FRIT Oracle Cartridge Installation Guide

**A. Synopsis**

The purpose of this document is to present the guidance to install and configure Oracle Datasource OpenShift Enterprise V2.2 cartridge. It is meant to be loaded into OpenShift from source code.

The cartridge currently supports the following features:

* Creating an Oracle Database tenant via a remote script call
* Setting environment variables to allow web servers to call newly created tenant in a datasource

1

**B. Installation**

**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

[WebSphere Non Root Permissions Configuratio](http://www-01.ibm.com/support/knowledgecenter/SS7JFU_8.5.5/com.ibm.websphere.express.doc/ae/tpro_nonrootpro.html?lang=en)n

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

**2.3. SELinux Permissions**

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

2

ownership of its own files.

**2.3.1. 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.

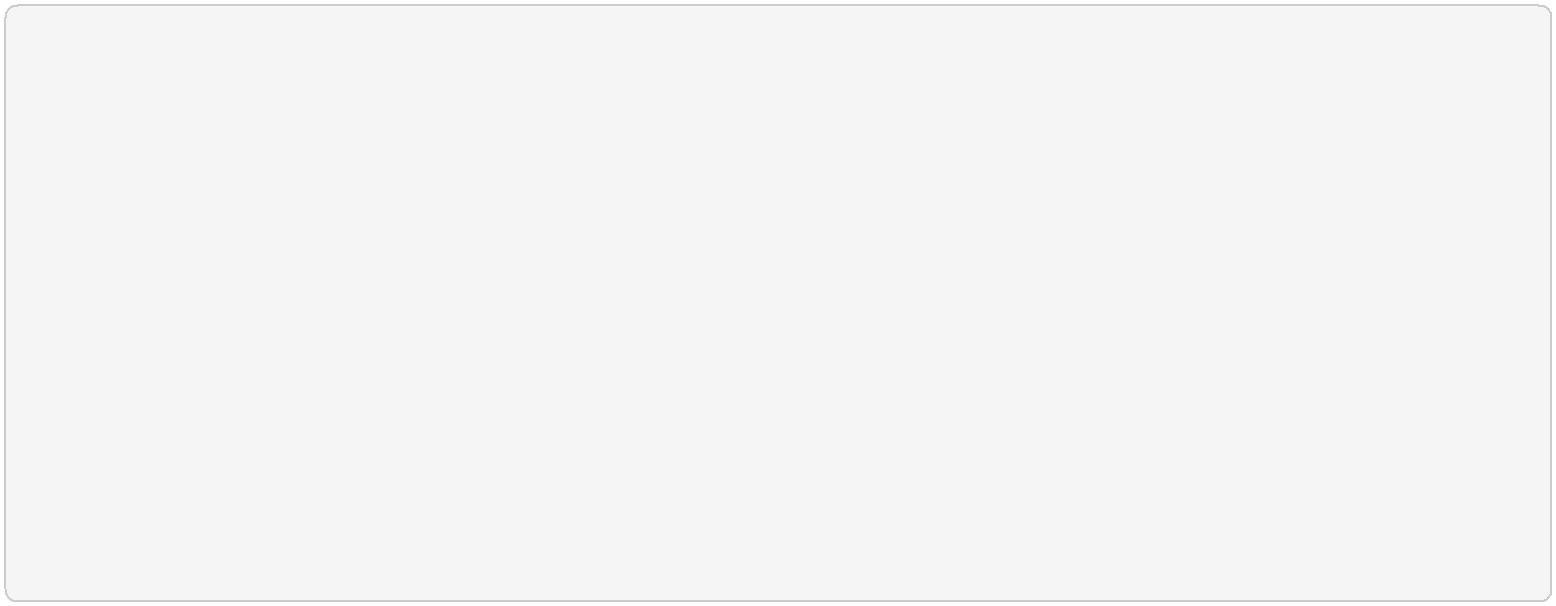


semanage fcontext -a -t openshift\_rw\_file\_t "/path-to/AppServer(/.\*)?" restorecon -R -v /path-to/AppServer/

**2.3.2. Create and Load WASpol.te**

The following SELinux policy will also have to be included in the node configuration installation. This SELinux Policy is required to be able to restart the WAS gears. When it is not there, the WAS gear will not restart, because the Java process is unable to reacquire the ports it needs as SELinux blocks the Java process.

The policy should be packaged inside the WASpol.te file:



module WASpol 1.0;

require {

type proc\_net\_t; type node\_t; type openshift\_t;

class tcp\_socket node\_bind; class file { read open };

}

allow openshift\_t node\_t:tcp\_socket node\_bind; allow openshift\_t proc\_net\_t:file { read open }

The WASpol.te file should be laid down with root level permissions on the file system and then compiled into a .pp file as per the below.

The .pp file is the SELinux binary policy. The SELinux policy can then be loaded with the command. The WASpol.pp file is included for convenience in the cartridge.

semodule -i WASpol.pp

The SELinux policy should now be loaded. The WASpol.te file is located under the usr directory.

To generate the WASpol.pp file a few commands must be run to compile the policy into binaries. The commands are:

3

Generate the WASpol.mod file with the command:

checkmodule -M -m -o /path-to/WASpol.mod WASpol.te

Generate the WASpol.pp file with the command:

semodule\_package -o WASpol.pp -m WASpol.mod

Load the WASpol.pp policy:

semodule -i WASpol.pp

To verify that the policy has been loaded correctly check that it exists with the command:

semodule -l | grep WASpol

4

**C. 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.

5

**D. Administration and configuration**

**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.

**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](https://&lt;GEAR_DNS&gt;:&lt;WC_ADMINHOST_SECURE_PROXY_PORT&gt;/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=secur](https://&lt;GEAR_DNS&gt;:&lt;WC_ADMINHOST_SECURE_PROXY_PORT&gt;/ibm/console/login.do?action=secure)e.

The Admin Console should then appear.

6

**E. Reference Information**

**WebSphere**

* [Command reference "manageprofiles.sh](http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.express.doc/ae/rxml_manageprofiles.html)"
* [Disable Security HTTPS for Web Ap](http://www-01.ibm.com/support/docview.wss?uid=swg21408274)p
* [Configure WebSphere to bind to specific I](http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/trun_multiplenic.html?lang=en)P
* [File Permissions for non-admin instal](http://www-01.ibm.com/support/knowledgecenter/SS7JFU_8.5.5/com.ibm.websphere.express.doc/ae/tpro_nonrootpro.html?lang=en)l

**OpenShift V2**

* [Cartridge Developers Guid](http://openshift.github.io/documentation/oo_cartridge_developers_guide.html)e
* [How to expose more than one public port in cartridg](https://www.openshift.com/content/at-least-one-port-for-external-use-excluding-8080-please)e

7