

xCP Docker Images

This document describes the details of the Docker images for xCP. Following is the list of images:

- [xcp-apphost](#)
- [xcp-bam](#)
- [xcp-bps](#)
- [xcp-xda](#)
- [xcp-xda-tools](#)
- [xcp-cs-setup](#)

xcp-apphost

Description

This image is used to run the web container that will host the xCP application WAR. It uses following base software:

- CentOS 7
- Oracle JRE 8
- Apache Tomcat 8.0.x

The exact version of each of the above matches the one supported by the patch version of xCP Docker image.

Ports

Port	Description
8080	HTTP port for application server
8443	HTTPS port for application server. This will be exposed only if SSL configuration related environment variables are provided

Volumes

Path	Description
/opt/tomcat/CustomConf	Stores the configuration files like <code>dfc.properties</code> , etc.
/opt/tomcat/ctsws_config	Stores the configuration files for interacting with CTS
/opt/tomcat/logs	Stores the log files generated by the app server
/opt/tomcat/webapps	Stores the WAR files deployed from xCP Designer

Environment Variables

Environment Variable	Optional	Default Value	Description
DOCBASE_NAME	Yes	repo	Name of the docbase repository
DOCBROKER_HOST	Yes	cs	Hostname or IP address of the Docbroker to connect to
DOCBROKER_PORT	Yes	1489	Port of the Docbroker to connect to
GLOBAL_REGISTRY_USER	Yes	dm_bof_registry	Global registry user name
GLOBAL_REGISTRY_PASSWORD	Yes	password	Global registry user password. This can be either plaintext or encrypted

Environment Variable	Optional	Default Value	Description
BAM_SERVER_PROTOCOL	Yes	http	Protocol to connect to the BAM server
BAM_SERVER_HOST	Yes	bam	Hostname or IP address of the BAM server
BAM_SERVER_PORT	Yes	8080	Port of the BAM server
BAM_SERVER_CONTEXT	Yes	bam-server	Context root of BAM server application WAR
CTS_ADMIN_DOMAIN	Yes		Domain of the administrator user for CTS server
CTS_ADMIN_USER	Yes	admin	Administrator user name for CTS server
TOMCAT_ADMIN_USER	Yes		Administrator user name to be used for Tomcat. No admin user will be added if this is left blank
TOMCAT_ADMIN_PWD	Yes		Administrator password to be used for Tomcat. No admin user will be added if this is left blank. This must be plaintext
SSL_ENABLED	Yes	false	Set this to true to enable SSL. If enabled, then you must at least provide values for SSL_KEY_STORE_FILE and SSL_KEY_STORE_PWD
SSL_KEY_STORE_FILE	Yes		Keystore file for SSL. This file must be placed inside the volume that maps to /opt/tomcat/CustomConf
SSL_KEY_STORE_PWD	Yes		Password for the keystore. This must be plaintext
SSL_KEY_ALIAS	Yes		If keystore contains multiple keys, then this variable should be specified to indicate the Alias for key to be used
SSL_KEY_PWD	Yes		If key alias is provided, then the password for the same. If this is left blank, then key alias configuration is ignored. This must be plaintext
SSL_KEY_STORE_TYPE	Yes	jks	Type of the keystore
CLUSTER_ENABLED	Yes	false	Set this to true to enable clustering. As of now, this will enable session replication across all the nodes in cluster. This means that sticky sessions are not required to be set on load balancer. Typically this kind of replication should not be used if there are large number of nodes in the cluster, but should be okay if only 2-3 nodes are there
CLUSTER_TYPE	Yes	multicast	<p>Type of communication to use for clustering. Possible values are <code>multicast</code> or <code>unicast</code>. Multicast is easier to setup as new nodes can join it dynamically, but most of the network providers used in Docker Swarm or Kubernetes do not support multicast networking. In such cases, <code>unicast</code> should be used.</p> <p>For <code>multicast</code>, <code>CLUSTER_ADDRESS</code> and <code>CLUSTER_PORT</code> can be provided (or use defaults).</p> <p>For <code>unicast</code>, <code>CLUSTER_UNICAST_SIBLINGS</code> must be provided</p>
CLUSTER_NODE_NAME	Yes	Hostname of the container	Node name is set as <code>jvmRoute</code> in <code>server.xml</code> file of Tomcat. This is normally used by load balancers

Environment Variable	Optional	Default Value	Description
CLUSTER_ADDRESS	Yes	228.0.0.4	Multicast address to be used for cluster communications. If there are multiple clusters to be created within same network, then combination of this address and port must be unique for each cluster. All nodes within a given cluster must use same address and port
CLUSTER_PORT	Yes	45550	Multicast port to be used for cluster communications
CLUSTER_UNICAST_SIBLINGS	Yes (Mandatory if CLUSTER_TYPE is unicast)		For unicast clustering, comma separated list of hostnames of IP addresses of all other nodes in the cluster

Configuration Files

Volume	File Name	Description
/opt/tomcat/CustomConf	dfc.properties	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables
/opt/tomcat/CustomConf	bam-server.properties	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables
/opt/tomcat/CustomConf	deployment.properties	This is populated using values provided in environment variables
/opt/tomcat/CustomConf	rest-api-runtime.properties	Modify as required
/opt/tomcat/CustomConf	transformation.properties	Modify as required
/opt/tomcat/ctsws_config	preferences.xml	<p>This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables. Also,</p> <ul style="list-style-type: none"> • Copy the <code>aek.key</code> file from CTS server (located at <code>\$CTS/config</code>) and place it under volume <code>/opt/tomcat/ctsws_config</code> • Copy the <code>msspassword.txt</code> from CTS server (located at <code>\$CTS/docbases/<your_docbase>/config/pfile</code>) and place it under volume <code>/opt/tomcat/ctsws_config/pfile</code>

xcp-bam

Description

This image is used to run the BAM web application. It uses following base software:

- CentOS 7
- Oracle JRE 8
- Apache Tomcat 8.0.x

The exact version of each of the above matches the one supported by the patch version of xCP Docker image.

Ports

Port	Description
8080	HTTP port for application server
8443	HTTPS port for application server. This will be exposed only if SSL configuration related environment variables are provided

Volumes

Path	Description
/opt/tomcat/CustomConf	Stores the configuration files like <code>dfc.properties</code> , etc.
/opt/tomcat/LogConf	Stores the configuration files for configuring BAM DB connection, logging, etc.
/opt/tomcat/logs	Stores the log files generated by the app server

Environment Variables

Environment Variable	Optional	Default Value	Description
BAM_PASSWORD_ENCRYPTED	Yes	false	Set this to true, if values for both <code>BAM_DB_PWD</code> and <code>REPOSITORY_ADMIN_PWD</code> are provided in encrypted form
BAM_DB_TYPE	Yes	postgres	Type of database to store BAM data. Possible values are <code>postgres</code> , <code>oracle</code> or <code>mssql</code>
BAM_DB_HOST	Yes	bam-db	Hostname or IP address of the BAM database server
BAM_DB_PORT	Yes	5432	Port of the BAM database server
BAM_DB_NAME	Yes	bamdata	Name of the BAM database
BAM_DB_USER	Yes	bamdba	User name to use for connecting to the BAM database
BAM_DB_PASSWORD	Yes	password	Password to use for connecting to the BAM database. This can be either plaintext or encrypted. If it is encrypted then you must set <code>BAM_PWD_ENCRYPTED</code> value to <code>true</code>
BAM_HA_ENABLED	Yes	false	Set this to true, if BAM server has to be started in high availability mode
DOCBASE_NAME	Yes	repo	Name of the docbase repository
DOCBROKER_HOST	Yes	cs	Hostname or IP address of the Docbroker to connect to
DOCBROKER_PORT	Yes	1489	Port of the Docbroker to connect to
GLOBAL_REGISTRY_USER	Yes	dm_bof_registry	Global registry user name
GLOBAL_REGISTRY_PASSWORD	Yes	password	Global registry user password. This can be either plaintext or encrypted
DOCBASE_ADMIN_USER	Yes	dmadmin	Administrator user name for the repository
DOCBASE_ADMIN_PASSWORD	Yes	password	Administrator password for the repository. This can be either plaintext or encrypted. If it is encrypted then you must set <code>BAM_PWD_ENCRYPTED</code> value to <code>true</code>
TOMCAT_ADMIN_USER	Yes		Administrator user name to be used for Tomcat. No admin user will be added if this is left blank
TOMCAT_ADMIN_PWD	Yes		Administrator password to be used for Tomcat. No admin user will be added if this is left blank. This must be plaintext

Environment Variable	Optional	Default Value	Description
SSL_ENABLED	Yes	false	Set this to true to enable SSL. If enabled, then you must at least provide values for SSL_KEY_STORE_FILE and SSL_KEY_STORE_PWD
SSL_KEY_STORE_FILE	Yes		Keystore file for SSL. This file must be placed inside the volume that maps to /opt/tomcat/CustomConf
SSL_KEY_STORE_PWD	Yes		Password for the keystore. This must be plaintext
SSL_KEY_ALIAS	Yes		If keystore contains multiple keys, then this variable should be specified to indicate the Alias for key to be used
SSL_KEY_PWD	Yes		If key alias is provided, then the password for the same. If this is left blank, then key alias configuration is ignored. This must be plaintext
SSL_KEY_STORE_TYPE	Yes	jks	Type of the keystore

Configuration Files

Volume	File Name	Description
/opt/tomcat/CustomConf	dfc.properties	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables
/opt/tomcat/LogConf	bam.properties	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables
/opt/tomcat/LogConf	log4j.properties	Modify as required

xcp-bps

Description

This image is used to run the Process Integrator (BPS) web application. It uses following base software:

- CentOS 7
- Oracle JRE 8
- Apache Tomcat 8.0.x

The exact version of each of the above matches the one supported by the patch version of xCP Docker image.

Ports

Port	Description
8080	HTTP port for application server
8443	HTTPS port for application server. This will be exposed only if SSL configuration related environment variables are provided

Volumes

Path	Description
/opt/tomcat/CustomConf	Stores the configuration files like dfc.properties, bps_template.xml, etc.
/opt/tomcat/LogConf	Stores the configuration files for configuring logging, etc.

Path	Description
/var/bps/msgstore	Stores the message data used by BPS
/opt/tomcat/logs	Stores the log files generated by the app server

Environment Variables

Environment Variable	Optional	Default Value	Description
DOCBASE_NAME	Yes	repo	Name of the docbase repository
DOCBROKER_HOST	Yes	cs	Hostname or IP address of the Docbroker to connect to
DOCBROKER_PORT	Yes	1489	Port of the Docbroker to connect to
GLOBAL_REGISTRY_USER	Yes	dm_bof_registry	Global registry user name
GLOBAL_REGISTRY_PASSWORD	Yes	password	Global registry user password. This can be either plaintext or encrypted
DOCBASE_ADMIN_USER	Yes	dmadmin	Administrator user name for the repository
DOCBASE_ADMIN_PASSWORD	Yes	password	Administrator password for the repository. This can be either plaintext or encrypted. If it is encrypted then you must set BAM_PWD_ENCRYPTED value to true
DOCBASE_ADMIN_DOMAIN	Yes		Administrator user domain for the repository
BPS_HA_ENABLED	Yes	false	Set this to true, if BPS server has to be started in high availability mode
BPS_INSTANCE_NAME	Yes	bps1	Unique instance name for BPS. This is required to be different for each BPS node in an environment
TOMCAT_ADMIN_USER	Yes		Administrator user name to be used for Tomcat. No admin user will be added if this is left blank
TOMCAT_ADMIN_PWD	Yes		Administrator password to be used for Tomcat. No admin user will be added if this is left blank. This must be plaintext
SSL_ENABLED	Yes	false	Set this to true to enable SSL. If enabled, then you must at least provide values for SSL_KEY_STORE_FILE and SSL_KEY_STORE_PWD
SSL_KEY_STORE_FILE	Yes		Keystore file for SSL. This file must be placed inside the volume that maps to /opt/tomcat/CustomConf
SSL_KEY_STORE_PWD	Yes		Password for the keystore. This must be plaintext
SSL_KEY_ALIAS	Yes		If keystore contains multiple keys, then this variable should be specified to indicate the Alias for key to be used
SSL_KEY_PWD	Yes		If key alias is provided, then the password for the same. If this is left blank, then key alias configuration is ignored. This must be plaintext
SSL_KEY_STORE_TYPE	Yes	jks	Type of the keystore

Configuration Files

Volume	File Name	Description
/opt/tomcat/CustomConf	dfc.properties	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables
/opt/tomcat/CustomConf	bps_template.xml	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables

Volume	File Name	Description
/opt/tomcat/LogConf	log4j.properties	Modify as required

xcp-xda

Description

This image is used to run the xDA application. It uses following base software:

- CentOS 7
- Oracle JRE 8

The exact version of each of the above matches the one supported by the patch version of xCP Docker image.

Ports

Port	Description
7000	HTTP port for the server. If SSL is enabled then this would use HTTPS protocol.

Volumes

Path	Description
/opt/xDA/catalog	Stores the environment catalog data configured by the user
/opt/xDA/config	Stores the configuration files for xDA
/opt/xDA/logs	Stores the log files generated by the server

Environment Variables

Environment Variable	Optional	Default Value	Description
ADMIN_PASSWORD	Yes		Used to set password for xDA's admin user. Password must be at least 8 characters long and must contain at least 1 non-letter character. Currently this property is supported only in HTTP mode.
SSL_ENABLED	Yes	false	Set this to true to enable SSL. If enabled, then you must at least provide values for SSL_KEY_STORE_FILE and SSL_KEY_STORE_PWD
SSL_KEY_STORE_FILE	Yes		Keystore file for SSL. This file must be placed inside the volume that maps to /opt/xDA/config
SSL_KEY_STORE_PWD	Yes		Password for the keystore. This must be plaintext
SSL_KEY_ALIAS	Yes		If keystore contains multiple keys, then this variable should be specified to indicate the Alias for key to be used
SSL_KEY_PWD	Yes		If key alias is provided, then the password for the same. If this is left blank, then key alias configuration is ignored. This must be plaintext
SSL_KEY_STORE_TYPE	Yes	jks	Type of the keystore

Configuration Files

Volume	File Name	Description
/opt/xDA/config	xda-config.properties	This is populated using values provided in environment variables. It can be modified further for other properties which are not exposed as environment variables

xcp-xda-tools

Description

This image is used to run the xDA Tools. It will open interactive `bash` shell, so this image must always be run using `-it` option of `docker run` command. User can run `xda.sh` to start xDA Tools. User can also write/copy any xDA scripts if required and execute from the shell.

It uses following base software:

- CentOS 7
- Oracle JRE 8

The exact version of each of the above matches the one supported by the patch version of xCP Docker image.

Ports

NA

Volumes

NA

Environment Variables

Environment Variable	Optional	Default Value	Description
XDA_SERVER_PROTOCOL	Yes	http	Protocol to connect to xDA server. Possible values are <code>http</code> or <code>https</code>
XDA_SERVER_HOST	Yes	xda	Hostname or IP address of xDA server
XDA_SERVER_PORT	Yes	7000	Port of xDA server to connect to

Configuration Files

Volume	File Name	Description
/opt/xda-tools/config	xda.properties	This is populated using values provided in environment variables

xcp-cs-setup

Description

This image is used only once while setting up the xCP environment. It installs xCP components on the Content Server and Independent Java Method Server(IJMS) machines:

- Install Process Engine - It installs Process Engine on CS. It also installs Process Engine on IJMS if `is_IJMS` has been set to true.
- Install xCP related DAR files - It installs DAR files on CS machine

It can also optionally install any other DAR files that user might want as part of the environment. Refer to volume description for `/extra_dars`. For example, this can be used to install CTS DAR files to avoid manually installing the same separately while setting up CTS server.

It uses CentOS 7 as the base OS, and includes compatible version of Documentum Composer which is used to install the DAR

files.

Ports

NA

Volumes

Path	Description
/cs-bpm	The following path on CS machine should be externalized and then mounted as volume in this container: /opt/dctm/wildfly9.0.1/server/DctmServer_MethodServer/deployments/bpm.ear In case of IJMS the path should be: /opt/dctm_docker/jms/wildfly9.0.1/server/DctmServer_MethodServerHA1/deployments/bpm.ear
/cs-dba	The following path on CS machine should be externalized and then mounted as volume in this container: /opt/dctm/dba
/cs-mdserver-conf	The following path on CS machine should be externalized and then mounted as volume in this container: /opt/dctm/mdserver_conf In case of IJMS the path should be: /opt/dctm_docker/mdserver_conf
/extra_dars	You can put any other DAR files that you might want to install as part of the setup under this volume. DAR files will be picked up in alphabetical order for installation

Environment Variables

Environment Variable	Optional	Default Value	Description
DOCBASE_NAME	Yes	repo	Name of the docbase repository
DOCBASE_OWNER	Yes	dmadmin	User name of the repository owner
DOCBASE_OWNER_PASSWORD	Yes	password	Password for the repository owner
DOCBROKER_HOST	Yes	cs	Hostname or IP address of the Docbroker to connect to
DOCBROKER_PORT	Yes	1489	Port of the Docbroker to connect to
JMS_HOST	Yes	cs	Hostname or IP address of the Method Server to connect to
JMS_REMOTE_PORT	Yes	9084	Management port of the Method Server for remote connection
JMS_PORT	Yes	9080	Port of the Method Server to connect to
JMS_USER	Yes	admin	Administrator user name of the Method Server
JMS_PASSWORD	Yes	jboss	Password for the user of the Method Server
IS_IJMS	Yes	false	To specify if this image is being used to install xCP components on IJMS
GLOBAL_REGISTRY_USER	Yes		Global registry user name. This is required only if IS_IJMS is set to true
GLOBAL_REGISTRY_PASSWORD	Yes		Global registry user password. This can be either plaintext or encrypted. This is required only if IS_IJMS is set to true
GLOBAL_REGISTRY_DOCBASE	Yes		Global registry docbase. This is required only if IS_IJMS is set to true
DOCKER_HOST	Yes		It is the IP address or fully qualified name of the docker host machine where CS is running. This is required only if IS_IJMS is set to false

Configuration Files

NA

