix/manifests/init.pp
```

Change(s) to be merged:

```
diff --git a/gce/dovecot/files/10-ssl.conf b/gce/dovecot/files/10-ssl.conf
index 1b35215..9d40219 100644
--- a/gce/dovecot/files/10-ssl.conf
+++ b/gce/dovecot/files/10-ssl.conf
@@ -23,7 +23,7 @@ ssl_key = </etc/pki/mail/private/hostkey.pem
 # PEM encoded trusted certificate authority. Set this only if you intend to use
 # ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
 # followed by the matching CRL(s). (e.g. ssl_ca = </etc/pki/dovecot/certs/ca.pem)
-ssl_ca = /etc/pki/mail/globalsign-ca.crt
+ssl_ca = </etc/pki/mail/globalsign-ca.crt

 # Request client to send a certificate. If you also want to require it, set
 # auth_sasl_require_client_cert=yes in auth section
```

Optional comments (for git log and email notification):

Yes

No

Automated Testing

- Many types of testing exist (unit, acceptance & integration).
- RSpec unit testing to automate individual module tests.
 - Basically rewriting Puppet module in the ruby RSpec language so the tests can examine your module for proper functionality.
 - Usually used as first line of tests to ensure the module will still function as intended after modification, updating or refactoring.
- Serverspec uses RSpec to perform acceptance tests of modules by running the module code locally or ssh to VM.
 - Verify that the module did what it was supposed to do.
 - Things like: package installed, service running, port listening.
 - Like unit tests, usually used at the individual module level to help ensure modifications and updates don't break your module.

Automated Testing cont'd

- Beaker is another acceptance testing system that also does VM provisioning, and supports several VM backends.
 - VMWare, EC2, vSphere, Vagrant, GCE, Docker, Openstack, Zones
 - Workflow: provision → validate → configure → test → revert → cleanup & report results
- Jenkins is a Continuous Integration system used to automate testing of software projects.
 - Basically a job scheduling & management system.
 - Usually a SCM commit or push hook will build/compile the entire software project and run various tests.

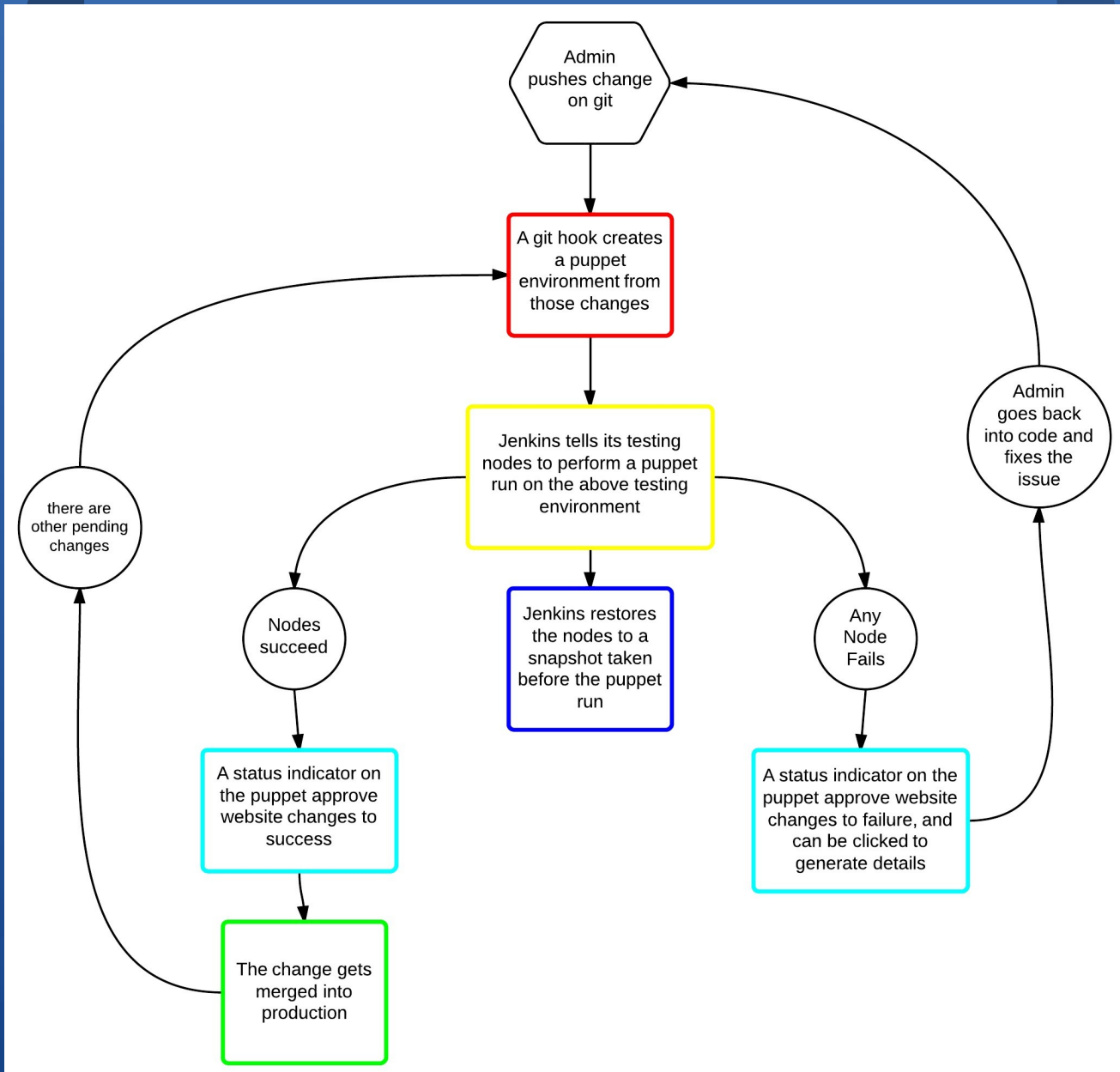
Jenkins CI

- For automated testing of pending production changes made to our Puppet catalog we decided to use the Continuous Integration method and run tests at the full host catalog level on a pool of VMs.
- Use the generic scheduling & management features of Jenkins to schedule test jobs on a pool of slave VMs.
- Catch potential problems/conflicts between modules and system-wide issues that the *Spec tests cannot.
- VM test pool represents all critical services.
- Only pending branches that successfully pass the Puppet agent test run on all VMs are allowed to be merged into production.

Production Approval & Jenkins

- Already had Git push hooks to trap pushes to production so they could be manually reviewed and approved for merge.
- Hooks and approval scripts modified to kick off test Puppet agent run of the pending branch, must pass on all VMs.
- Push starts 4 jobs to test the branch, managed by Jenkins:
 1. Sync Git branch to Foreman as known environment (puppet:import:puppet_classes[\$ENV,batch] rake task).
 2. Assign VMs in Jenkins slave pool to test environment (Foreman server REST API).
 3. Run the Puppet agent test on each VM, with optional 2nd idempotent test (no changes made during the 2nd run).
 4. Reset VMs to pre-test state (RHEV REST & shell API).

Jenkins Process



Using Jenkins



- Approval script will only allow production merges if the Jenkins tests passed for the pushed branch. If testing is in progress then have to wait until finished. If testing failed then merge is never allowed.
- If multiple branches are pending approval and one is merged, then that change is also merged into the remaining pending branches and retested by Jenkins.
- All testing is automated, the only manual process is getting the staff to populate pool of RHEV VMs with a good representation of important production services and hosts.

Approval Changes

Git/Puppet updates to production that are pending approval.



Hello Jason A. Smith, there are currently 2 changes waiting for approval:

Main Production Approvals

Date	Age	User	Environment	Changes	Changelog	Status	Approve	Reject
Wed Mar 25 11:49:21 2015	2 hours	Jason A. Smith	production	diff	pending-production-██████████-3e6f59b-20150325T154921UTC		merge	delete
Wed Mar 25 14:24:20 2015	10 minutes	Jason A. Smith	production	diff	pending-production-██████████-3e6f59b-20150325T182420UTC		merge	delete

The final result for all slaves is: FAILURE

Results for pending-production-██████████-3e6f59b-20150325T182420UTC [build # 1]

Jenkins Test Host	Status	Timestamp	Puppet Report	Puppet Output
██████████.bnl.gov		03/25/15, 14:25:20	foreman reports	jenkins console
██████████.bnl.gov		03/25/15, 14:25:20	foreman reports	jenkins console

For more details, visit the [Jenkins dashboard](#).

[Go back to the puppet approve page.](#)

Merge Verification

Checking the Jenkins test results.... **Passed!**

Are you sure you want to merge your own pending changes for the production environment shown below Jason A. Smith?

Please review the changes below, you must scroll to the bottom before you can confirm (javascript required).

File(s) touched by this merge request:

```
1 file changed, 1 insertion(+), 1 deletion(-)
M       gce/ganglia/manifests/init.pp
```

Change(s) to be merged:

```
diff --git a/gce/ganglia/manifests/init.pp b/gce/ganglia/manifests/init.pp
index 5d5ddd5..38b5e24 100644
--- a/gce/ganglia/manifests/init.pp
+++ b/gce/ganglia/manifests/init.pp
@@ -62,7 +62,7 @@ class ganglia {
}
```



Checking the Jenkins test results.... **Failed!**

The job to test pending-production-██████████-3e6f59b-20150325T182420UTC did not succeed in jenkins, the status of the nodes that ran the test is below.

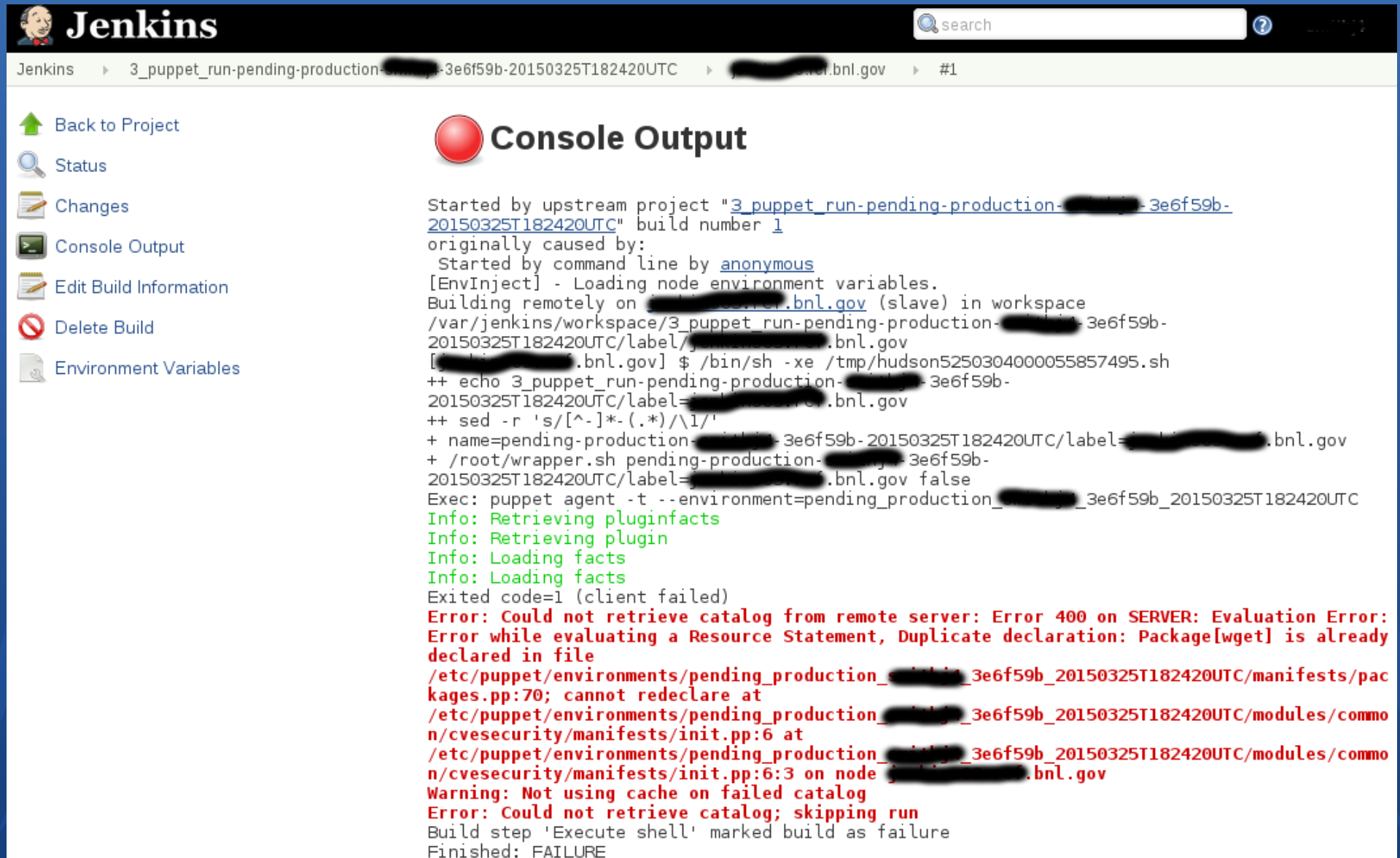
You cannot merge a change that failed jenkins testing! Please fix the cause of the failure and resubmit your branch.

The final result for all slaves is: FAILURE

Results for pending-production-██████████-3e6f59b-20150325T182420UTC [build # 1]

Jenkins Test Host	Status	Timestamp	Puppet Report	Puppet Output
██████████usatlas.bnl.gov		03/25/15, 14:25:20	foreman reports	jenkins console
██████████rcf.bnl.gov		03/25/15, 14:25:20	foreman reports	jenkins console

Jenkins Console



Jenkins ?

Jenkins > 3_puppet_run-pending-production-**[REDACTED]**-3e6f59b-20150325T182420UTC > **[REDACTED]**.bnl.gov > #1

- Back to Project
- Status
- Changes
- Console Output
- Edit Build Information
- Delete Build
- Environment Variables

Console Output

```
Started by upstream project "3_puppet_run-pending-production-[REDACTED]-3e6f59b-20150325T182420UTC" build number 1
originally caused by:
  Started by command line by anonymous
[EnvInject] - Loading node environment variables.
Building remotely on [REDACTED].bnl.gov (slave) in workspace
/var/jenkins/workspace/3_puppet_run-pending-production-[REDACTED]-3e6f59b-20150325T182420UTC/label=[REDACTED].bnl.gov
[REDACTED].bnl.gov] $ /bin/sh -xe /tmp/hudson5250304000055857495.sh
++ echo 3_puppet_run-pending-production-[REDACTED]-3e6f59b-20150325T182420UTC/label=[REDACTED].bnl.gov
++ sed -r 's/[^-]*-(.*)/\1/'
+ name=pending-production-[REDACTED]-3e6f59b-20150325T182420UTC/label=[REDACTED].bnl.gov
+ /root/wrapper.sh pending-production-[REDACTED]-3e6f59b-20150325T182420UTC/label=[REDACTED].bnl.gov false
Exec: puppet agent -t --environment=pending_production_[REDACTED]_3e6f59b_20150325T182420UTC
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Loading facts
Exited code=1 (client failed)
Error: Could not retrieve catalog from remote server: Error 400 on SERVER: Evaluation Error: Error while evaluating a Resource Statement, Duplicate declaration: Package[wget] is already declared in file
/etc/puppet/environments/pending_production_[REDACTED]_3e6f59b_20150325T182420UTC/manifests/packages.pp:70; cannot redeclare at
/etc/puppet/environments/pending_production_[REDACTED]_3e6f59b_20150325T182420UTC/modules/common/cvesecurity/manifests/init.pp:6 at
/etc/puppet/environments/pending_production_[REDACTED]_3e6f59b_20150325T182420UTC/modules/common/cvesecurity/manifests/init.pp:6:3 on node [REDACTED].bnl.gov
Warning: Not using cache on failed catalog
Error: Could not retrieve catalog; skipping run
Build step 'Execute shell' marked build as failure
Finished: FAILURE
```

Miscellaneous

- Monthly Jenkins job to update slave VM snapshots.
 - Yum update, Puppet base config update & Jenkins slave.jar update, then update RHEV VM snapshot.
 - Last major TODO item is to automate the process of reclassifying the Jenkins slave VMs using only our base class during this update, then revert back to their normal classification data for future testing.
- Cleanup Jenkins history
 - delete old Jenkins job results.

Future Plans

- Add Jenkins to our production Puppet Master server.
 - Need staff to setup the pool of test VMs that have critical Puppet modules & services configured on them.
- Look into the possibility of adding service/host validation tests to verify that everything is still working properly after the Puppet agent runs.
 - Could use a monitoring tool like Nagios/Icinga or maybe Serverspec to verify that the resulting Puppet agent run performed as expected (software is installed, configured & running properly).

Credits

- Gabriel Richman, Oberlin College (Summer Intern)
- Jason A. Smith, BNL (Project Mentor)
- Tony Wong, BNL (Project Supervisor)
- John S. De Stefano Jr., BNL (Puppet Expert)
- William Strecker-Kellogg, BNL (Puppet Expert)
- James Pryor, NC State U (Puppet Expert)
- Tejas Rao, BNL (RHEV Expert)

Questions/Comments?

References

- Jenkins: <https://jenkins-ci.org/>
- Foreman: <http://theforeman.org/>
- RHEV: <http://www.redhat.com/rhev3/>
- Puppet: <https://puppetlabs.com/>
- Git: <http://git-scm.com/>
- RSpec: <http://rspec-puppet.com/>
- Serverspec: <http://serverspec.org/>
- Beaker: <https://github.com/puppetlabs/beaker/wiki>