# Create an OSEv3 group that contains the master, nodes, etcd, and lb groups.

# The lb group lets Ansible configure HAProxy as the load balancing solution.

# Comment lb out if your load balancer is pre-configured.

[OSEv3:children]

masters

nodes

etcd

lb

# Set variables common for all OSEv3 hosts

[OSEv3:vars]

#openshift\_pkg\_version=-3.9.14

#openshift\_image\_tag=v3.9.14

#openshift\_cockpit\_deployer\_version=3.9.14

#openshift\_web\_console\_version=v3.9.14

ansible\_ssh\_user=root

openshift\_deployment\_type=openshift-enterprise

# apply updated node defaults

#openshift\_node\_kubelet\_args={'pods-per-core': ['10'], 'max-pods': ['250'], 'image-gc-high-threshold': ['90'], 'image-gc-low-threshold': ['80']}

# enable ntp on masters to ensure proper failover

openshift\_clock\_enabled=true

# HA Settings

openshift\_rolling\_restart\_mode=system

openshift\_master\_cluster\_method=native

openshift\_master\_cluster\_hostname=openshift-cluster.HobbyLobby.corp

openshift\_master\_cluster\_public\_hostname=openshift-cluster.HobbyLobby.corp

##### LDAP Configuration

# LDAP auth

#openshift\_master\_identity\_providers=[{'name': 'HobbyCorp', 'challenge': 'true', 'login': 'true', 'kind': 'LDAPPasswordIdentityProvider', 'attributes': {'id': ['distinguishedName'], 'email': ['mail'], 'name': ['cn'], 'preferredUsername': ['sAMAccountName']}, 'bindDN': '', 'bindPassword': '', 'ca': '', 'insecure': 'false', 'url': 'ldap://HobbyLobby.corp:389/OU=Hobby Lobby,DC=HobbyLobby,DC=corp?sAMAccountName'}]

# Configuring the ldap ca certificate

#openshift\_master\_ldap\_ca=<ca text>

# or

#openshift\_master\_ldap\_ca\_file=<path to local ca file to use>

openshift\_master\_identity\_providers=[{'name': 'HobbyCorp', 'challenge': 'true', 'login': 'true', 'kind': 'LDAPPasswordIdentityProvider', 'attributes': {'id': ['distinguishedName'], 'email': ['mail'], 'name': ['cn'], 'preferredUsername': ['sAMAccountName']}, 'bindDN': 'CN=svc\_ldap\_openshift,OU=ServiceAccounts,OU=Corporate,OU=Hobby Lobby,DC=HobbyLobby,DC=corp', 'bindPassword': 'nlyi&24#gjII\*3Ec', 'ca': '', 'insecure': 'true', 'url': 'ldap://hldc01.HobbyLobby.corp:389/OU=Users,OU=Corporate,OU=Hobby Lobby,DC=HobbyLobby,DC=corp?sAMAccountName'},{'name': 'htpasswd\_auth', 'login': 'true', 'challenge': 'true', 'kind': 'HTPasswdPasswordIdentityProvider', 'filename': '/etc/origin/master/htpasswd'}]

openshift\_master\_htpasswd\_users={'cluster-admin':'$apr1$XRucgGlb$bwxbkpoVVJlkBtrSCtzGo0'}

# HobbyCorp Custom Settings

#openshift\_docker\_blocked\_registries=all

#openshift\_docker\_blocked\_registries=registry.access.redhat.com,docker.io

#openshift\_docker\_insecure\_registries=hlsatellite01.hobbylobby.corp:5000

#openshift\_docker\_additional\_registries=hlsatellite01.hobbylobby.corp:5000

#openshift\_examples\_modify\_imagestreams=True

#oreg\_url=hl-redhat-openshift3\_ose-${component}:${version}

#openshift\_logging\_image\_prefix=hl-redhat-openshift3\_

#openshift\_metrics\_image\_prefix=hl-redhat-openshift3\_

#openshift\_provisioners\_image\_prefix=hl-redhat-openshift3\_

#osm\_etcd\_image=hl-redhat-rhel7\_etcd

#openshift\_cockpit\_deployer\_prefix=hl-redhat-openshift3\_

#openshift\_web\_console\_prefix=hl-redhat-openshift3\_

#openshift\_logging\_eventrouter\_image\_prefix=hl-redhat-openshift3\_

#openshift\_master\_default\_subdomain=osapps.HobbyLobby.corp

#openshift\_hosted\_registry\_routehost=openshift-registry.HobbyLobby.corp

# Firewall configuration because the default is not suggested

os\_firewall\_use\_firewalld=True

##### Need to configure persistent storage for registry #### Not NFS ####

openshift\_hosted\_registry\_storage\_kind=nfs

openshift\_hosted\_registry\_storage\_access\_modes=['ReadWriteMany']

openshift\_hosted\_registry\_storage\_host=hlisi01nfs.hobbylobby.corp

openshift\_hosted\_registry\_storage\_nfs\_directory=/OpenShift

openshift\_hosted\_registry\_storage\_volume\_name=pv-registry01

openshift\_hosted\_registry\_storage\_volume\_size=50Gi

##### Need decission from network team

osm\_cluster\_network\_cidr=172.16.5.0/25

openshift\_portal\_net=172.16.5.128/25

osm\_host\_subnet\_length=4

#### Need to look at supplying custom certificates signed by internal CA

#openshift\_master\_overwrite\_named\_certificates=true

#openshift\_master\_named\_certificates=[{"certfile": "/path/to/custom1.crt", "keyfile": "/path/to/custom1.key", "names": ["public-master-host.com"], "cafile": "/path/to/custom-ca1.crt"}]

# Enable Cluster metrics

openshift\_metrics\_install\_metrics=true

##### Need to setup persistent storage of cluster metrics

#openshift\_metrics\_cassandra\_storage\_type=dynamic

#openshift\_master\_metrics\_public\_url=https://openshift-metrics.hobbylobby.corp

openshift\_metrics\_storage\_kind=nfs

openshift\_metrics\_storage\_access\_modes=['ReadWriteOnce']

openshift\_metrics\_storage\_host=hlisi01nfs.hobbylobby.corp

openshift\_metrics\_storage\_nfs\_directory=/OpenShift

openshift\_metrics\_storage\_volume\_name=pv-metrics01

openshift\_metrics\_storage\_volume\_size=50Gi

# Enable Cluster logging

openshift\_logging\_install\_logging=true

##### Need to setup persistent storage of cluster logging

#openshift\_logging\_es\_pvc\_dynamic=true

#openshift\_master\_logging\_public\_url=https://openshift-logging.hobbylobby.corp

openshift\_logging\_storage\_kind=nfs

openshift\_logging\_storage\_access\_modes=['ReadWriteOnce']

openshift\_logging\_storage\_host=hlisi01nfs.hobbylobby.corp

openshift\_logging\_storage\_nfs\_directory=/OpenShift

openshift\_logging\_storage\_volume\_name=pv-logging01

openshift\_logging\_storage\_volume\_size=50Gi

##### Neeed to setup PVs for Ansible Broker ### Not NFS ? ###

openshift\_hosted\_etcd\_storage\_kind=nfs

openshift\_hosted\_etcd\_storage\_nfs\_directory=/OpenShift

openshift\_hosted\_etcd\_storage\_volume\_name=pv-absetcd01

openshift\_hosted\_etcd\_storage\_access\_modes=["ReadWriteOnce"]

openshift\_hosted\_etcd\_storage\_volume\_size=10G

openshift\_hosted\_etcd\_storage\_host=hlisi01nfs.hobbylobby.corp

##### Need to configure whitelist at a later date

ansible\_service\_broker\_local\_registry\_whitelist=['.\*-apb$']

##### Need project for ansible template service broker

openshift\_template\_service\_broker\_namespaces=['openshift','myproject']

# Security

openshift\_web\_console\_inactivity\_timeout\_minutes=30

# host group for masters

[masters]

pocosmaster01.HobbyLobby.corp

pocosmaster02.HobbyLobby.corp

pocosmaster03.HobbyLobby.corp

# host group for etcd

[etcd]

pocosinfra01.HobbyLobby.corp

pocosinfra02.HobbyLobby.corp

pocosinfra03.HobbyLobby.corp

# Specify load balancer host

[lb]

pocoslb01.HobbyLobby.corp

# host group for nodes, includes region info

[nodes]

pocosmaster01.HobbyLobby.corp

pocosmaster02.HobbyLobby.corp

pocosmaster03.HobbyLobby.corp

pocospod01.HobbyLobby.corp openshift\_node\_labels="{'region': 'infra'}"

pocospod02.HobbyLobby.corp openshift\_node\_labels="{'region': 'primary'}"

#### Need to look into labelling for region for production