VistA Services Assembler Phase 2 (VSA-P2)
Joint Legacy Viewer (JLV) 2.5.1
Deployment, Installation, Backout, and Rollback (DIBR) Guide

Version 1.1

November 2016

Department of Veterans Affairs (VA)

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
11/29/2016	1.1	Resubmitted with client comments addressed	AbleVets
11/22/2016	1.0	Draft submitted for review CLIN 0003AL	AbleVets
11/10/2016	0.1	Initial draft of the document	AbleVets

Artifact Rationale

This document describes the Deployment, Installation, Backout, and Rollback Plan 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, Backout, and Rollback Plan 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

Table of Figures

Table of Tables

1 Introduction

The Joint Legacy Viewer (JLV) is a graphical user interface (GUI) that displays data from the Department of Veterans Affairs (VA) electronic health record (EHR) systems, the Department of Defense (DoD) electronic medical record (EMR) systems, and VA and DoD Virtual Lifetime Electronic Record (VLER) community partners, in a single user interface. The JLV web application provides a common data display of view-only, real-time patient information.

Authorized DoD and VA users can view patient records through JLV, which provides a combined view of patient record data. The combined view will group similar data from each health information system and display them chronologically on a single screen, eliminating the need to access two separate applications.

1.1 Purpose

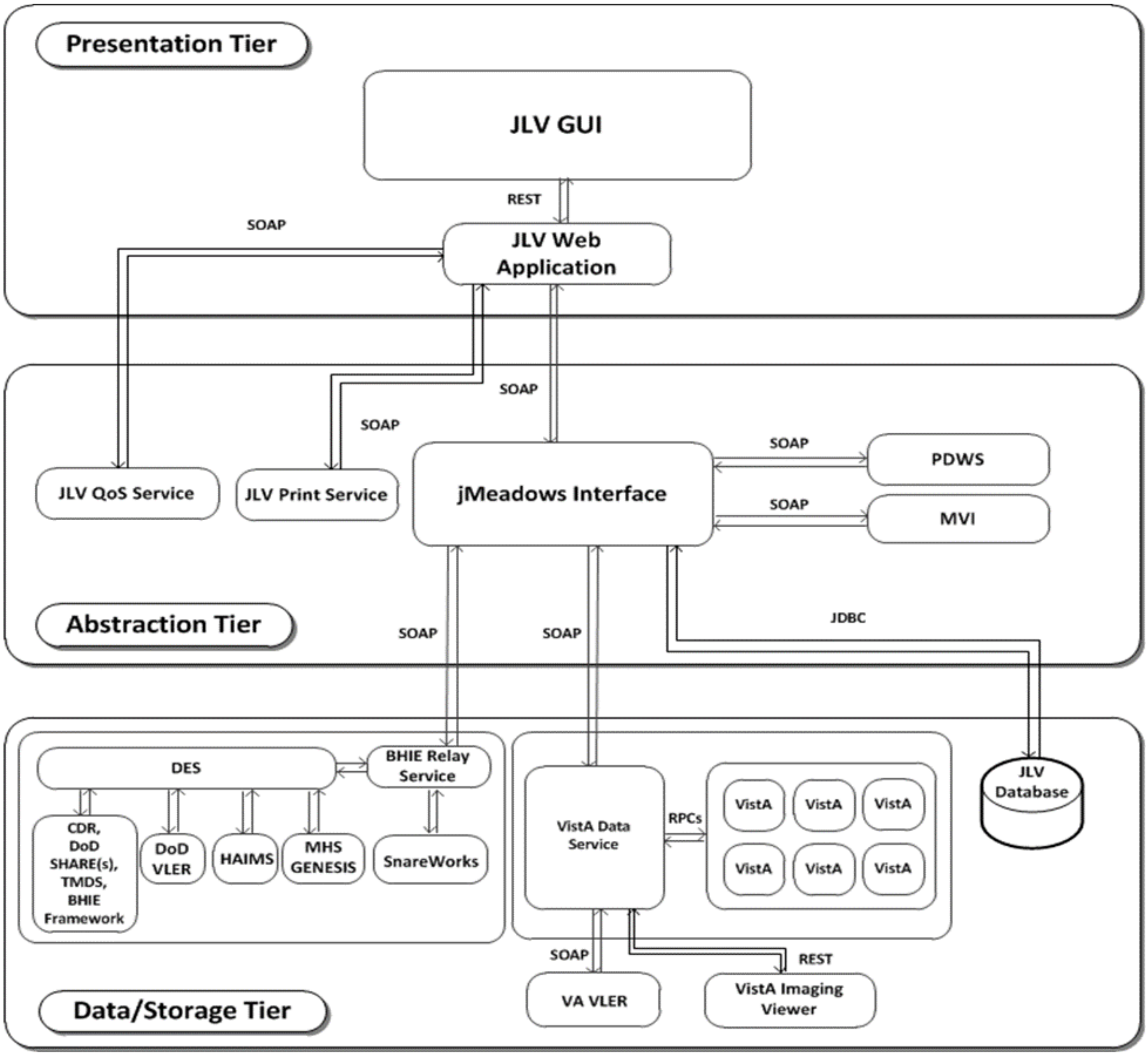
The Installation, Backout, and Rollback (DIBR) Guide provides a single, common document that defines the ordered, technical steps required to install the JLV product version 2.5.1. Further, it outlines the steps to back out the installation, and roll back to the previously installed version of the product, if necessary. The installation process is to be completed at the two VA data centers, located at the Austin Information Technology Center (AITC), and the Philadelphia Information Technology Center (PITC).

The JLV system specifications can be found in the CLIN 0003AA JLV 2.5.1 System Design Document, in Section 4, System Architecture. Once submitted, the document will be available on the Technical Services Project Repository (TSPR)[1].

Figure 1 illustrates the main components of JLV, and the messaging protocols that communicate within, and between, tiers in the system.

[1] **NOTE:** Access to TSPR is restricted, and must be requested.

Figure 1: JLV Architecture and Components



1.2 Dependencies

Currently, JLV is dependent on ancillary systems that connect the application to specific data sources. If any of these sources encounter a disruption in data services, the data will not be pulled over into JLV.

JLV is also dependent on internal VA updating processes that include database flips and updates to the servers and security patches. If any of the Enterprise VA Operational Procedures disrupt the normal operation of JLV, the application will not be functional.

1.3 Constraints

The physical environments held at AITC and PITC, which provide security and environmental control over the JLV servers, is restricted by Elevated Privilege (EP) access. Limitations with EP access coincides with the ability to respond to technical impacts to the servers. There are also constraints on the hosting sites, where multiple interests impact service technicians as they balance their job responsibilities.

Compliance standards are set by Section 508 of the Rehabilitation Act of 1973, which requires federal agencies to provide software and website accessibility to people with disabilities. These standards are tested and approved prior to delivery of the production code. 508 compliance will be met by the submission of the Final Section 508 Compliance Test Results report. Once submitted, the document will be available on the TSPR.

Monitoring performance metrics are completed on a weekly cycle.

2 Roles and Responsibilities

Tables 1 and 2, below, outline the project and DIBR roles and responsibilities. The JLV Support team is comprised of the AbleVets Systems Administrators and Engineers.

Table 1: Project Roles and Responsibilities

Name	Title/Group	Company
Latricia (Renae) Facundus	Enterprise Program Management Office (EPMO)/ Authorization Approval and Project Manager (PM)	VA
Chad Guebert	Contract PM Lead	AbleVets
Brad Goo	Technical Lead/Application Architect	Hawaii Resource Group (HRG) Technologies LLC
Michael Cardenas	Application Support/Sr. System Engineer, JLV Support Team	HRG Technologies LLC
Gene Sanchez	Enterprise Operations/ Application Manager	Leidos
Meltron Kendrick	System Administrator/Systems	Technatomy
Jose Negron	System Engineer/Data Center	ByLight

Table 2: Deployment, Installation, Backout, and Rollback Roles and Responsibilities

Team	Phase/Role	Tasks	Project Phase (See Table 6)
JLV Support	Deployment	Plan and schedule deployment (including orchestration with vendors)	Phase 0
JLV Support	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Phase 0
JLV Support	Deployment	Test for operational readiness	Phase 0
JLV Support	Deployment	Execute deployment	Phase 0

Team	Phase/Role	Tasks	Project Phase (See Table 6)
JLV Support	Installation	Plan and schedule installation	Phase 0
JLV Support	Installation	Ensure authority to operate and that certificate authority security documentation is in place	Phase 0
JLV Support	Installation	Validate through facility Point of Contact (POC) to ensure that Information Technology (IT) equipment has been accepted using asset inventory processes	Phase 0
JLV Support	Installation	Coordinate training	Phase 0
JLV Support	Backout	Confirm availability of backout instructions and backout strategy (What are the criteria that trigger a backout?)	Phase 0
JLV Support	Post-Deployment	Hardware, Software and System Support	Phase 0

3 Deployment

The deployment of JLV is planned as a phased rollout.

- Once EPMO approval is complete, the JLV Support team schedules their deployment, in coordination with the VA environment team.
- An Automated Notification Request (ANR) is completed prior to the known effective downtime.
- Once deployment is complete in the production environment, production testing is verified by the JLV Support team. Please see Section 4.7, Access Requirements and Skills Needed for Installation, for additional information.
- If there is an issue with deployment, the JLV Support team and management will make a determination to proceed with backout. For more information, refer to Section 5.1, Backout Strategy.

3.1 Timeline

The deployment and installation have a duration of eight hours, per environment.

3.2 Site Readiness Assessment

The JLV application is already a production, enterprise-wide application being hosted at AITC and PITC. New versions of the JLV application will be applied to the specific host servers remotely, via EP access.

3.2.1 Deployment Topology (Targeted Architecture)

This section is not applicable to the deployment of JLV.

3.2.2 Site Information (Locations, Deployment Recipients)

The hosted site will be at the AITC and PITC VA Data Centers.

3.2.3 Site Preparation

Servers have the latest program updates and security patches. These updates are performed on a regularly-scheduled basis.

Table 3 describes preparation required by the site(s) prior to deployment.

Table 3: Site Preparation

Site	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
AITC/PITC	Security Patches	None identifiable	Implement/Verify	JLV Support
AITC/PITC	Program Updates	None identifiable	Implement/Verify	JLV Support

3.3 Resources

Descriptions of the hardware, software, facilities, and documentation are detailed in the following subsections.

3.3.1 Facility Specifics

The JLV application is deployed at both AITC and PITC Data Centers.

3.3.2 Hardware

Table 4 describes the hardware specifications required at each site prior to deployment. Please see Table 2, DIBR Roles and Responsibilities, for details about who is responsible for preparing the site to meet the hardware specifications.

Table 4: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Windows Server	2008 R2 Enterprise (64-bit)	N/A	Intel® Xeon® Central Processing Unit (CPU) E5-4650L 0 @ 2.6GHz, 2600 MHz (2 processors)	Dell	12 Servers for AITC 12 servers for PITC
Database (DB) Server	2008 R2 Enterprise (64-bit)	N/A	Intel® Xeon® CPU E5-4650L 0 @ 2.6GHz, 2600 MHz (2 processors)	Dell	2 Servers for AITC 2 servers for PITC

3.3.3 Software

Table 5 describes software specifications required at each site prior to deployment. Please see Table 2, DIBR Roles and Responsibilities, for details about who is responsible for preparing the site to meet the software specifications.

Table 5: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
DB Server	N/A	N/A	Microsoft (MS) Structured Query Language (SQL) Server 2008 R2	MS	N/A
Windows Server	N/A	N/A	Oracle WebLogic Server Version 10.3.6.	Oracle	N/A

3.3.4 Communications

JLV Support communicates with the VA Network team for implementation and backout activities via e-mail, Instant Message (IM), and phone.

3.3.4.1 Deployment/Installation/Backout Checklist

Table 6: Deployment, Installation, and Backout Checklist

Activity	Day	Time	Individual Who Completes Task
Deployment	Saturday	5:00 A.M. Easter Standard Time, (EST), with an expected completion time of 1:00 P.M. EST.	JLV Support
Installation	Saturday	5:00 A.M. EST, with an expected completion time of 1:00 P.M. EST.	JLV Support
Backout	As needed	As needed, with an eight hour expected completion time.	JLV Support

4 Installation

4.1 Pre-Installation and System Requirements

Please see Section 3.3.2, Hardware, and Section 3.3.3, Software, for information regarding pre-installation system requirements.

4.2 Platform Installation and Preparation

Refer to the JLV 2.5.1 Change Management (CM) Implementation Plan document for information about the installation and deployment of the JLV System. Once submitted, the document will be available on the TSPR.

Table 7: Implementation Plan Summary

Considerations	Associated Details
Affected Systems	Veterans Information System and Technology Architecture (VistA) Data Service (VDS)
Identify who is impacted by the Change	Users of the JLV Web Application
Estimated timeframe for restoring service	Eight hours
Required pre-implementation work	Download installation files

4.3 Download and Extract Files

All of the software installation files, their locations, and the chronological steps for downloading and extracting the software prior to installation, is held in a VA development location accessible via EP access.

4.4 Database Creation

The JLV database is an SQL Server 2008 database, and is used to store user profile information and audit records.

Refer to the CLIN 1003AA JLV 2.5.1 System Design Document for the database design overview, and details regarding the database tables. Once submitted, the document will be available on the TSPR.

4.5 Installation Scripts

Currently there are no installation scripts for the installation of JLV. The application is installed manually, with oversight by the JLV Support team.

4.6 Cron Scripts

Not applicable. There are no Cron Scripts that will be run.

4.7 Access Requirements and Skills Needed for Installation

Elevated permissions are required for installation activities. HRG System Engineers have been granted VA EP, and are designated to access the application servers for deployment, maintenance, and backout activities.

4.8 Installation Procedure

The following steps detail the installation of JLV system components in the AITC and PITC environments.

1. Update JLV databases in AITC-EO Cloud Environment (15-minute time estimate).
    a. Remote desktop into VAAUSJLVSQL201 server.
    b. Open Microsoft SQL Server Management Studio.

    c. Run the SQL Script “JLV_2.5.1_update.sql” (provided with the JLV 2.5.1 source code package submission).

2. Update JLV databases in PITC-EO Cloud Environment (15-minute time estimate).

    d. Remote desktop into VAPHIJLVSQL201 server.

    e. Open Microsoft SQL Server Management Studio.

    f. Run the SQL Script “JLV_2.5.1_update.sql” (provided with the JLV 2.5.1 source code package submission).

3. Install jMeadows in AITC - EO Cloud environment (30-minute time estimate).

    a. Remote desktop into VAAUSJLVWEB209 server.

    b. Upload the *jMeadows-[JLV version]-production.war* build to *D:\builds\* directory on VAAUSJLVWEB209 server.

    c. Previously deployed *jMeadows-[previous installation]-production.war* build remains as a backup in the *D:\builds\* directory.

    d. Open properties file of previously deployed jMeadows war file, validate all endpoints.

    e. Validate all external endpoints are available by testing network connectivity through telnet utility.

    f. Validate all external endpoint web services are available by testing connectivity through web browser on jMeadows servers.

    g. Ensure endpoints in properties file of the new build file match endpoints from the previous build:

        i. VISTA_URL = https://jlvvds-aitc.med.va.gov/VistaDataService/VistaDataService?wsdl
        ii. BHIE_RELAY_SERVICE_URL = http://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
        iii. PDWS_PS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?wsdl
        iv. PDWS_PR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientRetrieve?wsdl
        v. PDWS_FS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilySearch?wsdl
        vi. PDWS_FR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilyRetrieve?wsdl
        vii. PDWS_PROC_CODE = P
        viii. PDWS_SND_DEV_ID = 177610
        ix. MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
        x. JNDI_JDBC = jdbc/JanusSQL
        xi. JNDI_JDBC_ENCRYPTED = jdbc/JanusSQLTDE
        xii. RPC_ENDPOINT_ENVIRONMENT = nc_gold
        xiii. RPC_ENDPOINT_ENVIRONMENT = enterprise

        xiv. CACHE_ENDPOINT_ENVIRONMENT = enterprise
        xv. SHARE_ENDPOINT_ENVIRONMENT = enterprise
        xvi. MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
        xvii. AHLTA_ENDPOINT_ENVIRONMENT = enterprise
        xviii. USE_SNAREWORKS = true

    h. Log in to the WebLogic Server Administration Console on VAAUSJLVWEB209 server.

    i. Undeploy previously deployed jMeadows-[previous installation]-production.war build.

    j. Deploy the jMeadows-[JLV version]-production.war build from D:\builds\ directory to the jMeadows cluster. WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB209, VAAUSJLVWEB210, VAAUSJLVWEB211, VAAUSJLVWEB212) and stages it in the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

    k. Modify deployment configuration to use /jMeadows context root.

    l. Start application.

    m. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

    n. Validate jMeadows endpoint web service is available by testing connectivity through web browser on jMeadows servers.

4. Install jMeadows in PITC - EO Cloud environment (30-minute time estimate).

    a. Remote desktop into VAPHIJLVWEB209 server.

    b. Upload the *jMeadows-[JLV version]-production.war* build to *D:\builds\* directory on VAPHIJLVWEB209 server.

    c. Previously deployed *jMeadows-[previous installation]-production.war* build remains as a backup in the *D:\builds\* directory.

    d. Open properties file of previously deployed jMeadows war file, validate all endpoints.

    e. Validate all external endpoints are available by testing network connectivity through telnet utility.

    f. Validate all external endpoint web services are available by testing connectivity through web browser on jMeadows servers.

    g. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

        i. VISTA_URL = https://jlvvds-pitc.med.va.gov/VistaDataService/VistaDataService?wsdl
        ii. BHIE_RELAY_SERVICE_URL = http://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
        iii. PDWS_PS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?wsdl

iv. PDWS_PR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientRetrieve?wsdl

v. PDWS_FS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilySearch?wsdl

vi. PDWS_FR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilyRetrieve?wsdl

vii. PDWS_PROC_CODE = P

viii. PDWS_SND_DEV_ID = 177610

ix. MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService

x. JNDI_JDBC = jdbc/JanusSQL

xi. JNDI_JDBC_ENCRYPTED = jdbc/JanusSQLTDE

xii. RPC_ENDPOINT_ENVIRONMENT = nc_gold

xiii. RPC_ENDPOINT_ENVIRONMENT = enterprise

xiv. CACHE_ENDPOINT_ENVIRONMENT = enterprise

xv. SHARE_ENDPOINT_ENVIRONMENT = enterprise

xvi. MEDWEB_ENDPOINT_ENVIRONMENT = enterprise

xvii. AHLTA_ENDPOINT_ENVIRONMENT = enterprise

xviii. USE_SNAREWORKS = true

h. Log in to the WebLogic Server Administration Console on VAPHIJLVWEB209 server.

i. Undeploy previously deployed *jMeadows-[previous installation]-production.war* build.

j. Deploy the *jMeadows-[JLV version]-production.war* build from *D:\builds\* directory to the jMeadows cluster. WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB209, VAPHIJLVWEB210, VAPHIJLVWEB211, VAPHIJLVWEB212) and stages it in the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

k. Modify deployment configuration to use/jMeadows context root.

l. Start application.

m. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

n. Validate jMeadows endpoint web service is available by testing connectivity through web browser on jMeadows servers.

5. Install JLV web application in AITC-EO Cloud environment (30-minute time estimate).

a. Remote desktop into VAAUSJLVWEB201 server.

b. Upload the *JLV-[JLV version]-production.war* build to *D:\deployable\* directory on VAAUSJLVWEB201 server.

c. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

i. If unavailable, open properties file of previously deployed JLV war file and validate jMeadows endpoint.

d. Validate all jMeadows web service is available by testing connectivity through web browser on JLV web servers.

e. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

i. grails.jmeadowsURL = https://jlvmds-aitc.med.va.gov/jMeadows/JMeadowsDataService

ii. grails.dodVlerURL = https://sa-dtc.med.osd.mil/

iii. grails.jlvqosURL = https://vaausjlvweb209.aac.dva.va.gov/JLVQoS/JLVQoSDataService?wsdl

iv. grails.jlvprintURL = https://vaausjlvweb209.aac.dva.va.gov/JLVPrintService/JLVPrintService?wsdl

f. Log in to the WebLogic Server Administration Console on VAAUSJLVWEB201 server.

g. Undeploy previously deployed *JLV-[previous installation]-production.war* build.

h. Deploy the *JLV-[JLV version]-production.war* build from *D:\builds\* directory to the JLV cluster. WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB201, VAAUSJLVWEB202, VAAUSJLVWEB203, VAAUSJLVWEB204) and stages it in the directory path ${JLV_DOMAIN}\servers\${SERVER_NAME}\stage.

i. Modify deployment configuration to use /JLV context root.

j. Start application.

k. Validate JLV endpoint is available by testing network connectivity through telnet utility.

l. Validate JLV web portal is available by testing connectivity through web browser outside of the JLV servers using the public URL.

6. Install JLV web application in PITC-EO Cloud environment (30-minute time estimate).

a. Remote desktop into VAPHIJLVWEB201 server.

b. Upload the *JLV-[JLV version]-production.war* build to *D:\builds\* directory on VAPHIJLVWEB201 server.

c. Validate jMeadows endpoint is available by testing network connectivity through a telnet utility.

i. If unavailable, open properties file of previously deployed JLV war file and validate jMeadows endpoint.

d. Validate all jMeadows web service is available by testing connectivity through web browser on JLV web servers.

e. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

   i. grails.jmeadowsURL = https://jlvmds-aitc.med.va.gov/jMeadows/JMeadowsDataService
   ii. grails.dodVlerURL = https://sa-dtc.med.osd.mil/
   iii. grails.jlvqosURL = https://vaphijlvweb209.aac.dva.va.gov/JLVQoS/JLVQoSDataService?wsdl
   iv. grails.jlvprintURL = https://vaphijlvweb209.aac.dva.va.gov/JLVPrintService/JLVPrintService?wsdl

f. Log in to the WebLogic Server Administration Console on VAPHIJLVWEB201 server.

g. Undeploy previously deployed *JLV-[previous installation]-production.war* build.

h. Deploy the *JLV-[JLV version]-production.war* build from *D:\builds\* directory. WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB201, VAPHIJLVWEB202, VAPHIJLVWEB203, VAPHIJLVWEB204) and stages it in the directory path ${JLV_DOMAIN}\servers\${SERVER_NAME}\stage.

i. Modify deployment configuration to use /JLV context root.

j. Start application.

k. Validate JLV endpoint is available by testing network connectivity through telnet utility.

l. Validate JLV web portal is available by testing connectivity through web browser outside of the JLV servers using the public URL.

7. Install VistA Data Service in AITC-EO Cloud environment (15-minute time estimate).

   a. Remote desktop into *VAAUSJLVWEB205* server.

   b. Upload the *VistaDataService-[JLV version]-production.war* build to *D:\builds\* directory on *VAAUSJLVWEB205* server.

   c. Open properties file of previously deployed Vista Data Service war file, validate all endpoints.

   d. Validate that external endpoints are available by testing network connectivity through telnet utility.

   e. Validate that external endpoints are available by testing connectivity through web browser on Vista Data Service servers.

   f. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

      i. appconfig.vler.dq.url = nhiapp-prd.va.gov http://nhiapp-prd.va.gov/NHINAdapterGatewayDocQuery/EntityDocQuery?wsdl
      ii. appconfig.vler.dr.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayDocRetrieve/EntityDocRetrieve?wsdl

        iii. appconfig.vler.pd.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayPatientDiscovery/EntityPatientDiscovery?wsdl
        iv. appconfig.vler.pa.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayPatientAnnounce/AnnouncePatientService

    g. Log in to the WebLogic Server Administration Console on *VAAUSJLVWEB205* server.

    h. Undeploy previously deployed *VistaDataService-[previous installation]-production.war* build.

    i. Deploy the *VistaDataService-[JLV version]-production.war* build from *D:\builds\* directory. WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB205, VAAUSJLVWEB206, VAAUSJLVWEB207, VAAUSJLVWEB208) and stages it in the directory path ${JLVVDS_DOMAIN}\servers\${SERVER_NAME}\stage.

    j. Modify deployment configuration to use /VistaDataService context root.

    k. Start application.

    l. Validate that VistA Data Service endpoint is available by testing network connectivity through telnet utility.

    m. Validate that VistA Data Service endpoint is available by testing connectivity through web browser on Vista Data Service servers.

8. Install VistA Data Service in PITC-EO Cloud environment (15-minute time estimate).

    a. Remote desktop into *VAPHIJLVWEB205* server.

    b. Upload the *VistaDataService-[JLV version]-production.war* build to *D:\builds\* directory on *VAPHIJLVWEB205* server.

    c. Open properties file of previously deployed Vista Data Service war file, validate all endpoints.

    d. Validate that external endpoints are available by testing network connectivity through telnet utility.

    e. Validate that external endpoints are available by testing connectivity through web browser on Vista Data Service servers.

    f. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

        i. appconfig.vler.dq.url = nhiapp-prd.va.gov http://nhiapp-prd.va.gov/NHINAdapterGatewayDocQuery/EntityDocQuery?wsdl
        ii. appconfig.vler.dr.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayDocRetrieve/EntityDocRetrieve?wsdl
        iii. appconfig.vler.pd.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayPatientDiscovery/EntityPatientDiscovery?wsdl

iv. appconfig.vler.pa.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayPatientAnnounce/AnnouncePatientService

g. Log in to the WebLogic Server Administration Console on *VAPHIJLVWEB205* server.

h. Undeploy previously deployed *VistaDataService-[previous installation]-production.war* build.

i. Deploy the *VistaDataService-[JLV version]-production.war* build from *D:\builds\* directory. WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB205, VAPHIJLVWEB206, VAPHIJLVWEB207, VAPHIJLVWEB208) and stages it in the directory path ${JLVVDS_DOMAIN}\servers\${SERVER_NAME}\stage.

j. Modify deployment configuration to use /VistaDataService context root.

k. Start application.

l. Validate that VistA Data Service endpoint is available by testing network connectivity through telnet utility.

m. Validate that VistA Data Service endpoint is available by testing connectivity through web browser on Vista Data Service servers.

9. Install JLV Print Service in PITC-EO Cloud environment (15-minute time estimate).

a. Remote desktop into *VAPHIJLVWEB209* server.

b. Upload the *JLVPrintService-[JLV version]-.war* build to *D:\builds\* directory on *VAPHIJLVWEB209* server.

c. Log in to the WebLogic Server Administration Console on *VAPHIJLVWEB209* server.

d. Undeploy previously deployed *JLVPrintService* build, if they exist.

e. Deploy the *JLVPrintService-[JLV version]-production.war* build from *D:\builds\* directory. WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB210, VAPHIJLVWEB211, VAPHIJLVWEB212).

f. Start application.

g. Validate that JLV Print Service endpoint is available by testing network connectivity through telnet utility.

h. Validate that JLV Print Service endpoint is available by testing connectivity through web browser on JLV Print Service servers.

10. Install JLV Print Service in AITC-EO Cloud environment (15-minute time estimate).

i. Remote desktop into *VAAUSJLVWEB209* server.

j. Upload the *JLVPrintService-[JLV version]-.war* build to *D:\builds\* directory on *VAAUSJLVWEB205* server.

k. Log in to the WebLogic Server Administration Console on *VAAUSJLVWEB209* server.

   l. Undeploy previously deployed *JLVPrintService* build, if they exist.

   m. Deploy the *JLVPrintService-[JLV version]-production.war* build from *D:\builds\* directory to server VAAUSJLVWEB210. WebLogic stages a copy of the .war file to the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

   n. Modify deployment configuration to use /JLVPrintService context root.

   o. Start application.

   p. Validate that JLV Print Service endpoint is available by testing network connectivity through telnet utility.

   q. Validate that JLV Print Service endpoint is available by testing connectivity through web browser on JLV Print Service servers.

11. Install JLV QOS Service in AITC-EO Cloud environment (15-minute time estimate).

   a. Remote desktop into *VAAUSJLVWEB209* server.

   b. Upload the *JLVQOS-[JLV version]-.war* build to *D:\builds\* directory on *VAAUSJLVWEB209* server.

   c. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

      i. ENV = AITC
      ii. JMEADOWS_URL = https://jlvmds.med.va.gov/jMeadows/JMeadowsDataService?wsdl
      iii. VISTA_URL = https://jlvvds-aitc.med.va.gov/VistaDataService/VistaDataService?wsdl
      iv. BHIE_RELAY_SERVICE_URL = https://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
      v. PDWS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?WSDL
      vi. MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
      vii. JNDI_JDBC = jdbc/JanusSQL_24
      viii. RPC_ENDPOINT_ENVIRONMENT = enterprise
      ix. CACHE_ENDPOINT_ENVIRONMENT = enterprise
      x. SHARE_ENDPOINT_ENVIRONMENT = enterprise
      xi. MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
      xii. AHLTA_ENDPOINT_ENVIRONMENT = enterprise
      xiii. SERVICE_MONITOR_TEST_BRS = TRUE
      xiv. SERVICE_MONITOR_TEST_JMDS = TRUE
      xv. SERVICE_MONITOR_TEST_MVI = TRUE
      xvi. SERVICE_MONITOR_TEST_PDWS = TRUE
      xvii. SERVICE_MONITOR_TEST_VDS = TRUE
      xviii. SERVICE_MONITOR_TEST_SHARE = FALSE
      xix. SERVICE_MONITOR_TEST_SNAREWORKS = TRUE
      xx. SERVICE_MONITOR_TEST_VISTA_SITES = FALSE

xxi. EMAIL_HOST = smtp.va.gov
xxii. EMAIL_SSL_PORT = 465
xxiii. EMAIL_FROM = jlv@hawaiirg.com
xxiv. EMAIL_TO = JLVQoS@HawaiiRG.com
xxv. EMAIL_SRC_SYS = AITC

d. Log in to the WebLogic Server Administration Console on *VAAUSJLVWEB209* server.

e. Undeploy previously deployed *JLVQOS* build.

f. Deploy the *JLVQoS-[JLV version]-production.war* build from *D:\builds\* directory. WebLogic distributes the .war file to the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

g. Modify deployment configuration to use /JLVQoS context root.

h. Start application.

i. Validate that JLV QoS endpoint is available by testing network connectivity through telnet utility.

j. Validate that JLV QoS endpoint is available by testing connectivity through web browser on JLV QoS servers.

12. Install JLV QOS Service in PITC-EO Cloud environment (15-minute time estimate).

a. Remote desktop into *VAPHIJLVWEB209* server.

b. Upload the *JLVQOS-[JLV version]-.war* build to *D:\builds\* directory on *VAPHIJLVWEB209* server.

c. Log in to the WebLogic Server Administration Console on *VAPHIJLVWEB209* server.

d. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

i. ENV = PITC
ii. JMEADOWS_URL = https://jlvmds-pitc.med.va.gov/jMeadows/JMeadowsDataService?wsdl
iii. VISTA_URL = https://jlvvds-pitc.med.va.gov/VistaDataService/VistaDataService?wsdl
iv. BHIE_RELAY_SERVICE_URL = https://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
v. PDWS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?WSDL
vi. MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
vii. JNDI_JDBC = jdbc/JanusSQL_24
viii. RPC_ENDPOINT_ENVIRONMENT = enterprise
ix. CACHE_ENDPOINT_ENVIRONMENT = enterprise
x. SHARE_ENDPOINT_ENVIRONMENT = enterprise
xi. MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
xii. AHLTA_ENDPOINT_ENVIRONMENT = enterprise

xiii. SERVICE_MONITOR_TEST_BRS = TRUE
xiv. SERVICE_MONITOR_TEST_JMDS = TRUE
xv. SERVICE_MONITOR_TEST_MVI = TRUE
xvi. SERVICE_MONITOR_TEST_PDWS = TRUE
xvii. SERVICE_MONITOR_TEST_VDS = TRUE
xviii. SERVICE_MONITOR_TEST_SHARE = FALSE
xix. SERVICE_MONITOR_TEST_SNAREWORKS = TRUE
xx. SERVICE_MONITOR_TEST_VISTA_SITES = FALSE
xxi. EMAIL_HOST = smtp.va.gov
xxii. EMAIL_SSL_PORT = 465
xxiii. EMAIL_FROM = jlv@hawaiirg.com
xxiv. EMAIL_TO = JLVQoS@HawaiiRG.com
xxv. EMAIL_SRC_SYS = PITC

e. Undeploy previously deployed *JLVQOS* build.

f. Deploy the *JLVQoS-[JLV version]-production.war* build from *D:\builds\* directory to server VAPHIJLVWEB209. WebLogic distributes the .war file to the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

g. Start application.

h. Modify deployment configuration to use /JLVQoS context root.

i. Validate that JLV QoS endpoint is available by testing network connectivity through telnet utility.

j. Validate that JLV QoS endpoint is available by testing connectivity through web browser on JLV QoS servers.

4.9 Installation Verification Procedure

After completing the process detailed in Section 4.8, Installation Procedure, perform the steps below to validate the installation and deployment.

Validate and test the application using test patients; CHDR 1 and CHDR 2:

1. Log in as VA user.
2. Validate Patient Search Patient Discovery Web Service (PDWS).
3. Validate VA Master Veteran Index (MVI).
4. Validate the VistA Data Service by ensuring VA data is being returned.
5. Validate that the jMeadows interface with the BHIE Relay Service is functional by ensuring DoD data is being returned.
6. Validate that VA Terminology mapping is occurring.
7. Validate that DoD Terminology mapping is occurring.
8. Validate the Health Monitor (Quality of Service (QoS)) Service.
9. Validate the JLV Print Service.

4.10 System Configuration

Table 8 describes the server configurations for JLV enterprise production infrastructure, hosted at the AITC and PITC data centers.

Table 8: JLV Server Configuration

Server Type	Server Specifics
JLV Web Application Servers	Four (4) servers each, with four (6) processors @2.26GHz and 16 Gigabyte (GB) Random Access Memory (RAM)
VDS Servers	Four (4) servers each, with four (6) processors @2.26GHz and 16 GB RAM
jMeadows Service Servers	Four (4) servers each, with four (6) processors @2.26GHz and 16 GB RAM
DB Servers	Two (2) servers each, with four (8) processors @2.26GHz and 28 GB RAM

4.11 Database Tuning

Not applicable.

4.12 Notification of Test Results

After completing the validation and testing steps, the test results will be provided to the JLV Management team, Information Assurance (IA) team, and VA Management team.

If testing/validation has failed, and the decision is made to restore the previous version of JLV:

- Notify the JLV Management team, IA team, VA Management team, and the Network Administrators as necessary, including the following teams:
  - Data Exchange Service (DES) team
  - JLV Management team

5 Backout Procedure

5.1 Backout Strategy

Refer to the JLV 2.5.1 CM Implementation Plan document, for the CM backout procedure. Once submitted, the document will be available on the TSPR.

The procedures involve backing out, or uninstalling, the currently deployed JLV system components, and restoring the previously-deployed version of JLV.

Table 9: Backout Plan Summary

Backout Plan Considerations	Associated Details
Affected systems	VistA Data Service
Identification of those who are impacted by the change	Users of the JLV Web Application
Estimated timeframe for restoring the service	Thirty minutes

Backout Plan Considerations	Associated Details
Required pre-implementation work	Not applicable

5.2 Backout Considerations

The following rollback points have been identified as the criteria for initiating the Backout Plan:

- The JLV application, as tested by the JLV Support team, does not operate as intended

5.2.1 Load Testing

Testers are unable to log into the JLV application in the production environment.

5.2.2 User Acceptance Testing

Validate and test the application using test patients CHDR 1 and CHDR 2:

1. Log in as a VA user.
2. Validate Patient Search PDWS.
3. Validate VA MVI.
4. Validate the VDS by ensuring VA data is being returned.
5. Validate that the jMeadows interface with the BHIE Relay Service is functional by ensuring DoD data is being returned.
6. Validate that VA terminology mapping is occurring.
7. Validate that DoD terminology mapping is occurring.
8. Validate the Health Monitor QoS Service.
9. Validate the JLV Print Service.

5.3 Backout Criteria

The JLV application, as tested by JLV Support, does not operate as intended.

5.4 Backout Risks

A backout is performed to uninstall the installed components if the JLV deployment did not pass the Installation Verification Procedure outlined in Section 4.9. The back out procedure restores the previously-deployed version of JLV. The risks for executing the back out are minimal as a back out is performed during previously announced downtime, and users are not accessing the system. Therefore, users would not have accessed the new JLV version and/or changes to user configuration files would not have occurred. When the restored system is online and validated, user access would continue as before.

If the backout plan is initiated later in the deployment window, restoration time may exceed the planned downtime for deployment. This risk is mitigated by scheduling deployments for weekends and other times when expected usage levels are low.

5.5 Authority for Backout

If a backout is necessary, approval for the backout will come from the current VA PM, Renae Facundus.

5.6 Backout Procedure

The following steps detail the uninstallation of JLV components in the AITC and PITC environments.

1. Uninstall jMeadows in EO Cloud environment.
    a. Remote desktop into *VAAUSJLVWEB209* server.
    b. Log into WebLogic Server Administration Console on *VAAUSJLVWEB209* server.
    c. In the WebLogic Server Administration Console, undeploy the *jMeadows-[JLV version]-production.war* build. WebLogic will also undeploy it from the clustered server servers (VAAUSJLVWEB206, VAAUSJLVWEB207, VAAUSJLVWEB208).
    d. In the WebLogic Server Administration Console, deploy *jMeadows-[previous installation]-production.war* build located in the builds directory *D:\deployable\*. WebLogic will also deploy it to the clustered servers (VAAUSJLVWEB206, VAAUSJLVWEB207, VAAUSJLVWEB208).
    e. Start the application.
    f. Validate all external endpoints are available by testing network connectivity through telnet utility.
    g. Validate all external endpoint web services are available by testing connectivity through web browser on jMeadows servers.
2. Uninstall JLV web application in AITC - EO Cloud environment.
    a. Remote desktop into VAAUSJLVWEB201 server.
    b. Log into WebLogic Server Administration Console on *VAAUSJLVWEB201* server.
    c. In the WebLogic Server Administration Console, undeploy the *JLV-[JLV version]-production.war* build. WebLogic will also undeploy it from the clustered server *VAAUSJLVWEB201*.
    d. In the WebLogic Server Administration Console, deploy *JLV-[previous installation]-production.war* build located in the builds directory *D:\deployable\*. WebLogic will also deploy it to the clustered servers (VAAUSJLVWEB202,VAAUSJLVWEB203, VAAUSJLVWEB204).
    e. Start the application.
    f. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.
    g. Validate jMeadows web service is available by testing connectivity through web browser on JLV web servers.

3. Uninstall JLV web application in PITC - EO Cloud environment.
    a. Remote desktop into VAPHIJLVWEB201 server.
    b. Log into WebLogic Server Administration Console on *VAPHIJLVWEB201* server.
    c. In the WebLogic Server Administration Console, undeploy the *JLV-[JLV version]-production.war* build. WebLogic will also undeploy it from the clustered server *VAPHIJLVWEB201*.
    d. In the WebLogic Server Administration Console, deploy *JLV-[previous installation]-production.war* build located in the builds directory *D:\deployable\*. WebLogic will also deploy it to the clustered servers (VAPHIJLVWEB202,VAPHIJLVWEB203, VAPHIJLVWEB204).
    e. Start the application.
    f. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.
    g. Validate jMeadows web service is available by testing connectivity through web browser on JLV web servers.
4. Uninstall VistA Data Service in AITC-EO Cloud environment.
    a. Remote desktop into *VAAUSJLVWEB205* server.
    b. Log into WebLogic Server Administration Console on *VAAUSJLVWEB205* server.
    c. In the WebLogic Server Administration Console, undeploy the *VistaDataService-[JLV version]-production.war* build. WebLogic will also undeploy it from the clustered server *VAAUSJLVWEB205*.
    d. In the WebLogic Server Administration Console, deploy *VistaDataService-[previous installation]-production.war* build located in the builds directory *D:\deployable\*. WebLogic will also deploy it to the clustered servers (VAAUSJLVWEB206, VAAUSJLVWEB207, VAAUSJLVWEB208).
    e. Start the application.
    f. Validate that external endpoints are available by testing network connectivity through telnet utility.
    g. Validate that external endpoints are available by testing connectivity through web browser on Vista Data Service servers.
5. Uninstall VistA Data Service in PITC-EO Cloud environment.
    a. Remote desktop into *VAPHIJLVWEB205* server.
    b. Log into WebLogic Server Administration Console on *VAPHIJLVWEB205* server.
    c. In the WebLogic Server Administration Console, undeploy the *VistaDataService-[JLV version]-production.war* build. WebLogic will also undeploy it from the clustered server *VAPHIJLVWEB205*.
    d. In the WebLogic Server Administration Console, deploy *VistaDataService-[previous installation]-production.war* build located in the builds directory *D:\deployable\*.

    WebLogic will also deploy it to the clustered servers (VAPHIJLVWEB206, VAPHIJLVWEB207, VAPHIJLVWEB208).

    e. Start the application.
    f. Validate that external endpoints are available by testing network connectivity through telnet utility.
    g. Validate that external endpoints are available by testing connectivity through web browser on Vista Data Service servers.

6. Recreate JLV database in AITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into VAAUSJLVSQL201.
    b. Recreate the tables of the previous version of the JLV database using the JLV.mdf and JLV_log.ldf files from system backups.
7. Recreate JLV database in PITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into VAAUSJLVSQL201.
    b. Recreate the tables of the previous version of the JLV database using the JLV.mdf and JLV_log.ldf files from system backups.
8. Uninstall JLV Print Service in AITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into *VAAUSJLVWEB209* server.
    b. Upload the *JLVPrintService-[JLV version]-.war* build to *D:\deployable\* directory on *VAAUSJLVWEB205* server.
    c. Log in to the WebLogic Server Administration Console on *VAAUSJLVWEB209* server.
    d. Undeploy previously deployed *JLVPrintService* build, if they exist.
    e. Deploy the *JLVPrintService-[JLV version]-production.war* build from *D:\deployable\* directory. WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB210, VAAUSJLVWEB211, VAAUSJLVWEB212).
    f. Start application.
9. Uninstall JLV Print Service in PITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into *VAPHIJLVWEB209* server.
    b. Upload the *JLVPrintService-[JLV version]-.war* build to *D:\deployable\* directory on *VAPHIJLVWEB209* server.
    c. Log in to the WebLogic Server Administration Console on *VAPHIJLVWEB209* server.
    d. Undeploy previously deployed *JLVPrintService* build, if they exist.
    e. Deploy the *JLVPrintService-[JLV version]-production.war* build from *D:\deployable\* directory. WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB210, VAPHIJLVWEB211, VAPHIJLVWEB212).

   f. Start application.

10. Uninstall JLV QoS Service in the AITC-EO Cloud environment (15-minute time estimate).

    a. Remote desktop into VAAUSJLVWEB209 server.
    b. Upload the *JLVQoSService-[JLV version]-.war* build to *D:\deployable\* directory on *VAAUSJLVWEB205* server.
    c. Log in to the WebLogic Server Administration Console on *VAAUSJLVWEB209* server.
    d. Undeploy previously deployed *JLVQoSService* build, if they exist.
    e. Deploy the *JLVQoSService-[JLV version]-production.war* build from *D:\deployable\* directory. WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB210, VAAUSJLVWEB211, VAAUSJLVWEB212).
    f. Start application.

11. Uninstall JLV QoS Service in the PITC-EO Cloud environment (15-minute time estimate).

    a. Remote desktop into *VAPHIJLVWEB209* server.
    b. Upload the *JLVQoSService-[JLV version]-.war* build to *D:\deployable\* directory on *VAPHIJLVWEB209* server.
    c. Log in to the WebLogic Server Administration Console on *VAPHIJLVWEB209* server.
    d. Undeploy previously deployed *JLVQoSService* build, if they exist.
    e. Deploy the *JLVQoSService-[JLV version]-production.war* build from *D:\deployable\* directory. WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB210, VAPHIJLVWEB211, VAPHIJLVWEB212).
    f. Start application.

5.7 Backout Verification Procedure

Validate the backout procedure by completing the steps below.

Validate and test the application using test patients CHDR 1 and CHDR 2:

1. Log in as VA user.
2. Validate Patient Search PDWS.
3. Validate VA MVI.
4. Validate the VistA Data Service by ensuring VA data is being returned.
5. Validate that the jMeadows interface with the BHIE Relay Service is functional by ensuring DoD data is being returned.
6. Validate that VA Terminology mapping is occurring.

7. Validate that DoD Terminology mapping is occurring.
8. Validate the Health Monitor QoS service.
9. Validate the JLV Print Service.

6 Rollback Procedure

Refer to Section 5.6, Backout Procedure.

6.1 Rollback Considerations

The JLV application, as tested by the JLV Support team, does not operate as intended.

6.2 Rollback Criteria

The JLV application, as tested by the JLV Support team, does not operate as intended.

6.3 Rollback Risks

A rollback is performed to uninstall the installed components if the JLV installation did not pass the Backout Verification Procedure outlined in Section 5.7, Backout Verification Procedure. The rollback procedure restores the previously-deployed version of JLV. The risks for executing the rollback are minimal as the procedure is performed during previously announced downtime, and users are not accessing the system. Therefore, users would not have accessed the new JLV version and/or changes to user configuration files would not have occurred. When the system is online and validated, user access would continue as before.

If the rollback is initiated later in the deployment window, restoration time may exceed the planned downtime for deployment. This risk is mitigated by scheduling deployments for weekends and other times when expected usage levels are low.

6.4 Authority for Rollback

If rollback is necessary, approval for the rollback will come from the current VA PM, Renae Facundus.

6.5 Rollback Procedure

Refer to Section 5.6, Backout Procedure.

6.6 Rollback Verification Procedure

Refer to Section 5.6, Backout Procedure.

A. Appendix A: Acronyms and Abbreviations

Table 10 lists the acronyms and abbreviations are used throughout this document.

Table 10: Acronyms and Abbreviations

Acronym	Definition
AITC	Austin Information Technology Center
ANR	Automated Notification Request
CM	Change Management
CPU	Central Processing Unit
DB	Database
DES	Data Exchange Service
DIBR	Deployment, Installation, Backout, and Rollback
DoD	Department of Defense
EHR	Electronic Health Record
EMR	Electronic Medical Record
EO	Enterprise Operations
EP	Elevated Privileges
EPMO	Enterprise Program Management Office
EST	Eastern Standard Time
GB	Gigabyte
GUI	Graphical User Interface
HRG	Hawaii Resources Group
IA	Integration Agreement
IM	Instant Message
IPT	Integrated Project Team
IT	Information Technology
JLV	Joint Legacy Viewer
MS	Microsoft
MVI	Master Veteran Index
OIT	Office of Information and Technology
PDWS	Patient Discovery Web Service
PITC	Philadelphia Information Technology Center
PM	Program Manager or Project Manager
POC	Point of Contact

Acronym	Definition
QoS	Quality of Service
RAM	Random Access Memory
SQL	Structured Query Language
TSPR	Technical Services Project Repository
VA	Department of Veterans Affairs
VDS	VistA Data Service
VIP	Veteran-Focused Integration Process
VistA	Veterans Health Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
VSA	VistA Services Assembler