

Centralized Fabric Management Using Puppet, Git & GLPI

Jason A. Smith
Brookhaven National Lab

Motivation

- Several years ago most admin work was either done manually or using home-made scripts
 - ssh in a loop from a management gateway
 - time-consuming, reactive, fire-fighting work
 - little sharing of work & backup expertise
- Standardize and unify our sysadmin work
- Self documenting build and config system
- Audit trail for complete change management
- Separate dev/test/prod env (little extra work)

Components

- Cobbler/RHEV – New system provisioning
- Puppet – Centralized config management
 - Complete service config after provisioning
 - Dashboard monitoring & change auditing
- Git – Puppet catalog repository
 - Distributed development & historical record
- GLPI – Asset mgmt. & node classification
 - Fusioninventory-agent: auto asset inventory
 - ENC uses GLPI, custom DB & dashboard

Provisioning

- Cobbler for hardware installs ([poster #539](#)):
 - Powerful Cheetah templating language and config/code reuse with “Snippets”
 - Single ks template used for most systems
 - Specify OS version & arch, network (MAC, IP, etc) & template metadata to install base OS, including fusioninventory-agent & puppet
- RHEV 3.0 for virtual machines:
 - Single template image used for new systems
 - 10 node cluster with 4TB of shared fiber storage

Cobbler Screenshot

Configuration

- Settings
- Check
- Events
- Distros
- Profiles
- Systems
- Repos
- Images
- Kickstart Templates
- Snippets

Actions

- Import DVD
- Sync ↕
- Reposync ↕
- Hardlink ↕
- Build ISO ↕
- Online Help Chat

Adding a System

⇒ **General**

Name Ex: vanhalen.example.org

Owners Owners list for authz_ownership (space delimited)

Profile Parent profile

Image Parent image (if not a profile)

Kernel Options Ex: selinux=permissive

Kernel Options (Post Install) Ex: clocksource=pit noapic

Kickstart Metadata Ex: dog=fang agent=86

Netboot Enabled Enabled PXE (re)install this machine at next boot?

Kickstart Path to kickstart template

Comment

Free form text description

⇒ **Networking (Global)**

Hostname

Gateway

Name Servers space delimited

Name Servers Search Path space delimited

⇒ **Networking**

Add Interface

Edit Interface

MAC Address (Place "random" in this field for a random MAC Address.)

IP Address

Bonding Mode

Static Enabled Is this interface static?

Subnet

DHCP Tag

RHEV Screenshot

Red Hat Enterprise Virtualization
User: smithj4 | Sign out | Guide | About

Basic Extended

New Server | New Desktop | Edit | Remove | Run Once | Change CD | Make Template

Virtual Machines

- apuppetst01 (Test puppet master for Jason)
- dcdcap01 (Storage Management dcdcap servers)**
- dcdcap04 (Storage Management dCache servers)
- git01 (Jason)

General | Network Interfaces | Virtual Disks | Snapshots | Permissions | Events | Applications | Monitor

Name:	dcdcap01	Defined Memory:	4096 MB	Origin:	RHEV
Description:	Storage Management dcdcap servers	Physical Memory Guaranteed:	2730 MB	Run On:	Any Host in Cluster
Template:	RHEL6_base	Number of CPU Cores:	4 (2 Socket(s), 2 Core(s) per Socket)	Custom Properties:	Not-Configured
Operating System:	Red Hat Enterprise Linux 6.x x64	Highly Available:	1		
Default Display Type:	Spice	USB Policy:	Disabled		
Priority:	Medium	Resides on Storage Domain:	ahostdisk01_48_Subnet		

Why Git?

- Distributed version control system
- Faster, completely localized project copies
 - Commits and other work can be done offline
 - Local copy contains complete history
- Reduced single point of repository failure
 - Git can merge changes between many “servers”
- Simple, fast & clean branching (and merging)
 - Branches easily merged with other branches
 - All changes can be treated as branches

Why Puppet?

- Cfengine, puppet, chef, etch, bcfg2, AutomateIt
- Puppet was selected for several reasons:
 - Simple yet powerful DSL (Domain-Specific Lang) & RAL (Resource Abstraction Layer)
 - Explicitly declared dependency graphing model
 - Provides better deterministic state convergence
 - Central config catalog & dependency resolution
 - Better security, conflict resolution & logic analysis
 - Web dashboard, GraphViz config visualization
 - Long history, stable codebase, large user base

GLPI Node Classification

GLPI **Inventory** Assistance Management Tools Plugins Administration Setup **Settings** Help Logout (Jason Smith)

Computers Monitors Software Networks Devices Printers Cartridges Consumables Phones Status

Central > Inventory > Computers

^ List: 2/2

Volumes Software Connections Management Documents Registry Tickets Links Notes Reservations Historical OCSNG Custom Fields

ID 2 Last update: 2012-02-15 16:00 (Imported from OCSNG)

Name:	gcmaster02	Contact:	root
Type:	-----	Contact Number:	382
Model:	PowerEdge R410	User:	[Nobody]
Location:	BCF	Group:	382
Manufacturer:	Dell Inc.	Technician in charge of the hardware:	Jason Smith
OS:	Red Hat Enterprise Linux Workstation release 6.2 (Santiago)	Network:	382
OS Version:	2.6.32-220.4.2.el6.x86_64	Domain:	rcf.bnl.gov
Service Pack:	#1 SMP Mon Feb 6 16:39:28 EST 2012	Serial Number:	FQ5TLM1
OS serial:		Inventory number:	382
OS Product ID:	ID-1000049759	Status:	testing
Auto update OCSNG:	Yes	Update Source:	-----
Last OCS inventory date: 2012-03-08 16:16 Import date in GLPI: 2012-03-08 16:20 Server localhost, Agent: FusionInventory-Agent_v2.1.14		Comments:	x86_64/00-00-26 09:27:10 Swap: 8191

[Update](#) [Delete](#)

Puppet Classes:

```
base afs lvm::fs(fs=[/var:sysvg:10G]) ganglia::node(cluster=gce_servers)
yumrepo::conf(repos=[testing:99]) git glpi mysql::server
glpi::fusioninventory-agent puppet::client(noclient=1) puppet::server
puppet::dashboard
```

Puppet Parameters:

```
iptables_allow_tcp_ports=[https,8140,130.199.6.238@3000]
httpd_www_fs_size=10G mysql_db_fs_size=20G backup_fs_size=40G
git_proxy_server=https://vproxytest02.rcf.bnl.gov
git_allow_from=130.199.6.238 glpi_allow_from=130.199.6.238
ssh_root_key_list=[jd,mizuki,pryor,raot,smithj4,willsk]
```

[Update Custom Fields](#)

Puppet Environments

- 3 puppet environments linked to git branches:
 - Development: extensive module changes
 - Testing: small changes and wider testing
 - Changes staged for more manual tests by wider audience before merging into production
 - Production: main server management
 - Changes must be approved before they are merged into the production branch/environment
- Git branches are automatically sync'ed to puppet environments by push hooks.
 - Also verifies puppet syntax and other checks

Production Approval

Git/Puppet updates to production that are pending approval.

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

Date	Age	User	Changes	Changelog	Approve	Reject
Fri Mar 9 15:43:12 2012	2 days	Zhenping Liu	diff	pending-zhliu-cb36590-20120309T204312UTC	merge	delete
Mon Mar 12 10:18:27 2012	1 minute	Jason A. Smith	diff	pending-smithj4-cb36590-20120312T141827UTC	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.
- 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 repo. You can clean these up by using the "git remote prune origin" command.

Cgit Diff View

The screenshot shows a web interface for a Git repository. At the top left is the 'git' logo and the text 'index : puppet/catalog'. Below this is the subtitle 'Git Repository for the RACF Puppet Catalog.' and the text 'RACF Puppet Master'. There are two buttons: 'development' with a dropdown arrow and 'switch'. Below the header is a navigation bar with links for 'summary', 'refs', 'log', 'tree', 'commit', 'diff', and 'stats'. The 'diff' link is highlighted. To the right of the navigation bar is a 'log msg' dropdown and a search box with a 'search' button. Below the navigation bar is a path bar showing 'path: root/gce/glpi/manifests/fusioninventory-agent.pp'. The main content area is titled 'Side-by-side diff' and contains a 'Diffstat' section. The Diffstat shows a bar chart for 'gce/glpi/manifests/fusioninventory-agent.pp' with 24 lines of changes (19 insertions and 5 deletions). Below the Diffstat is a diff command: 'diff --git a/gce/glpi/manifests/fusioninventory-agent.pp b/gce/glpi/manifests/fusioninventory-agent.pp'. The diff output shows the following changes:

```
diff --git a/gce/glpi/manifests/fusioninventory-agent.pp b/gce/glpi/manifests/fusioninventory-agent.pp
index 93ed6fb..dfd2f40 100644
--- a/gce/glpi/manifests/fusioninventory-agent.pp
+++ b/gce/glpi/manifests/fusioninventory-agent.pp
@@ -1,8 +1,22 @@
-class glpi::fusioninventory-agent {
+class glpi::fusioninventory-agent ( $server=undef ) {
+ # Check for parameterized class invocation or global parameter:
+ if ( $server ) {
+ # Called as a parameterized class, use that server name:
+ $server_name = $server
+ } elsif ( $glpi_server ) {
+ # Global parameter is set, use that server name:
+ $server_name = $glpi_server
+ } else {
+ # Default puppet server name:
+ $server_name = 'puppet.racf.bnl.gov'
+ }
+
+ # Install the fusioninventory-agent package:
+ package { 'fusioninventory-agent':
- ensure => installed,
- require => Yumrepo[ 'base' ],
+ ensure => latest,
+ schedule => daily,
+ require => Yumrepo[ 'base' ],
+ notify => Service[ 'fusioninventory-agent' ],
+ }
```

Puppet Dashboard

puppet dashboard v1.1.1 » Home • Nodes • **Groups** • Classes • Reports

Nodes 2579

- Currently successful 1829
- Currently failing 10
- Ever succeeded 1833
- Ever failed 175
- Never reported 740
- Not currently reporting 1691
- Hidden 0
- File Search
- Custom query
- [Add node](#)

Class

- afs 0
- base 41
- bnl_banner 1
- cloudtestbed_vm 0
- cvms 4
- desktop 21
- dns 0
- epel 0
- frontier 4
- httd_host 1
- [Add class](#)

Group

- Atlas dCache 20
- Desktops 21
- Phenix dCache 24
- Web servers 9
- [Add group](#)

Group: Atlas dCache [Edit](#) [Destroy](#)

Parameters
— No parameters —

Groups
— No groups —

Classes
— No classes —

Derived groups
— No child groups —

Daily run status
Number and status of runs during the last 30 days:

Nodes for this group

	Hostname	Source	Latest report
✓	dcsrm02.usatlas.bnl.gov	dcsrm02.usatlas.bnl.gov	2012-03-16 16:40 EDT
✓	dcdc03.usatlas.bnl.gov	dcdc03.usatlas.bnl.gov	2012-03-16 16:40 EDT
✓	dcsrddb01.usatlas.bnl.gov	dcsrddb01.usatlas.bnl.gov	2012-03-16 16:40 EDT
✓	dcd00r11.usatlas.bnl.gov	dcd00r11.usatlas.bnl.gov	2012-03-16 16:31 EDT
✓	dcd00r12.usatlas.bnl.gov	dcd00r12.usatlas.bnl.gov	2012-03-16 16:22 EDT
✓	dcd00r08.usatlas.bnl.gov	dcd00r08.usatlas.bnl.gov	2012-03-16 16:22 EDT
✓	chimera01.usatlas.bnl.gov	chimera01.usatlas.bnl.gov	2012-03-16 16:21 EDT
✓	dcd00r13.usatlas.bnl.gov	dcd00r13.usatlas.bnl.gov	2012-03-16 16:21 EDT
✓	dcd00r06.usatlas.bnl.gov	dcd00r06.usatlas.bnl.gov	2012-03-16 16:20 EDT
✓	dcd00r14.usatlas.bnl.gov	dcd00r14.usatlas.bnl.gov	2012-03-16 16:20 EDT

Puppet Config & Scalability

- Still using 2.6.16 on RHEL5 with ruby 1.8.5
 - testing upgrade to 2.7 on RHEL6 with ruby 1.8.7
- Apache with Phusion Passenger (mod_rails)
- Queue daemon with activemq for fast DB updates of storeconfigs
- Over 2k agents currently using puppet
- Noticed MySQL errors with inventory service enabled at a rate \geq about 1 client/second
- Tomcat/JRuby in future for improved scalability

Future Plans

- Change Management
 - Policy & procedures used to control changes made to production systems (ITIL, DevOps).
 - Changes made only during official windows.
 - Absolutely no unauthorized changes, no “cowboy” type behavior tolerated.
 - Use testbed environment to test changes before putting them into production.
 - Create replica of prod using VMs for auto-tests
 - Tools like Puppet, Git & GLPI can help make changes and keep a historical change record.

Automated Validation

- Add a new “validation” git branch & puppet environment
 - Contents: production with all changes currently pending approval automatically merged in
- Replica of all critical production services using RHEV VMs
- Automated testing of production and proposed changes using puppet agent runs and nagios monitoring of all Vms to validate that all production systems still work as expected

Why do it?

- Uncontrolled change can work sometimes, but often cause self inflicted problems and future firefighting episodes & upgrade nightmares.
- Stop duplicating work and effort, standardize.
- Stop making time consuming manual changes.
- Without it, servers become like snowflakes: they may all start out identical, but over time, config drift eventually makes each one unique.

Benefits

- Shift staff time from perpetual reactive firefighting mode, that often only addresses the symptoms, to more proactive work, that addresses the root causes of problems (fire prevention).
- Repeatable and standard build & config process means it is often faster and easier to rebuild problematic servers, rather than waste hours or days troubleshooting problems.

References

- Cobbler: <http://cobbler.github.com>
- RHEV:
<http://www.redhat.com/products/virtualization>
- FusionInventory: <http://fusioninventory.org>
- GLPI: <http://www.glpi-project.org>
- Git: <http://git-scm.com>
- Puppet: <http://puppetlabs.com>
- Email: smithj4@bnl.gov