

Purpose

Using Ansible:

- Deploy a single broker for OpenShift Origin M4
- Deploy one or more node for OpenShift Origin M4

Scenario

Class assignment where we were required to download Ansible Playbook from:

https://github.com/maxamillion/ansible-openshift_origin

(For Ansible 1.4, OpenShift Origin Release 2, Fedora)

and modify it so it would work for:

- Ansible 2.1.0
- OpenShift Origin M4
- Centos 6.7

Methodology

Use the existing file structure provided from above git and re-write the playbook by translating the comprehensive guide step by step in chronological order

Prerequisite

Ansible Host

- ```
- Ansible 2.1.0
- python-netaddr package to support "ipaddr()" filter for Ansible
- updated hosts list /etc/ansible/hosts
 - group: brokers, nodes*
```

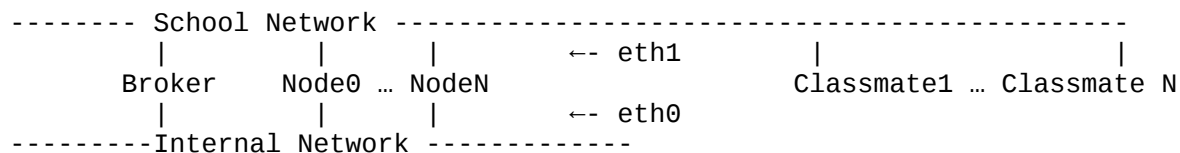
Each node will have fqdn "node#" based on order it is entered  
i.e. [Nodes]

```
192.168.1.6 <-- pos 0
192.168.1.7 <-- pos 1
```

```
192.168.1.6's fqdn = node0.DOMAIN_NAME
192.168.1.7's fqdn = node1.DOMAIN_NAME
```

## Broker & Node

- Centos 6.7
- SSH public key from Ansible Host installed.  
(See next page for preparation tools if using KVM)
- two Ethernet interfaces (default: eth0 is internal, eth1 is DHCP external)
- if cloning VM. Ensure /etc/udev/rules.d/70-persistent-net.rules is empty so that new device # starts at eth0



**Known Issue:**

1. If External interface (DHCP Client) IP changes, DNS record for broker & node's external domain fqdn needs to be updated to reflect the new IP

\*\* Currently no script was written to automate this process

- Can obtain node's `ipaddress_eh1` via `mco`.
- Factor is set on default to update node's inventory every minute

2. TSIG for nsupdate is changed upon every playbook run.

- Key creation steps can be replaced with a static key value via `group_vars` instead

## Post Installation

Please follow Section 12 of openshift origin comprehensive guide to create district and add node(s) and import cartridges from node

## OpenShift Origin Components Overview

### **Broker**

- **OpenShift-Broker** : authenticate (i.e. httpasswd) user  
authorize user (i.e. gear size allowed) to manage their gears
  - looks up and store user/gear information in **MongoDB**
  - process user request by sending commands via  
MCollective→ **ActiveMQ** ←MCollective ←Node
  - nsupdate CNAME record to reflect location of gear (Node)
  - administer gears on node (i.e. move gear between node)
- **OpenShift-Console**: provide client access to manage their account and gears  
(i.e. WebConsole, rhc cli)

**MongoDB** : Used to store user/gear data such as ownership of gears

**ActiveMQ** : A Message queue where the Broker and Node communicates with one another

**DNS** : Points gear's sub-domain to the correct node so that it can be access using Apache Virtual Host by name

### **Node**

- Process request from Broker to create, delete, restart application
- Creates and configures Linux account on system each representing a gear
- Set disk quota based on gear size
- Run user's application in contained environment
- Provide git and ssh access for clients to their application
- Provide public access to each web application using virtual host by name

## Components layout (Based on Comprehensive Guide)

Broker Host (QTY: 1)

- Broker
- Authoritative DNS
- MongoDB
- ActiveMQ

Node Host (Qty 1 or more)

- Node

## Files

**ansible-openshift\_origin/** Ansible playbook and files for setting up Openshift

```
|
|-- site.yml Main Playbook for the installation
```

**ansible\_prep/** (Optional) Shell Scripts for preparing cloned VM for Ansible

- For KVM only

- **Prerequisite:** libguestfs-tools-c must be installed

```
| -- add_knownhosts [IP] Add target's fingerprint to ~/.ssh/known_hosts
| - This prevent the "Authenticity of host cannot be
| established" message from interfering
| with Ansible playbook run
```

```
-- set_ip [vm] [IP] Edit target VM's /etc/sysconfig/network-scripts/ifcfg-eth0
 - set line "IPADDR" to "IPADDR=[IP]"
 - VM must be offline
```

```
-- set_keys Optional. (Use ssh-copy-vm instead)
 - Runs Ansible ping module against all hosts found in
 /etc/ansible/hosts. Determines which host is running
 sshd but is refusing SSH connection due to missing SSH
 public key. It then determine if IP belongs to a
 locally hosted VM running on KVM. If it is, prompt
 to initiate shutdown of VM to add SSH key by editing
 image file of the VM
```

[illegible]

## Settings

File: ansible-openshift\_origin/group\_vars/all

### Networking

eth\_dev\_internal internal facing device name i.e. eth0  
eth\_dev\_external external facing device name

### Domain

infra\_domain: external facing domain name  
internal\_domain: internal facing domain name

### Broker

broker\_fqdn external facing fqdn (Access web console externally)  
broker\_fqdn\_internal internal facing fqdn  
broker\_auth\_privkey\_path /etc/openshift/server\_priv.pem  
broker\_auth\_pubkey\_path /etc/openshift/server\_pub.pem  
broker\_rsync\_key\_name ssh public key copied to node  
broker\_rsync\_key\_path ssh public key path  
  
broker\_auth\_salt Generated using: openssl rand -base64 64  
broker\_session\_secret Generated using: openssl rand -base64 64  
(Should be different from broker\_auth\_salt)

### Web Console

broker\_webconsole\_user Default user created for accessing web-console  
broker\_webconsole\_passwd (To administer use htpasswd on /etc/openshift/htpasswd)  
broker\_webconsole\_secret Generated using: openssl rand -base64 64

### Named

named\_forwarder\_ip Forwarders for DNS Server

### ActiveMQ

mq\_fqdn ActiveMQ Server internal fqdn  
mq\_server\_user used to set up a user account on ActiveMQ  
used by Mcollective(Broker/Node) to access ActiveMQ  
mq\_server\_password password for above account  
mq\_server\_adminpass Admin password for ActiveMQ Server  
mq\_psk: mcpsk

### MongoDB

mongo\_db\_fqdn Default is set to access it locally (localhost)  
mongo\_db\_name openshift\_broker\_dev  
mongo\_auth\_user used by broker to access above database  
mongo\_auth\_passwd used by broker to access above database  
mongo\_admin\_user admin account for mongo server as a whole  
mongo\_admin\_passwd admin password

### Common

ntpserver ntp server used for time sync

## **Node**

The following settings determines which cartridge will be installed on the node

|                      |                                           |
|----------------------|-------------------------------------------|
| cartridges_mandatory | mandatory cartridge required by openshift |
| cartridges_app       | programming language cartridge            |
| cartridges_db        | database cartridge                        |
| cartridges_admin     | administrative add-on cartridge           |
| cartridges_rec_dep   | recommended dependencies cartridge        |
| cartridges_opt_dep   | optional dependencies cartridge           |