Clinical Data/Health Data Repository 2.2

CHDS*2.2*1

Deployment, Installation, Back-Out, and Rollback Guide

January 2022

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Revision History

Date	Patch	Description	Author
01/11/2022	CHDS*2.2*1	• The purpose of this patch/upgrade is to bring the CHDR application into TRM, CRISP and Fortify compliance • OS Upgrade: Solaris M8 Supercluster per AITC deployment • Oracle WebLogic Middleware: Version 12.2.1.4 • Oracle Database: Version 19c • JAVA 1.8.x	Liberty ITS

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Guide for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Guide is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

1 Introduction

The CHDR application is an interagency data transfer application responsible for synchronizing the Allergy and Pharmacy data for Active Dual Consumer (ADC) patients contained in the DOD's Clinical Data Repository (CDR) and the VA's Health Data Repository (HDR).

This document describes how to deploy and install CHDS*2.2*1, as well as how to back-out the product and rollback to a previous version or data set.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom CHDS*2.2*1 will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

Not applicable for CHDS*2.2*1.

1.3 Constraints

Not applicable for CHDS*2.2*1.

2 Roles and Responsibilities

Table 1: Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	HPSCLIN	Deployment	Provide .ear files and Installation Guide to the AITC team	N/A
2	AITC	Deployment	Plan and schedule deployment (including orchestration with vendors)	N/A
3	AITC	Deployment	Execute deployment	N/A
4	AITC	Installation	Plan and schedule installation	N/A
5	AITC	Installation	Ensure authority to operate and that certificate authority security documentation is in place	N/A

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
6	HPSCLIN	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	N/A
7	AITC and HPSCLIN	Post Deployment	Hardware, Software and System Support	N/A

3 Deployment

The deployment is planned as a standard National Patch Module rollout. Once approval has been given to nationally release CHDS*2.2*1, the patch will be released via the National Patch Module. At this point, it will be available for installation and deployment at AITC.

Message monitoring will be performed by both AITC and the HPSCLIN team. It is anticipated that there will be a 14-day compliance period.

3.1 Timeline

There is no specific timeline for deployment. This is considered a maintenance release and installation will be performed by AITC, within the constraints of the compliance period for the release.

3.2 Site Readiness Assessment

The CHDR application is centrally located at AITC and is not directly deployed to any site locations.

3.2.1 Deployment Topology (Targeted Architecture)

CHDS*2.2*1 will be deployed at AITC.

3.2.2 Site Information (Locations, Deployment Recipients)

The CHDR application is centrally located at AITC and is not directly deployed to any site locations.

3.2.3 Site Preparation

Not applicable to CHDS*2.2*1.

The following table describes preparation required by the site prior to deployment.

Table 2: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
N/A	N/A	N/A	N/A	N/A

3.3 Resources

The documents in **Table 3** can be found on the SOFTWARE library as well as the Veterans Document Library (VDL).

SOFTWARE: https://REDACTED/SOFTWARE/

VDL: https://www.va.gov/vdl/application.asp?appid=155

Table 3: Associated Patch Documents

File Name	Description
CHDS_2_2_P1_DIBR	Deployment, Installation, Back-out, and Rollback Guide
CHDS_2_2_P1_IG	Installation Guide

3.3.1 Facility Specifics

The CHDR application is centrally located at AITC.

The following table lists facility-specific features required for deployment.

Table 4: Facility-Specific Features

Site	Space/Room	Features Needed	Other
N/A	N/A	N/A	N/A

3.3.2 Hardware

The CHDR application is centrally located at AITC.

The following table describes hardware specifications required at each site prior to deployment.

Table 5: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
N/A	N/A	N/A	N/A	N/A	N/A

Please see **Table 1** for details about who is responsible for preparing the site to meet these hardware specifications.

3.3.3 Software

The CHDR application is centrally located at AITC.

The following table describes software specifications required at each site prior to deployment.

Table 6: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
N/A	N/A	N/A	N/A	N/A	N/A

Please see **Table 1** for details about who is responsible for preparing the site to meet these software specifications.

3.3.4 Communications

CHDS*2.2*1 will be deployed using the standard method of patch release from the National Patch Module. When CHDS*2.2*1 is released, the National Patch Module will send a notification to all the personnel who have subscribed to those notifications.

3.3.4.1 Deployment/Installation/Back-Out Checklist

Table 7: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy	N/A	N/A	N/A
Install	N/A	N/A	N/A
Back-Out	N/A	N/A	N/A

4 Installation

4.1 Pre-installation and System Requirements

The CHDR application is hosted on the Solaris M8 Supercluster - Unix platform at AITC.

All applications in the VA, are required to run on TRM and CRISP compliant platforms. For the CHDR application this includes the M8 Supercluster Unix platform, Oracle JAVA, Oracle WebLogic, and Oracle Database. AITC system and WebLogic administrators are responsible for patching the components while the development and/or sustainment teams are responsible for testing the applications on any required TRM and CRISP compliant patched components.

Although the AITC WebLogic Administrators have created/converted a new Pre-installation considerations/step to be performed by AITC production WebLogic administrators are as follows:

1 Verify TRM compliant versions of JAVA and WebLogic are installed and configured.

2 Verify a new compliant domain exists in parallel with the existing WebLogic domain to ensure a successful rollback if necessary. Ports in the new compliant domain can be switched to the same ports as the existing domain to support the rollback.

3 Verify the new WebLogic domain includes current certificates in WebLogic keystores and AITC standard WebLogic domain configurations.

4 Verify applications directory chdr-core and the core.properties exists in the domain directory.

5 Verify core.properties file parameter hl7.processingId=P.

6 Verify WebLogic managed server startup parameter dgov.va.med.environment.production" is set to "true" in the WebLogic managed server startup parameters.

7 Verify timeout value in WebLogic domain JTA tab is changed from 30 to 3600 seconds for a transaction time out.

8 Any references to the production CHDR database schema must be 'chdr2' versus 'chdr'.

9 Verify JMS module has been completely configured with Persistent Stores and JMS servers.

10 Verify security realms match between old and new domains.

4.2 Platform Installation and Preparation

AITC to verify the TRM compliant versions of the following software:

1 Oracle WebLogic Middleware: Version 12.2.1.4

2 Oracle Database: Version 19c

3 JAVA 1.8.x

4.3 Download and Extract Files

HPSCLIN team will provide a request for change (RFC) to include the required software file(s) and the chronological steps for downloading and extracting the file(s) prior to installation.

4.4 Database Creation

Not applicable for CHDS*2.2*1.

4.5 Installation Scripts

Not applicable for CHDS*2.2*1.

4.6 Cron Scripts

Not applicable for CHDS*2.2*1.

4.7 Access Requirements and Skills Needed for the Installation

AITC administrators with access to perform deployments and installations.

4.8 Installation Procedure

The installation procedures will take 2 steps. Step 1 can be done at any time the AITC administrators schedules allow. Step 2 will be the schedules event for cutover from the old to new domain.

1 Assign managed server ports that do not match current production ports, bring the new domain online with managed servers down, implement changes described in this document, deploy the CHDR application, start the managed servers and verify healthy status and deployment is Active. Upon successful implementation of the changes in the new domain, shutdown the managed servers on new domain.

2 With the new domain managed servers down, configure the ports in the new domain to match the ports in the current production domain, take the current domain managed servers offline, start the managed servers in the new domain and verify health status.

3 Monitor the Audited_Events table in the database and all 6 managed server WebLogic log files for Faults and exceptions and if the deployment is not working and cannot be corrected, perform the rollback by bringing the current domain back online.

4.8.1 Verify TRM compliant WebLogic installation and respective Domain

At the WebLogic Admin Console, verify the version displayed in the footer of the console screen is a TRM compliant version.

Verify the WebLogic domain was created or converted to be compatible with the TRM compliant installation of WebLogic.

4.8.2 Verify TRM compliant JDK is installed and referenced in the Domain

Following the CRISP initiative and TRM compliance requirements, system administrators must:

1 Identify the appropriate version of JAVA

2 Install it in the **/u01/app/oracle/java** directory

3 After installation, create a symbolic link **/u01/app/oracle/java/latest**

4 Point this symbolic link to the desired version of JAVA within the same **/u01/app/oracle/java** directory

   a. **ln -s /u01/app/oracle/java/jdk1.8.0_xxx /u01/app/oracle/java/latest**

The **/u01/app/oracle/java/latest** will be used in the WebLogic configurations to minimize impact to JAVA updates and/or changes

4.8.3 Configure CHDR WebLogic Directory Structure

The current directory structure on CHDR machines is as follows:

APPLICATION_HOME = /u01/app/install --- contains deployable CHDR applications support files.

DOMAIN_HOME = /u01/app/domains/<chdr domain name> --- contains the WebLogic domain created for the respective environment.

DOMAIN_HOME/applications – contains CHDR application component properties files.

WL_HOME = /u01/app/oracle/<installation directory> --- contains the WebLogic installation and supporting tools to administer WebLogic domains.

JAVA_HOME = /u01/app/oracle/java/latest --- points to the latest installation of JAVA.

The new WebLogic server home instance will be in directory:

WLS_HOME = <WL_HOME>/wlserver

4.8.4 Verify WebLogic Domain components

1 Verify 2 machines have been created in the domain.

2 Verify 6 managed servers have been created, Admin, and 3 managed servers on machine 1 and 3 additional managed servers assigned to machine 2.

3 Verify all respective managed servers have been assigned to a cluster.

4 For each machine configured in a domain, verify the Node Manager is reachable.

5 Verify the Default XA and NonXA Data Sources in the new domain connecting to the Database.

6 Verify the JMS queue configuration has been implemented and is in place. Verification includes persistent stores and JMS server assignments.

7 The setDomainEnv.sh file has been modified for the new release. The new file will be provided by the CHDR dev team for AITC admin deployment to both machines. The updated content includes:

```
#@REM CHDR Specific Configuration -- START
VLJ_DIR=${DOMAIN_HOME}/applications
export VLJ_DIR
# TRM upgrade changes to support jpa 2.1 in weblogic domain.
export MW_HOME=/u01/app/oracle/wl122
PRE_CLASSPATH="${PRE_CLASSPATH}:${MW_HOME}/oracle_common/modules/javax.persistence.jar"
#PRE_CLASSPATH="${PRE_CLASSPATH}:${MW_HOME}/wlserver/modules/com.oracle.weblogic.jpa21support_1.0.0.0_2-1.jar"
PRE_CLASSPATH="${PRE_CLASSPATH}:${VLJ_DIR}"
PRE_CLASSPATH="${PRE_CLASSPATH}:${DOMAIN_HOME}/lib/commons-dbcp-1.2.2.jar"
PRE_CLASSPATH="${PRE_CLASSPATH}:${DOMAIN_HOME}/lib/commons-pool-1.3.jar"
PRE_CLASSPATH="${PRE_CLASSPATH}:${DOMAIN_HOME}/lib/commons-collections-3.2.jar"
#PRE_CLASSPATH="${PRE_CLASSPATH}:${DOMAIN_HOME}/lib/ojdbc6.jar"
export PRE_CLASSPATH


#@REM KAAJEE Specific JVM Properties
```

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.wsee.bind.suppressDeployErrorMessage=true"
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.wsee.skip.async.response=true"
JAVA_OPTIONS="${JAVA_OPTIONS} -Dgov.va.med.environment.servertype=weblogic"
JAVA_OPTIONS="${JAVA_OPTIONS} -Dgov.va.med.environment.production=false"
#JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.alternateTypesDirectory=${KAAJEE_DIR}"
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.configuration.schemaValidationEnabled=false"
JAVA_OPTIONS="${JAVA_OPTIONS} -
Dehcache.disk.store.dir=${DOMAIN_HOME}/servers/${SERVER_NAME}/tmp"
#JAVA_OPTIONS="${JAVA_OPTIONS} -
Dpsl.configuration=${DOMAIN_HOME}/applications/psl/psl.properties"


export JAVA_OPTIONS
log4jk="password"
export log4jk
log4jp="SQL"
export log4jp
caipp="c41ppr0c3ss"
export caipp
caipep="{3DES}F6KrWewnUOh1259rarwEDw=="
export caipep
CLASSPATH=${PRE_CLASSPATH}:${CLASSPATH}
export CLASSPATH
echo
echo JAVA_OPTIONS=${JAVA_OPTIONS}
echo
echo JAVA_PROPERTIES=${JAVA_PROPERTIES}
echo
echo
echo CLASSPATH=${CLASSPATH}
echo
echo
echo
```

4.8.5 WebLogic Managed Servers Start Parameters

Each managed server in the CHDR domain will require a certain amount of system resources to handle its respective required load and a class path defined specific to the CHDR applicatoin. These resources are assigned in the configuration Server Start tab of each managed server.

The following are the entries for the class path and arguments in the Server Start tab have been modified based on the SQA entries and the current production configuration.

The Class Path is the same for all servers.

The .ms1 server has different resource assignments for the Arguments as shown here:

Class Path:

```
$CLASSPATH:/u01/app/oracle/weblogic-server-
12.2.1.4/wlserver/server/lib/weblogic_sp.jar:/u01/app/oracle/weblogic-server-
12.2.1.4/wlserver/server/lib/weblogic.jar:/u01/app/oracle/weblogic-server-
12.2.1.4/oracle_common/modules/javax.persistence.jar:/u01/app/domains/chdr-
prd/applications:/u01/app/domains/chdr-prd/lib/commons-collections-
3.2.jar:/u01/app/domains/chdr-prd/lib/commons-dbcp-1.2.1.jar:/u01/app/domains/chdr-
prd/lib/commons-pool-1.2.jar
```

Arguments: chdr-prod.ms1

```
-server -Xms5g -Xmx5g -XX:PermSize=256m -XX:MaxPermSize=1g -XX:-UseGCOverheadLimit -
XX:+DisableExplicitGC -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -
XX:+UseConcMarkSweepGC -Dweblogic.wsee.bind.suppressDeployErrorMessage=true -
Dgov.va.med.environment.production=true -Dweblogic.wsee.skip.async.response=true -
Dgov.va.med.environment.servertype=weblogic -Dweblogic.log.Log4jLoggingEnabled=false -
Dlog4j.configuration=file:/u01/app/domains/chdr-prd/lib/log4j.xml -
Dweblogic.configuration.schemaValidationEnabled=false -Dweblogic.Name=chdr-prd.ms1 -
Djava.security.auth.login.config=/u01/app/domains/chdr-prd/lib/CAIP_JAAS.config -
DDSKey.store=/u01/app/domains/chdr-prd/lib/CAIP_Keystore.jks -
Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBeanServerBu
ilder -javaagent:/u01/app/appdynamics/javaagent.jar -XX:-UseSplitVerifier -
Djavax.net.ssl.trustStore=/u01/app/domains/chdr-prd/trust.jks -
Djavax.net.ssl.trustStorePassword=chdrTrust -
Djavax.net.ssl.keyStore=/u01/app/domains/chdr-prd/identity.jks -
Djavax.net.ssl.keyStorePassword=Chdr123qw -Dweblogic.log.DisplayPatchInfo=true -
Dhttps.protocols=TLSv1.2 -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.2
```

Arguments: chdr-prod.ms2 - .ms6

```
-server -Xms4g -Xmx4g -XX:CompileThreshold=8000 -XX:PermSize=256m -XX:MaxPermSize=512m
-XX:SurvivorRatio=12 -XX:+UseConcMarkSweepGC -XX:+UseParNewGC -

Dweblogic.wsee.bind.suppressDeployErrorMessage=true -

Dgov.va.med.environment.production=true -

Dweblogic.wsee.skip.async.response=true -

Dgov.va.med.environment.servertype=weblogic -

Dweblogic.log.Log4jLoggingEnabled=false -

Dlog4j.configuration=file:/u01/app/domains/chdr-prd/lib/log4j.xml -

Dweblogic.configuration.schemaValidationEnabled=false -

Dweblogic.Name=chdr-prd.ms2 -Djava.security.auth.login.config=/u01/app/domains/chdr-
prd/lib/CAIP_JAAS.config -

DDSKey.store=/u01/app/domains/chdr-prd/lib/CAIP_Keystore.jks -

Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBeanServerBu
ilder -

javaagent:/u01/app/appdynamics/javaagent.jar -

XX:-UseSplitVerifier -

Djavax.net.ssl.trustStore=/u01/app/domains/chdr-prd/trust.jks -

Djavax.net.ssl.trustStorePassword=chdrTrust -

Djavax.net.ssl.keyStore=/u01/app/domains/chdr-prd/identity.jks -

Djavax.net.ssl.keyStorePassword=Chdr123qw -

Dweblogic.log.DisplayPatchInfo=true -
```

```
Dhttps.protocols=TLSv1.2 -
Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.2
```

The Server Start tab can be found by executing the following steps:

1 Log into the respective WebLogic console.

2 In the Domain Structure window expand Environments.

3 Click on Servers.

4 Click on a server in the Server table to pull up the server configuration.

5 Select the Server Start tab and locate the Arguments box.

6 In the Change Center box in the top left corner of the screen click Lock & Edit.

7 Enter the respective parameters described above and click the Save button.

Once all the preceding steps have been taken for installing and configuring a baseline domain, restart all the servers including the admin server.

4.9 CHDR Application Deployment

In the chdr domain directory on both machines verify directories DOMAIN_HOME/applications and DOMAIN_HOME/lib exist.

Verify DOMAIN_HOME/applications/chdr-core/core.properties file contains the correct production information.

Verify the DOMAIN_HOME/lib directory contains the updated and required libraries for the new CHDR application.

Retain current production CAIP_* files within the DOMAIN_HOME/lib directory but replace all other libraries with those in the chdr-lib.tar file provided with the new .ear file. The list of libraries should be as follows:

```
-rw-------  1 weblogic weblogic  121757 Apr 22  2021 commons-dbcp-1.2.2.jar
-rw-------  1 weblogic weblogic   62103 Apr 22  2021 commons-pool-1.3.jar
-rwx------  1 weblogic weblogic  102394 May  6  2021 jmxtools-1.2.jar
-rwx------  1 weblogic weblogic   38015 May  6  2021 commons-logging-1.0.4.jar
-rw-------  1 weblogic weblogic  571259 May  6  2021 commons-collections-3.2.jar
-rwx------  1 weblogic weblogic   53241 May  6  2021 com.bea.core.apache.commons.logging_1.1.0.jar
-rwx------  1 weblogic weblogic  194354 May  6  2021 xml-apis.jar
-rwx------  1 weblogic weblogic 1223877 May  6  2021 xercesImpl.jar
-rwx------  1 weblogic weblogic 3176148 May  6  2021 xalan-2.7.1.jar
-rwx------  1 weblogic weblogic   34313 May  6  2021 wllog4j.jar
-rwx------  1 weblogic weblogic    5197 May  6  2021 wlcommons-logging.jar
-rwx------  1 weblogic weblogic  278281 May  6  2021 serializer.jar
-rwx------  1 weblogic weblogic   84091 May  6  2021 resolver.jar
```

```
-rw-------  1 weblogic weblogic     702 May  6  2021 readme.txt
-rwx------  1 weblogic weblogic    6501 May  6  2021 log4j.xml.kaajee
-rwx------  1 weblogic weblogic    5707 May  6  2021 log4j.xml
-rwx------  1 weblogic weblogic    6945 May  6  2021 log4j.dtd
-rwx------  1 weblogic weblogic  391834 May  6  2021 log4j-2.17.1.jar
```

4.10 Installation Verification Procedure

Monitor the Audited_Events table in the database and all 6 managed server WebLogic log files for Faults and exceptions and if the deployment is not working and cannot be corrected, perform the rollback by bringing the previous domain back online.

4.11 System Configuration

The RFC outlines any needed system configurations.

4.12 Database Tuning

Not applicable for CHDS*2.2*1.

5 Back-Out Procedure

The RFC outlines the back-out procedures.

5.1 Back-Out Strategy

Take CHDS*2.2*1 domain offline and bring the previous domain back online.

5.2 Back-Out Considerations

Back-out would only be considered if there was a catastrophic failure that causes loss of function for the application or a significant patient impact issue.

5.2.1 Load Testing

Not applicable for CHDS*2.2*1.

5.2.2 User Acceptance Testing

Not applicable for CHDS*2.2*1.

5.3 Back-Out Criteria

Back-out would only be considered if there was a catastrophic failure that causes loss of function for the application or a significant patient impact issue.

5.4 Back-Out Risks

A back-out would result in security vulnerabilities by reinstating the non-TRM compliant versions of software.

5.5 Authority for Back-Out

AITC and the HPSCLIN team have the authority to collaborate a back-out of CHDS*2.2*1.

5.6 Back-Out Procedure

1. Take new WebLogic domain offline.
2. Bring old WebLogic domain online.
3. Verify message processing is restored.
4. Triage reasons for failure of new domain deployment.

5.7 Back-out Verification Procedure

Monitor the Audited_Events table in the database and all 6 managed server WebLogic log files.

6 Rollback Procedure

Not applicable for CHDS*2.2*1.

6.1 Rollback Considerations

Not applicable for CHDS*2.2*1.

6.2 Rollback Criteria

Not applicable for CHDS*2.2*1.

6.3 Rollback Risks

Not applicable for CHDS*2.2*1.

6.4 Authority for Rollback

Not applicable for CHDS*2.2*1.

6.5 Rollback Procedure

Not applicable for CHDS*2.2*1.

6.6 Rollback Verification Procedure

Not applicable for CHDS*2.2*1.