RED HAT CONSULTING

WebSphere Cartridge Installation Guide

PREPARED FOR - FRIT

Table of Contents

1. Synopsis

The purpose of this document is to present the guidance to install and configure WebSphere 8.5.5.1 OpenShift Enterprise V2.2 cartridge. It is meant to be loaded into OpenShift from source code. There are a few installation steps that are outside OpenShift regarding the installation of IBM's WebSphere but also directory permissions and SELinux policy enablement.

The cartridge currently supports the following features:

- Provisioning of new IBM WebSphere Application Server instance in minutes
- Full build & Deploy life cycle (as with EAP cartridge)

2. Installation

2.1. Setup OSE Environment

The setup of the OSE Environment can be accomplished as per your usual way of deploying broker and nodes. This could be via the OSE install script, or any other CM tools like Puppet and Ansible

2.2. WebSphere Application Server Installation

> In contradiction to the deployment model of other cartridges (that includes all binaries of a certain technology), we've decided not to put the installation files into the cartridge.
> The reasons for these decisions are:
> * IBM WebSphere Application Server Binaries are very large (around 2-3 GB)
> * Installation process for the binaries takes takes a long time (up to 15 minutes according to the computing resources)

2.2.1. Binary Installation

The installation of IBM WebSphere on the filesystem can be done either via the IBM agent installer or any other means that are currently employed. The main thing to note here is that profile creation inside the IBM WAS installation would need to be enabled to allow non root users to create them. That is because each gear in OSE will create its own profile and each gear runs as its own UUID and not as root.

2.2.2. Non-Root permissions

In order to create profiles by non-root users, special file permission settings have to be set on your WebSphere installation. Please follow the steps described here:

WebSphere Non Root Permissions Configuration

We have included the `setWebSpherePermissionsForNonRootProfileCreation.sh` that sets basic file permissions on the directories that gears would require to access.

2.2.3. SELinux Permissions & IPv6

With SELinux enabled on the system, we will require that the following group context be set on the IBM WAS AppServer directory. This would ensure that gear that run under the `openshift_rw_file_t` group context can have read/write permissions to shared directories under IBM WAS. This does not mean that gears will be able to step on each other in these shared directories since each gear will have ownership of its own files.

Set SELinux Context for WebSphere

Since IBM WebSphere Application is installed outside of the gear's sandbox, you need to customize SELinux permission settings in a way that the installation directory "/path-to/AppServer" can be accessed with read/write.

```
semanage fcontext -a -t openshift_rw_file_t "/path-to/AppServer(/.*)?"
restorecon -R -v /path-to/AppServer/
```

Disable IPv6

If there are no requirements to use IPv6 on your system, then we recommend disabling it. Keeping IPv6 enabled in OpenShift 2 will cause the WebSphere gears to not be restarted properly, and in some scenarios, not restarted at all. If IPv6 is a requirement then we recommend you work with Red Hat support to create an SELinux policy that accomodates this use case.

Disabling IPv6 is a three step process:

1. Create a file `/etc/modprobe.d/ipv6.conf` with the following contents:

   ```
   `options ipv6 disable=1`
   ```

2. For completeness, it is a good idea to configure the ip6tables service not to start at boot by issuing the following command:

   ```
   `chkconfig ip6tables off`
   ```

3. Safe reboot the box

3. Cartridge Installation

The cartridge can be installed as any other OSE cartridge. However, you MUST have to make sure that WebSphere Application Server has been installed before (as described in the preceding sections):

Extract the zipped source code of the WAS cartridge under

```
/usr/libexec/openshift/cartridges
```

You will also need to set the correct SELinux Context on the cartridge so that it is consistent with the rest of the cartridges on each node. This file context is:

```
system_u:object_r:bin_t:s0
```

To set this context run the following command:

```
chcon -R -u system_u /usr/libexec/openshift/cartridges/ose2-was-frb-cart-frb-was/
```

On each OpenShift node where you wish to make this cartridge available execute the following commands:

```
cd /usr/libexec/openshift/cartridges
oo-admin-cartridge --action install --recursive --source
/usr/libexec/openshift/cartridges
```

To make the cartridge available run this command from the broker:

```
oo-admin-ctl-cartridge --activate -c import-node node.hostname
```

This cartridge needs an existing installation of the WebSphere Application Server on each of your nodes. You need to define the location of the installation through a system wide environment variable

```
echo "/path-to/AppServer" > /etc/openshift/env/OPENSHIFT_WEBSPHERE_INSTALL_LOCATION
```

The cartridge keys off this global OpenShift environment variable to know where the WAS binaries are located so that it may create a profile for each gear created.

4. Administration and configuration

4.1. How profile creation works

This cartridge will call `${OPENSHIFT_WEBSPHERE_DIR}/install/bin/manageprofiles.sh` and create a profile with the name of the OpenShift app that the user created followed by the domain space name. The final format looks like: "APPNAME-DOMAIN-FQDN-GEAR_UUID" . The profile will be created underneath the `profile` directory inside your gears `data` directory.

It is very important for the non-root users to be configured to be allowed the necessary permissions to create profiles so that profile creation from within the cartridge can occur.

4.2. Access to WebSphere Admin Console

The WebSphere Administration Console can be access in two ways:

- Option 1: Preferred - After you have created your gear, do an `rhc port-forward <GEAR_NAME>` and open a browser with the following URL:

```
https://<YOUR_LOCAL_IP>:9043/ibm/console
```

- Option 2: The Admin Console is also exposed via a separate external port that can be determined as follows:

```
rhc ssh <GEAR_NAME>
export | grep WC_ADMINHOST_SECURE_PROXY_PORT
```

Now point your browser to the following URL: `https://<GEAR_DNS>:<WC_ADMINHOST_SECURE_PROXY_PORT>/ibm/console/logon.jsp` and enter your credentials. Unfortunately the Admin Console tries to redirect us to the local port `9043`.

Now manually change port `9043` back to `WC_ADMINHOST_SECURE_PROXYPORT` and change `login.jsp` to `login.do` so that the URL looks like follows: `https://<GEAR_DNS>:<WC_ADMINHOST_SECURE_PROXY_PORT>/ibm/console/login.do?action=secure`.

The Admin Console should then appear.

5. Reference Information

WebSphere

- Command reference "manageprofiles.sh"
- Disable Security HTTPS for Web App
- Configure WebSphere to bind to specific IP
- File Permissions for non-admin install

OpenShift V2

- Cartridge Developers Guide
- How to expose more than one public port in cartridge