**BBP aPaaS documentation:**

**APAAS V3 DEPLOYMENT FOR BUSINESSBANKING APPLICATION:**

**Flow**: Internal Nexus artifact-> aPaaS V3 image build-> Deploy to aPaaS V3-> promotion to external nexus to pull and run image -> deployment via promotion job for https URL projects

After provisioning of projects on aPaaS V3 platform like 8370, 8928. etc., flow can be summarized as:

* Configuring Jenkins build for image building and deploying the application with groovy script.
* MA properties should be properly set for relevant environments via property utils tool.
* Vault secrets have been properly defined for correct deployment.
* Building an image of the nexus artefact on top of JBoss image.
* Performing deployment on aPaaS with the same image.
* After deployment, a route has been created to test application via soap UI.
* Need to test the services with proper wsdl invocation to get response.
* Usage of promotion job for further https URLs project deployment.
* Certs are also needs to be present on BPM side for *proper* handshake.

**Following are the step by step details for the deployment:**

**Step-1 Pre-requisites:**

**From aPaaS side we need some pre-requisites to make the configuration ready for making connection to BPM:**

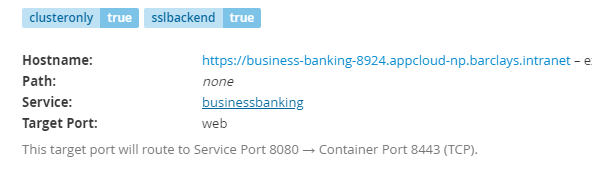
1. For SSL pass-through route: (Remember we need to use https route from BPM)

As we need to point aPaaS from BPM server, we required https pass-through route as per:

<https://confluence.barcapint.com/display/GRPCLOUDKB/Mutual+Authentication%3A+Jboss+Configuration+Hints>

This route contains two parameters requires as ssl backend and cluster only as true as compared to normal route.

For creating this route, we need to approach aPaaS support team with service and FQDN details with the new route name.



Pass-through requests for reference:

**Project Request**

|  |  |
| --- | --- |
| 8924 | https://gtisjira.barcapint.com/browse/OSE-8857 |
| 8925 | https://gtisjira.barcapint.com/browse/OSE-9090 |
| 8926 |  |
| 8927 |  |
| 8928 | https://gtisjira.barcapint.com/browse/OSE-9090 |
| 8929 |  |
| 8930 |  |
| 8931 |  |

1. According to the post, we need to add keystore and truststore jks file from vault manger: <https://confluence.barcapint.com/display/GRPCLOUDKB/Mutual+Authentication%3A+Jboss+Configuration+Hints>

**Keystore and Trust Store:** ( Need Naveen and Bishwa’s input here)

It is recommended that a dedicated trust and keystore is created to secure incoming communication, to provide more control around the client certificate trust.

The keystore should contain the client facing certificate and private key whose common name should reflect the hostname of the Pass-through route, so that when the client checks the certificate it will match the hostname used to make the connection.

The keystore should contain the client facing certificate and public whose common name should reflect the hostname of the route, so that when the client checks the certificate it will match the hostname used to make the connection. e.g. if  route of myapp-9999.appcloud-np.barclays.intranet is used as the route hostname this should be defined in the certificate CN.

The truststore should contain the certificates required to verify the client certificate. Jboss, by default, only verifies the client certificate.  If required, the trust can be limited to a particular certificate by only populating the trust store with the relevant client certs.

Depending on level of authenication required reate a trustsore containing either the:

a).  The certificate that will be used by the client to authenticate to the service, or

b). The signers of the client certificate

We need to place certs for every environment once in vault manager for having deployment in CIT-C. CIT-D and so on. and same in case of passwords for DS usernames also.

* Added cert to ma-truststore

e.g, [https://cftjira.barcapint.com/browse/BARCDEVOPS-111649](https://cftjira.barcapint.com/browse/BARCDEVOPS-111649#_blank)

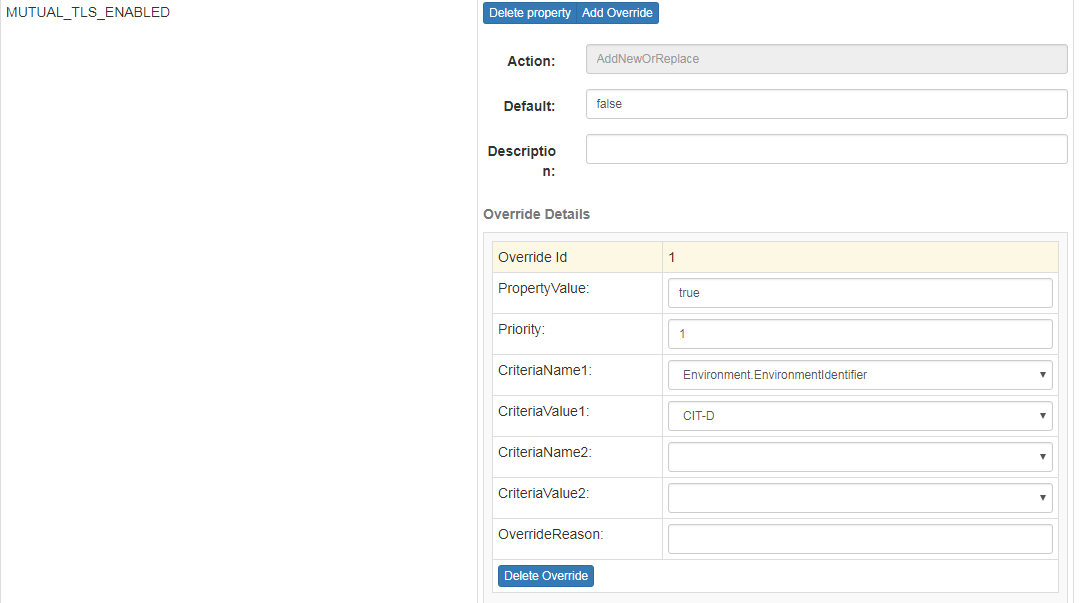
* Added jks file

e.g, [https://cftjira.barcapint.com/browse/BARCDEVOPS-111641](https://cftjira.barcapint.com/browse/BARCDEVOPS-111641#_blank)

* Added jks password

e.g, [https://cftjira.barcapint.com/browse/BARCDEVOPS-111598](https://cftjira.barcapint.com/browse/BARCDEVOPS-111598#_blank)

1. For making MA changes under property utils for the environments like CIT-C, CIT-D, etc.,



* Add property MUTUAL\_TLS\_ENABLED as per above

e.g, [https://cftjira.barcapint.com/browse/BARCDEVOPS-111558](https://cftjira.barcapint.com/browse/BARCDEVOPS-111558#_blank)

1. For SSL Handshake on BPM side:

Below steps has been followed: ( Need Naveen and Bishwa’s input here)

* Generate new keystore
* Generate new certificate request
* Raise new cert now request approved
* Get new certificate imported in KS -
* Add bpm cert imported in truststore
* Add new cert in bpm truststore
* Once we have vault cleaned.
* Add cert and KS in apaas vault

**Step-2: Image building via Jenkins:**

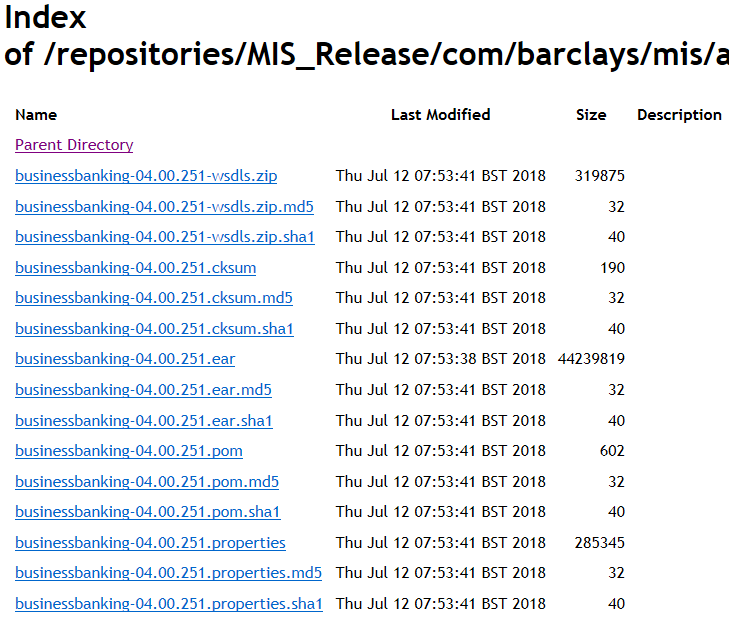
We have dedicated Jenkins Job for picking up ear file (that has already been placed on Nexus by MTS Team) by specifying the version inside job:

<https://jenkins1a.intranet.barcapint.com:8444/jenkins/job/BUK/job/BPMMDB/job/8370BBPForSoapUI/>

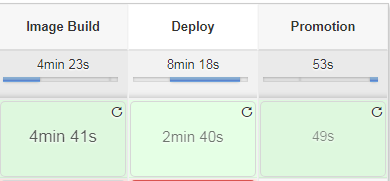
* This is using MCAs gear configuration files (<https://stash.barcapint.com:8443/projects/GRP_BPM/repos/gear_config_files>) which I’ve forked to GRP\_BPM repo.
* We are getting uploaded version of ear on internal Nexus (<https://barcorpnexus.barcapint.com:8443/nexus> ) under path [/com/barclays/mis/apps/platforms/businessbanking/](https://barcorpnexus.barcapint.com:8443/nexus/service/local/repositories/MIS_Release/content/com/barclays/mis/apps/platforms/businessbanking/04.00.251/businessbanking-04.00.251-wsdls.zip)<version>

e.g.,

<https://barcorpnexus.barcapint.com:8443/nexus/content/repositories/MIS_Release/com/barclays/mis/apps/platforms/businessbanking/04.00.251/>



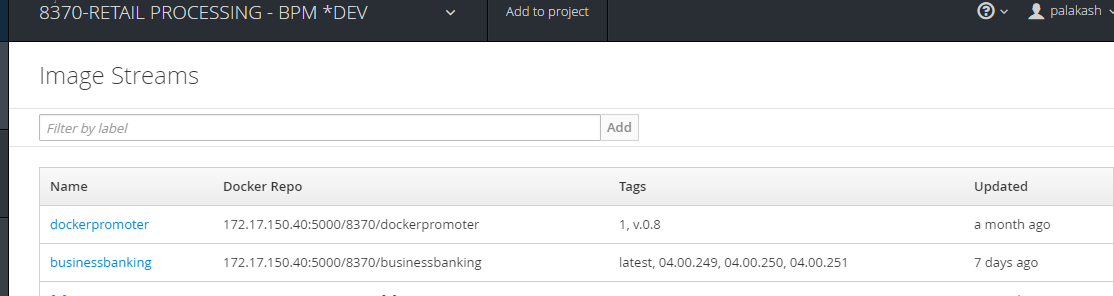
* It has three stages shown as below:



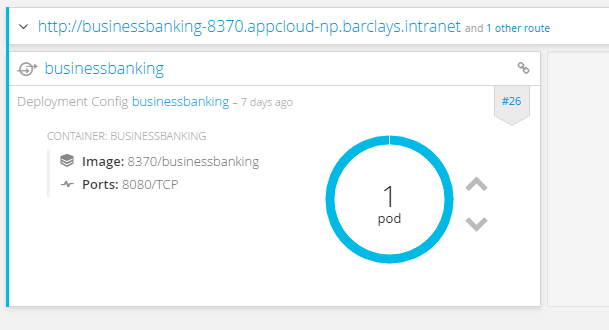
Above job is used to build image from nexus artifact and deploy to 8370 aPaaS for quick soap UI test and for verification from BPM side for the response.

* After image building, the image used to store in internal aPaaS V3 docker registry as a part of image stream which can be checked through aPaaS V3 platform: Details for docker registry is likewise depends upon the namespace:

e.g., Host-172.17.150.40:5000 (inaccessible through URL).



* After then the same image will be deployed on already existed image catalog (currently 8370) for aPaaS V3 platform (gl and sl) under our project (like 8370, 9059.) as a pod which run container for our application and create a route to access it and can be tested from soap UI.

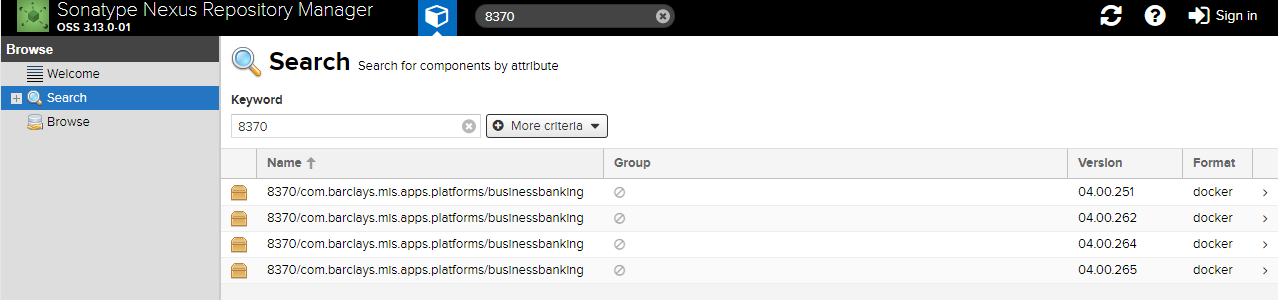


* Then it to push the image to external nexus repo (<https://barclays-registry.barcapint.com:18443>) to make it available for pulling the same configuration for next or other environment deployments for https URLs project.
* Currently we’re using 8370 project repo for promoting businessbanking application to external nexus repo.

* Once it will be deployed to 8370 it will promote the same image to external nexus repo under 8370:

URL for external Nexus;

<https://barclays-registry.barcapint.com:18443/>



**Step 3- Deployments to projects containing https route:**

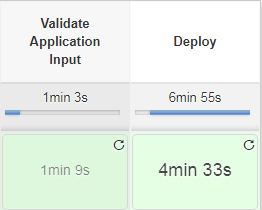
It will then use to deploy the tested image to promote on other environments or to another aPaaS environment where it can be used from BPM side via https route;

**For Promotion Job:**

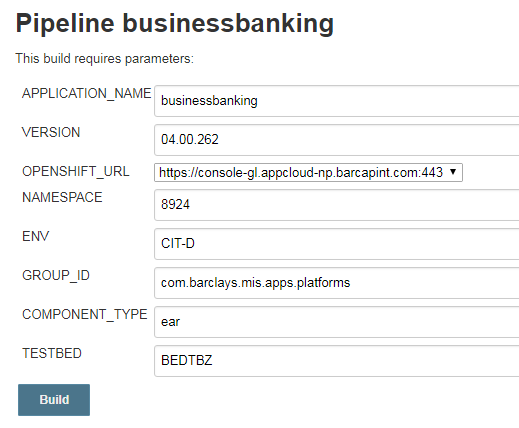
* We are using release/api branch of latest pipeline of MCA tools for this job.
* We have defined separate promotions Jenkins job defined for that inside promotion folder:

<https://jenkins1a.intranet.barcapint.com:8444/jenkins/job/BUK/job/BPMMDB/job/Promotion/job/businessbanking/>

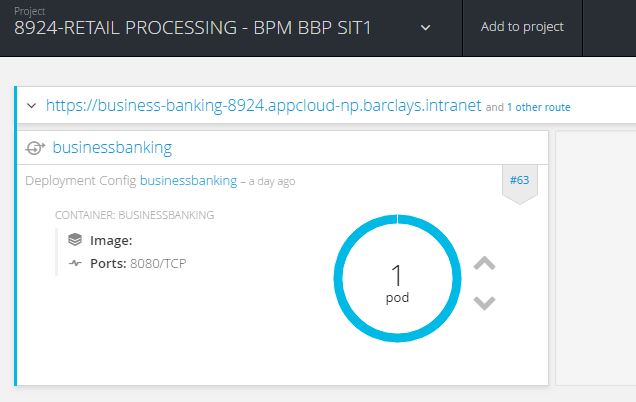
* It has following stages:



And need to provide parameters accordingly to build it:



* It will then deploy it to proper aPaaS Namespace provided above ready for BPM.



* **For target port 8443 settings:**

We need to change the service.yaml to set the target port as 8443 instead of 8080.

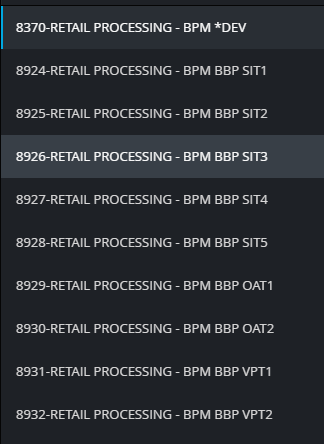


**Step 4- For other projects deployments:**

We have below different projects already setup for deployment of application in GL NP. We need the similar setup for PROD/others as well.

URL for accessing projects:

<https://console-gl.appcloud-np.barcapint.com>



**Important contacts:**

**bchat/DLs**: IT\_aPaaSV3, IT\_Bitbucket, IT\_Jenkins, IT\_JIRA, IT\_DEVTOOLS

**MQ team:**

**1-** Any urgent BAU Production MQ incident/queries to L1: Middleware Service Operations Team Account <[serviceoperations.middleware@barclays.com](mailto:serviceoperations.middleware@barclays.com)>  
  
**2**- BAU Production MQ L3 queries including Certificate renewal: PaaS Messaging L3 : Infrastructure Services <[PaaSMessagingL3InfrastructureServices@barclayscorp.com](mailto:PaaSMessagingL3InfrastructureServices@barclayscorp.com)>  
  
**3**- Test MQ incidents/queries to PaaS Messaging NonProd : Infrastructure Services <[paasmessagingnonprodinfrastructureservices@barclayscorp.com](mailto:paasmessagingnonprodinfrastructureservices@barclayscorp.com)>

**Issues and resolutions:**

1. **There was a vault resolve expression error per below which was resolved by setting up proper passwords for usernames in vault manager:**

08:06:31,787 ERROR [org.jboss.as.controller.management-operation] (ServerService Thread Pool -- 27) JBAS014612: Operation ("enable") failed - address: ([

    ("subsystem" => "datasources"),

    ("data-source" => "DB2\_DS1")

]) - failure description: "JBAS014802: Cannot resolve expression '${VAULT::Db2Ds::UCYTBX::1}'"

1. **If Jenkins throws error like below: Need to retrigger again:**

Pulling image barclays-registry.barcapint.com:5000/bukeng/com.barclays.buk.jboss/jboss-sti-builder:0.1.206 ...

error: build error: failed to pull image: unauthorized: authentication required

error: The build 8924/businessbanking-8 status is "Failed"

[Pipeline] }

[Pipeline] // withCredentials

[Pipeline] }

[Pipeline] // withEnv

[Pipeline] }

[Pipeline] // ws

[Pipeline] }

[Pipeline] // node

[Pipeline] }

[Pipeline] // stage

[Pipeline] End of Pipeline

ERROR: script returned exit code 1

Finished: FAILURE

Using openshift URL CIPE:  [https://console-gl.appcloud-np.barcapint.com:443](https://console-gl.appcloud-np.barcapint.com/)

:createDeploymentConfig FAILED

FAILURE: Build failed with an exception.

\* Where:

Build file '/home/syspcbjenkins/store/workspace/BUK/BPMMDB/8924-RETAIL-PROCESSING-BPM-BBP-SIT1@2/v3.gradle' line: 531

\* What went wrong:

Execution failed for task ':createDeploymentConfig'.

> Could not get unknown property 'imageGroup' for task ':createDeploymentConfig' of type org.gradle.api.DefaultTask.

\* Try:

Run with --info or --debug option to get more log output.

\* Exception is:

org.gradle.api.tasks.TaskExecutionException: Execution failed for task ':createDeploymentConfig'.

        at org.gradle.api.internal.tasks.execution.ExecuteActionsTaskExecuter.executeActions(ExecuteActionsTaskExecuter.java:84)

        at org.gradle.api.internal.tasks.execution.ExecuteActionsTaskExecuter.execute(ExecuteActionsTaskExecuter.java:55)

        at org.gradle.api.internal.tasks.execution.SkipUpToDateTaskExecuter.execute(SkipUpToDateTaskExecuter.java:62)

        at org.gradle.api.internal.tasks.execution.ValidatingTaskExecuter.execute(ValidatingTaskExecuter.java:58)

        at org.gradle.api.internal.tasks.execution.SkipEmptySourceFilesTaskExecuter.execute(SkipEmptySourceFilesTaskExecuter.java:88)

        at org.gradle.api.internal.tasks.execution.ResolveTaskArtifactStateTaskExecuter.execute(ResolveTaskArtifactStateTaskExecuter.java:46)

1. **To extracts logs from pod side;**
2. **Go to under terminal tab for apaas environment;**

**Steps**: On aPaaS URL and under 8370/XXXX project

1. Go to business banking application.
2. Go to application ->Pods
3. Click on  terminal tab

1. **For co-event logs**

Type cd /home/jboss

Type cat co-event.log

1. **To check Version:**

sh-4.2$ ls

6.4.19.0

sh-4.2$ pwd

/apps/jboss/jboss-as

1. **To check server.log**

Go to /opt/eap/standalone/logs

1. **To check deployed ear**

Go to /opt/eap/standalone/deployments

1. **To check services.xml**

Go to /config/