Joint Legacy Viewer (JLV) 2.5.2 Deployment, Installation, Backout, and Rollback (DIBR) Guide

April 2017

Version 1.3

Department of Veterans Affairs (VA)

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
04/04/2017	1.3	Final comments addressed. Document approved.	AbleVets
03/30/2017	1.2	Resubmitted for final review with all client comments addressed	AbleVets
03/16/2017	1.1	Resubmitted with client comments addressed	AbleVets
02/20/2017	1.0	Draft submitted for review	AbleVets
01/15/2017	0.1	Initial draft of the artifact	AbleVets

Artifact Rationale

This document describes the deployment, installation, backout, and rollback (DIBR) 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 is updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

JLV is a centrally hosted, java-based web application that is managed as a single code baseline, and deployed in separate Department of Defense (DoD) and Department of Veteran Affairs (VA) environments. JLV is a browser-based, graphical user interface (GUI) that provides an integrated, read-only view of Electronic Health Record (EHR) data from the DoD, VA, and Virtual Lifetime Electronic Record (VLER) eHealth Exchange (eHX) partners, within a single application.

The JLV GUI retrieves and displays clinical data from a number of native data sources and systems. The data is then presented to the user in a simple to use, web-based interface, through widgets. Each widget corresponds to a clinical data domain. JLV eliminates the need for VA and DoD clinicians to access separate, disparate viewers. Born from a joint DoD-VA venture called JANUS, JLV was directed by the Secretary of Defense and Secretary of Veterans Affairs in early 2013 to further support interoperability between the two departments.

JLV users can create and personalize tabs, drag and drop widgets onto tabs, sort data within a widget's columns, set date filters, and expand a widget for a detailed view of patient information. Within each widget, a circular, blue icon indicates the data retrieved is from a VA source; a square orange icon indicates that the data retrieved is from a DoD source; and a hexagonal, purple icon indicates data that the data retrieved is from VA VLER partners.

1.1 Purpose

The Deployment, Installation, Backout, and Rollback (DIBR) Guide provides a single, common document that defines the ordered, technical steps required to install the JLV 2.5.2 product. 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).

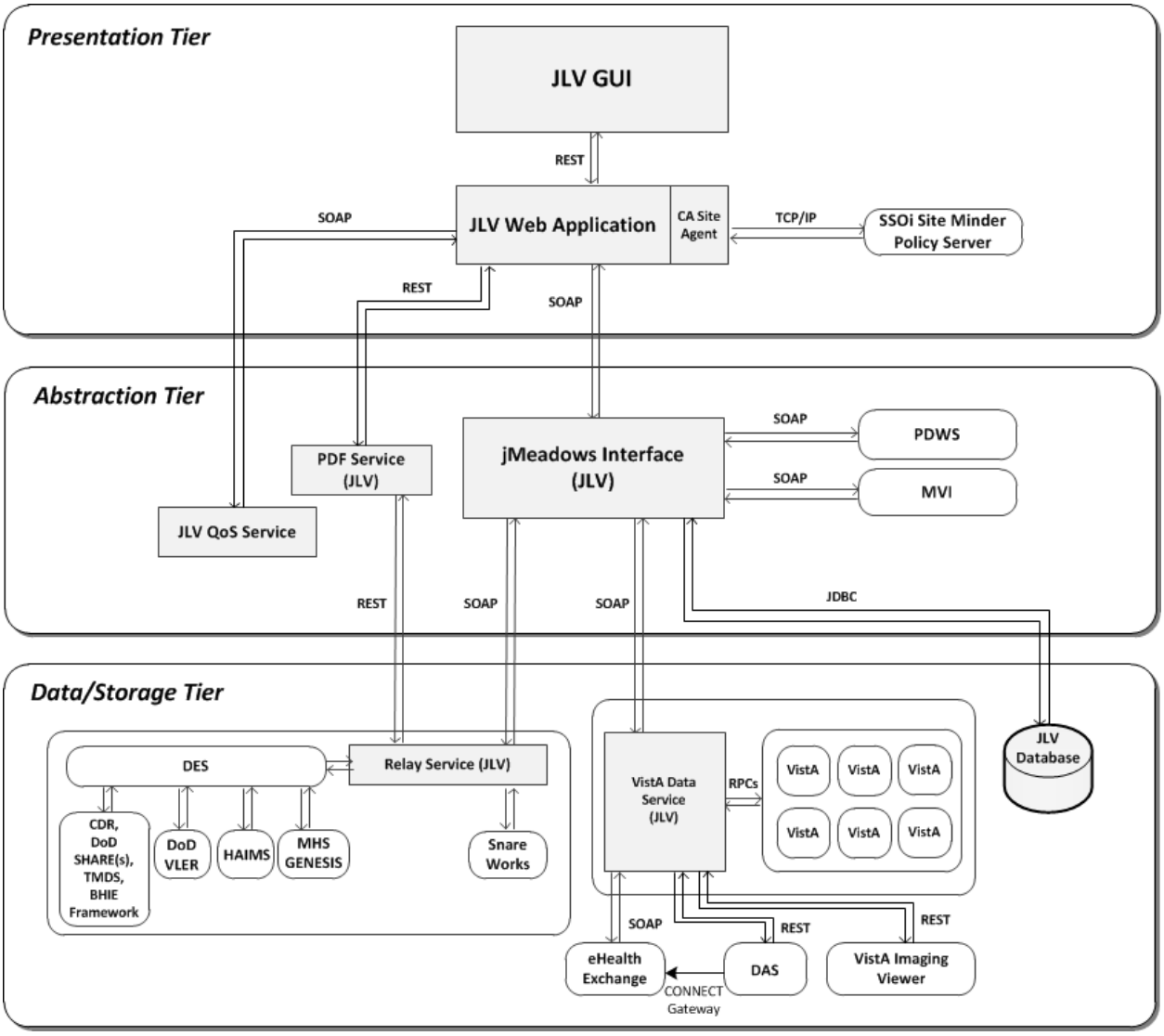
The JLV system specifications can be found in the *CLIN 0003AA JLV 2.5.2 System Design Document (SDD)*, in *Section 4, System Architecture*. All referenced documentation for JLV 2.5.2, once approved, is available on the Technical Services Project Repository (TSPR)[1].

JLV is read only interface to multiple VA data sources. Figure 1 illustrates the three tiers (presentation, abstraction, and data/storage) of the JLV architecture, the location of JLV system components within the tiers, and the external systems that JLV communicates with in enterprise environments. In the diagram, components of the JLV system (GUI, web application, Quality of Service (QoS) service, Print service, jMeadows interface, Relay service, Veterans Information System and Technology Architecture (VistA) Data service (VDS), Rich Text Format (RTF) Conversion service, and database are shaded. Communication protocols used between JLV components and external systems are labeled as Simple Object Access Protocol (SOAP) or

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

REpresentational State Transfer (REST). New communication protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), is used to/from Single Sign On Internal (SSOi).

Figure 1: JLV Architecture and Components



1.2 Dependencies

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 is not 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 is not functional.

1.3 Constraints

The physical environments held at AITC and PITC, which provide security and environmental control over the JLV servers, are 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 is met by the submission of the final Section 508 compliance test results. All referenced documentation for JLV 2.5.2, once approved, is available on the TSPR.

2 Roles and Responsibilities

Table 1 and Table 2 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

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

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

3 Deployment

The workflow surrounding a deployment of JLV is:

- Once EPMO approval is complete, the JLV Support team schedules the 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 makes a determination to proceed with a 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.

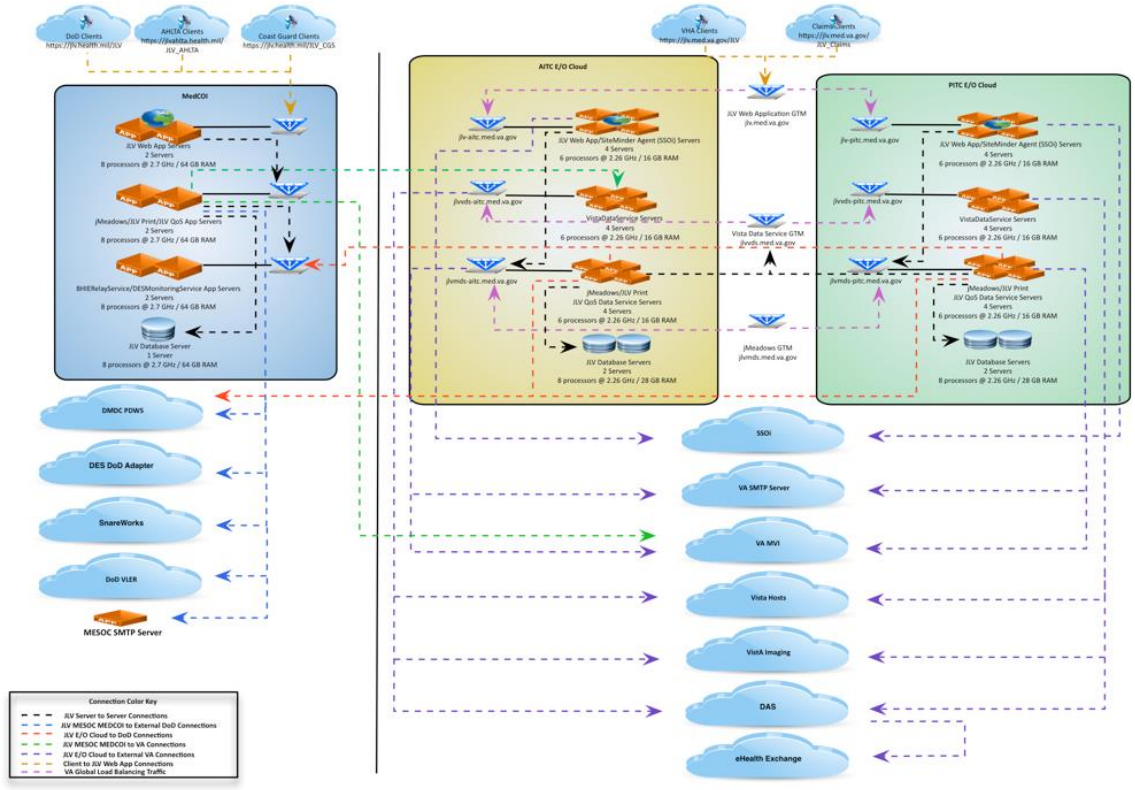
3.2 Site Readiness Assessment

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

3.2.1 Deployment Topology (Targeted Architecture)

Figure 2 below represents an overview of the JLV production infrastructure hosted at DoD Military Health System Enterprise Services Operations Center (MESOC), and VA AITC and PITC. The JLV system specifications can be found in the *CLIN 0003AA JLV 2.5.2 SDD*, in *Section 4, System Architecture*. All referenced documentation for JLV 2.5.2, once approved, is available on the TSPR.

Figure 2: JLV Production Infrastructure in the DoD and VA Environments



3.2.2 Site Information (Locations, Deployment Recipients)

The host sites for JLV are 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 regular, monthly patching schedule, determined by Information Technology Operations (ITOPS).

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 in the EO cloud environment at both the 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: Virtual Machine Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Windows Server	Windows Server 2008 R2 Enterprise (64-bit)	N/A	6 Processors, 16 GB RAM	Dell	12 Servers for AITC 12 servers for PITC
Database (DB) Server	Windows Server 2008 R2 Enterprise (64-bit) Microsoft SQL Server 2008 R2	N/A	8 processors, 28 GB RAM	Dell	2 Servers for AITC 2 Servers for PITC
	Windows Serer 2012 R2 Enterprise (64-bit) Microsoft SQL Server 2012	N/A	8 processors, 28 GB RAM	Dell	1 Server for AITC 1 Server 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	Manufacturer	Other
Microsoft SQL Server 2012	N/A	2012	MS	N/A
Windows Server 2008 R2	N/A	2008 R2	MS	N/A
Windows Server 2012 R2	N/A	2012 R2	MS	N/A
Oracle WebLogic Server Version 10.3.6.	N/A	10.3.6	Oracle	N/A

3.3.4 Communications

Members of the JLV Support team perform installation and deployment activities in the EO Cloud environment, and communicate with the VA Network team, as needed. Where possible, installation is performed during weekends and/or off-hours, to minimize the impact on users.

An overview of typical steps and/or communication during the implementation process is as follows:

1. Submit JLV release notification.
2. Plan system downtime and change notifications:
    a. Veterans Health Administration (VHA) team updates JLV newsfeed on appropriate forums.
    b. JLV PM and Office of Information and Technology (OIT) PM are notified.
3. Backup systems and/or current deployment (to be performed for future releases).
4. Perform installation/deployment:
    a. Current installation removed from service (to be performed for future releases).
5. Validate installation:
    a. Verify EO Cloud installation.
6. Notification that systems are online:
    a. Notify Product team and users.

3.3.4.1 Deployment/Installation/Backout Checklist

Table 6: Deployment, Installation, and Backout Checklist

Activity	Day	Time	Individual Who Completes Task
Deployment	Saturday	Deployment dependent on planned maintenance ANR.	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 Change Management (CM) Plan* for information about the installation and deployment of the JLV system. All referenced documentation for JLV 2.5.2, once approved, is available on the TSPR.

Table 7: Implementation Plan Summary

Considerations	Associated Details
Affected Systems	JLV
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 software installation files are located in the D:\builds directory. 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. Refer to Section 4.8, Installation Procedures.

4.4 Database Creation

The JLV database is created with a restore database schema. The database is a SQL Server 2012 database, used to store user profile information, audit records, and medical standard translation/mapping reference tables.

Refer to the *CLIN 1003AA JLV 2.5.2 SDD* for the database design overview, and details regarding the database tables. All referenced documentation for JLV 2.5.2, once approved, is available on the TSPR.

4.5 Installation Scripts

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 are run.

4.7 Access Requirements and Skills Needed for Installation

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

4.8 Installation Procedures

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

1. Update JLV databases in AITC-Enterprise Operations (EO) Cloud Environment (15-minute time estimate). Manual validation occurs once the following occurs.
    b. Remote desktop into VAAUSSQLJLV405 server.
    c. Open Microsoft SQL Server Management Studio (SSMS)
    d. In SSMS, connect to 'localhost'
    e. Open SQL Script "JLV_2.5.2_updates.sql".
    f. Execute the SQL Script "JLV_2.5.2_update.sql" (provided with the JLV 2.5.2 source code package submission).
2. Update JLV databases in PITC-EO Cloud Environment (15-minute time estimate).
    a. Remote desktop into VAPHISQLJLV405 server.
    b. Open Microsoft SQL Server Management Studio (SSMS)
    c. In SSMS, connect to 'localhost'
    d. Open SQL Script "JLV_2.5.2_updates.sql".
    e. Execute the SQL Script "JLV_2.5.2_update.sql" (provided with the JLV 2.5.2 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, view build file; compare text files to 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:

- VISTA_Universal Resource Locator (URL) = https://jlvvds-aitc.med.va.gov/VistaDataService/VistaDataService?wsdl
- BHIE_RELAY_SERVICE_URL = http://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
- PDWS_PS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?wsdl
- PDWS_PR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientRetrieve?wsdl
- PDWS_FS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilySearch?wsdl
- PDWS_FR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilyRetrieve?wsdl
- PDWS_PROC_CODE = P
- PDWS_SND_DEV_ID = 177610
- MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
- JNDI_JDBC = jdbc/JanusSQL
- JNDI_JDBC_ENCRYPTED = jdbc/JanusSQLTDE
- RPC_ENDPOINT_ENVIRONMENT = nc_gold
- RPC_ENDPOINT_ENVIRONMENT = enterprise
- CACHE_ENDPOINT_ENVIRONMENT = enterprise
- SHARE_ENDPOINT_ENVIRONMENT = enterprise
- MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
- AHLTA_ENDPOINT_ENVIRONMENT = enterprise
- USE_SNAREWORKS = true

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

i. Undeploy previously deployed jMeadows build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous jMeadows deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

j. Deploy the jMeadows-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.

- At the next page, type in path to location of war file ‘d:\builds’
- Click Radio next to jMeadows build to be deployed, click Next.
- Set application name to ‘jMeadows-[JLV version]’.
- Click Finish to complete installation to the jMeadows cluster.
- Once deployment completes, click Activate Changes.
- 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 JLV properties file 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, view build file; compare text files to 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.

- VISTA_URL = https://jlvvds-pitc.med.va.gov/VistaDataService/VistaDataService?wsdl
- BHIE_RELAY_SERVICE_URL = http://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
- PDWS_PS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?wsdl
- PDWS_PR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientRetrieve?wsdl
- PDWS_FS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilySearch?wsdl
- PDWS_FR_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientFamilyRetrieve?wsdl

- PDWS_PROC_CODE = P
- PDWS_SND_DEV_ID = 177610
- MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
- JNDI_JDBC = jdbc/JanusSQL
- JNDI_JDBC_ENCRYPTED = jdbc/JanusSQLTDE
- RPC_ENDPOINT_ENVIRONMENT = nc_gold
- RPC_ENDPOINT_ENVIRONMENT = enterprise
- CACHE_ENDPOINT_ENVIRONMENT = enterprise
- SHARE_ENDPOINT_ENVIRONMENT = enterprise
- MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
- AHLTA_ENDPOINT_ENVIRONMENT = enterprise
- USE_SNAREWORKS = true

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

i. Undeploy previously deployed jMeadows build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous jMeadows deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

j. Deploy the jMeadows-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’
- Click Radio next to jMeadows build to be deployed, click Next.
- Set application name to ‘jMeadows-[JLV version]’.
- Click Finish to complete installation to the jMeadows cluster.
- Once deployment completes, click Activate Changes.
- 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 a telnet utility.

      - 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.

      - grails.jmeadowsURL = https://jlvmds-aitc.med.va.gov/jMeadows/JMeadowsDataService
      - grails.dodVlerURL = https://sa-dtc.med.osd.mil/
      - grails.jlvqosURL = https://vaausjlvweb209.aac.dva.va.gov/JLVQoS/JLVQoSDataService?wsdl
      - 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 build through the WebLogic Admin Console.

      - Click Deployments link.
      - Click Lock & Edit.
      - Click Checkbox next to previous JLV deployment.
      - Click Delete.
      - Click OK to confirm removal.
      - Once removal is complete, click Activate Changes.

   h. Deploy the JLV-[JLV version]-production.war build through the WebLogic Admin Console.

      - War files are staged in the D:\builds\ directory
      - Click Deployments link.
      - Click Lock & Edit.
      - Click Install.
      - At the next page, type in path to location of war file ‘d:\builds’.

- Click Radio next to JLV build to be deployed, click Next.
- Set application name to 'JLV_[JLV version]'.
- Click Finish to complete installation to the JLV cluster.
- Once deployment completes, click Activate Changes.
- 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.

      - 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.

      - grails.jmeadowsURL = https://jlvmds-aitc.med.va.gov/jMeadows/JMeadowsDataService
      - grails.dodVlerURL = https://sa-dtc.med.osd.mil/
      - grails.jlvqosURL = https://vaphijlvweb209.aac.dva.va.gov/JLVQoS/JLVQoSDataService?wsdl
      - 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 build through the WebLogic Admin Console.

      - Click Deployments link.
      - Click Lock & Edit.
      - Click Checkbox next to previous JLV deployment.
      - Click Delete.

- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

h. Deploy the JLV-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLV build to be deployed, click Next.
- Set application name to 'JLV_[JLV version]'.
- Click Finish to complete installation to the JLV cluster.
- Once deployment completes, click Activate Changes.
- 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 JLV_CLAIMS web application in AITC-EO Cloud environment (30-minute time estimate).

a. Remote desktop into *VAAUSJLVWEB201* server.

b. Upload the JLV_CLAIMS -[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.

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.

- grails.jmeadowsURL = https://jlvmds-aitc.med.va.gov/jMeadows/JMeadowsDataService
- grails.dodVlerURL = https://sa-dtc.med.osd.mil/
- grails.jlvqosURL = https://vaausjlvweb209.aac.dva.va.gov/JLVQoS/JLVQoSDataService?wsdl
- grails.jlvprintURL = https://vaausjlvweb209.aac.dva.va.gov/JLVPrintService/JLVPrintService?wsdl

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

g. Deploy the JLV_CLAIMS [JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLV_CLAIMS build to be deployed, click Next.
- Set application name to 'JLV_CLAIMS_[JLV version]'.
- Click Finish to complete installation to the JLV cluster.
- Once deployment completes, click Activate Changes.
- 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.

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

i. Start application.

j. Validate JLV_CLAIMS endpoint is available by testing network connectivity through telnet utility.

k. Validate JLV_CLAIMS web portal is available by testing connectivity through web browser outside of the JLV servers using the URL https://jlv.med.va.gov/JLV_CLAIMS.

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

a. Remote desktop into *VAPHIJLVWEB201* server.

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

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

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.

- grails.jmeadowsURL = https://jlvmds-pitc.med.va.gov/jMeadows/JMeadowsDataService
- grails.dodVlerURL = https://sa-dtc.med.osd.mil/
- grails.jlvqosURL = https://vaphijlvweb209.aac.dva.va.gov/JLVQoS/JLVQoSDataService?wsdl

- grails.jlvprintURL = https://vaphijlvweb209.aac.dva.va.gov/JLVPrintService/JLVPrintService?wsdl

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

g. Deploy the JLV_CLAIMS [JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLV_CLAIMS build to be deployed, click Next.
- Set application name to 'JLV_CLAIMS_[JLV version]'.
- Click Finish to complete installation to the JLV cluster.
- Once deployment completes, click Activate Changes.
- 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.

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

i. Start application.

j. Validate JLV_CLAIMS endpoint is available by testing network connectivity through telnet utility.

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

9. 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.

- appconfig.vler.dq.url = nhiapp-prd.va.gov http://nhiapp-prd.va.gov/NHINAdapterGatewayDocQuery/EntityDocQuery?wsdl

- appconfig.vler.dr.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayDocRetrieve/EntityDocRetrieve?wsdl
- appconfig.vler.pd.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayPatientDiscovery/EntityPatientDiscovery?wsdl
- 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 build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous VistaDataService deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

i. Deploy the VistaDataService-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to VistaDataService build to be deployed, click Next.
- Set application name to 'VistaDataService_[JLV version]'.
- Click Finish to complete installation to the VistaDataService cluster.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB205, VAAUSJLVWEB206, VAAUSJLVWEB207, VAAUSJLVWEB208) and stages it in the directory path ${VistaDataService_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. If VistA Data Service endpoint is not available, check and validate the deployment.

10. 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.

- appconfig.vler.dq.url = nhiapp-prd.va.gov http://nhiapp-prd.va.gov/NHINAdapterGatewayDocQuery/EntityDocQuery?wsdl
- appconfig.vler.dr.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayDocRetrieve/EntityDocRetrieve?wsdl
- appconfig.vler.pd.url = http://nhiapp-prd.va.gov/NHINAdapterGatewayPatientDiscovery/EntityPatientDiscovery?wsdl
- 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 build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous VistaDataService deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

i. Deploy the VistaDataService-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’.
- Click Radio next to VistaDataService build to be deployed, click Next.
- Set application name to ‘VistaDataService_[JLV version]’.
- Click Finish to complete installation to the VistaDataService cluster.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB205, VAPHIJLVWEB206, VAPHIJLVWEB207, VAPHIJLVWEB208) and stages it

in the directory path
${VistaDataService_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. If VistA Data Service endpoint is not available, check validate the deployment.

11. 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 through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLVPrintService deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

e. Deploy the JLVPrintService -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’.
- Click Radio next to JLVPrintService build to be deployed, click Next.
- Set application name to ‘JLVPrintService_[JLV version]’.
- Click Finish to complete installation to the JLVPrintService server.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the VAPHIJLVWEB210 server and stages it in the directory path
${ JLVPrintService_Server}\servers\${SERVER_NAME}\stage.

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

g. Start application.

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

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

12. Install 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:\builds\ directory on VAAUSJLVWEB205 server.

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

    d. Undeploy previously deployed JLVPrintService build through the WebLogic Admin Console.

    - Click Deployments link.
    - Click Lock & Edit.
    - Click Checkbox next to previous JLVPrintService deployment.
    - Click Delete.
    - Click OK to confirm removal.
    - Once removal is complete, click Activate Changes.

    e. Deploy the JLVPrintService -[JLV version]-production.war build through the WebLogic Admin Console.

    - War files are staged in the D:\builds\ directory
    - Click Deployments link.
    - Click Lock & Edit.
    - Click Install.
    - At the next page, type in path to location of war file ‘d:\builds’.
    - Click Radio next to JLVPrintService build to be deployed, click Next.
    - Set application name to ‘JLVPrintService_[JLV version]’.
    - Click Finish to complete installation to the JLVPrintService server.
    - Once deployment completes, click Activate Changes.
    - WebLogic distributes the .war file to the VAAUSJLVWEB210 server and stages it in the directory path
      ${ JLVPrintService_Server}\servers\${SERVER_NAME}\stage.

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

    g. Start application.

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

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

13. 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.

- ENV = AITC
- JMEADOWS_URL = https://jlvmds.med.va.gov/jMeadows/JMeadowsDataService?wsdl
- VISTA_URL = https://jlvvds-aitc.med.va.gov/VistaDataService/VistaDataService?wsdl
- BHIE_RELAY_SERVICE_URL = https://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
- PDWS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?WSDL
- MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
- JNDI_JDBC = jdbc/JanusSQL_24
- RPC_ENDPOINT_ENVIRONMENT = enterprise
- CACHE_ENDPOINT_ENVIRONMENT = enterprise
- SHARE_ENDPOINT_ENVIRONMENT = enterprise
- MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
- AHLTA_ENDPOINT_ENVIRONMENT = enterprise
- SERVICE_MONITOR_TEST_BRS = TRUE
- SERVICE_MONITOR_TEST_JMDS = TRUE
- SERVICE_MONITOR_TEST_MVI = TRUE
- SERVICE_MONITOR_TEST_PDWS = TRUE
- SERVICE_MONITOR_TEST_VDS = TRUE
- SERVICE_MONITOR_TEST_SHARE = FALSE
- SERVICE_MONITOR_TEST_SNAREWORKS = TRUE
- SERVICE_MONITOR_TEST_VISTA_SITES = FALSE
- EMAIL_HOST = smtp.va.gov
- EMAIL_SSL_PORT = 465
- EMAIL_FROM = jlv@hawaiirg.com
- EMAIL_TO = JLVQoS@HawaiiRG.com
- EMAIL_SRC_SYS = AITC

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

e. Undeploy previously deployed JLVQoS build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLVQoS deployment.
- Click Delete.
- Click OK to confirm removal.

- Once removal is complete, click Activate Changes.

f. Deploy the JLVQoS -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLVQoS build to be deployed, click Next.
- Set application name to 'JLVQoS_[JLV version]'.
- Click Finish to complete installation to the JLVQoS server.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the VAAUSJLVWEB209 server and stages it in the directory path ${ JLVQoS_Server}\servers\${SERVER_NAME}\stage.

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

h. Start application through WebLogic.

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.

14. 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.

- ENV = PITC
- JMEADOWS_URL = https://jlvmds-pitc.med.va.gov/jMeadows/JMeadowsDataService?wsdl
- VISTA_URL = https://jlvvds-pitc.med.va.gov/VistaDataService/VistaDataService?wsdl
- BHIE_RELAY_SERVICE_URL = https://janusjlvds-mesa.health.mil/BHIERelayService/BHIERelayService?wsdl
- PDWS_URL = https://pkidws.dmdc.osd.mil/pdws/EntityPatientSearch?WSDL
- MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService
- JNDI_JDBC = jdbc/JanusSQL_24
- RPC_ENDPOINT_ENVIRONMENT = enterprise

- CACHE_ENDPOINT_ENVIRONMENT = enterprise
- SHARE_ENDPOINT_ENVIRONMENT = enterprise
- MEDWEB_ENDPOINT_ENVIRONMENT = enterprise
- AHLTA_ENDPOINT_ENVIRONMENT = enterprise
- SERVICE_MONITOR_TEST_BRS = TRUE
- SERVICE_MONITOR_TEST_JMDS = TRUE
- SERVICE_MONITOR_TEST_MVI = TRUE
- SERVICE_MONITOR_TEST_PDWS = TRUE
- SERVICE_MONITOR_TEST_VDS = TRUE
- SERVICE_MONITOR_TEST_SHARE = FALSE
- SERVICE_MONITOR_TEST_SNAREWORKS = TRUE
- SERVICE_MONITOR_TEST_VISTA_SITES = FALSE
- EMAIL_HOST = smtp.va.gov
- EMAIL_SSL_PORT = 465
- EMAIL_FROM = jlv@hawaiirg.com
- EMAIL_TO = JLVQoS@HawaiiRG.com
- EMAIL_SRC_SYS = PITC

e. Undeploy previously deployed JLVQoS build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLVQoS deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

f. Deploy the JLVQoS -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’.
- Click Radio next to JLVQoS build to be deployed, click Next.
- Set application name to ‘JLVQoS_[JLV version]’.
- Click Finish to complete installation to the JLVQoS server.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the VAPHIJLVWEB209 server and stages it in the directory path ${ JLVQoS_Server}\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 Procedures

After completing the process detailed in Section 4.8, Installation Procedures, perform a manual smoke test through each module as an end user using the following steps 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. Log in as VBA user to JLV_CLAIMS application.
3. Validate Patient Search Patient Discovery Web Service (PDWS).
4. Validate VA Master Veteran Index (MVI).
5. Validate the VistA Data Service by ensuring VA data is being returned.
6. Validate that the jMeadows interface with the Relay Service is functional by ensuring DoD data is being returned.
7. Validate that VA Terminology mapping is occurring.
8. Validate that DoD Terminology mapping is occurring.
9. Validate the Health Monitor (QoS).
10. Validate the JLV Print Service.
11. Validate the RTF Conversion 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 VM Server Configuration

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

4.11 Database Tuning

Database tuning is dependent upon the specific software releases. If applicable, instructions are provided in the release notes.

5 Backout Procedures

5.1 Backout Strategy

The backout strategy is to uninstall the currently deployed JLV system components, and restore the previously-deployed version of JLV.

5.2 Backout Considerations

The criteria for backing out of the current installation is that JLV, as tested by VA and partner testers and the JLV Support team, does not operate as intended.

5.2.1 Load Testing

Load testing is currently being coordinated.

5.2.2 User Acceptance Testing (UAT)

The UAT results are not available at the time of this writing. The data will be available in all JLV 2.5.2 testing documentation submitted after testing is complete.

If the UAT fails, a request is made to the VA PM for approval to back out.

5.3 Backout Criteria

The criteria for backing out of the current installation is that JLV, as tested by VA and partner testers and the JLV Support team, 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 procedures. The backout procedures restore the previously-deployed version of JLV. The risks for executing the backout are minimal, as a backout is performed during a previously announced downtime, and users are not accessing the system. Therefore, users would not have accessed the new JLV version, and 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 comes from the current VA PM, Renae Facundus.

5.6 Backout Procedures

The following steps detail the procedures for uninstalling JLV components in the AITC and PITC environments.

1. Uninstall jMeadows in AITC - EO Cloud environment.
   a. Remote desktop into *VAAUSJLVWEB209* server.
   b. Log into WebLogic Server Administration Console on *VAAUSJLVWEB209* server.
   c. Undeploy the new version of the jMeadows build through the WebLogic Admin Console.
      - Click Deployments link.
      - Click Lock & Edit.
      - Click Checkbox next to previous jMeadows deployment.
      - Click Delete.
      - Click OK to confirm removal.
      - Once removal is complete, click Activate Changes.
   d. Deploy the previous version of jMeadows, jMeadows-[JLV version]-production.war build through the WebLogic Admin Console.
      - War files are staged in the D:\builds\ directory.
      - Click Deployments link.
      - Click Lock & Edit.
      - Click Install.
      - At the next page, type in path to location of war file 'd:\builds'.
      - Click Radio next to jMeadows build to be deployed, click Next.
      - Set application name to 'jMeadows-[JLV version]'.
      - Click Finish to complete installation to the jMeadows cluster.
      - Once deployment completes, click Activate Changes.
      - 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.
   e. Start the pertinent JLV Servers/Services.
   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 jMeadows in PITC - EO Cloud environment.
   a. Remote desktop into *VAPHIJLVWEB209* server.
   b. Log into WebLogic Server Administration Console on *VAPHIJLVWEB209* server.
   c. Undeploy new version of the jMeadows build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous jMeadows deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

d. Deploy the previous version, jMeadows -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to jMeadows build to be deployed, click Next.
- Set application name to 'jMeadows_-[JLV version]'.
- Click Finish to complete installation to the jMeadows cluster.
- Once deployment completes, click Activate Changes.
- 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.

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.

3. 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. Undeploy the new version of the JLV build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLV deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

d. Deploy the previous version of JLV, JLV-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.

- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’.
- Click Radio next to JLV build to be deployed, click Next.
- Set application name to ‘JLV-[JLV version]’.
- Click Finish to complete installation to the JLV cluster.
- Once deployment completes, click Activate Changes.
- 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.

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 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. Undeploy the new version of the JLV build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLV deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

d. Deploy the previous version of JLV, JLV-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’.
- Click Radio next to JLV build to be deployed, click Next.
- Set application name to ‘JLV -[JLV version]’.
- Click Finish to complete installation to the JLV cluster.
- Once deployment completes, click Activate Changes.
- 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.

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.

5. Uninstall JLV_Claims web application in AITC-EO Cloud environment.

   a. Remote desktop into *VAAUSJLVWEB201* server.

   b. Log into WebLogic Server Administration Console on *VAAUSJLVWEB201*server.

   c. Undeploy the new version of the JLV_CLAIMS build through the WebLogic Admin Console.

      - Click Deployments link.
      - Click Lock & Edit.
      - Click Checkbox next to previous JLV deployment.
      - Click Delete.
      - Click OK to confirm removal.
      - Once removal is complete, click Activate Changes.

6. Uninstall JLV_Claims web application in PITC-EO Cloud environment.

   a. Remote desktop into *VAPHIJLVWEB201* server.

   b. Log into WebLogic Server Administration Console on *VAPHIJLVWEB201*server.

   c. Undeploy the new version of the JLV_CLAIMS build through the WebLogic Admin Console.

      - Click Deployments link.
      - Click Lock & Edit.
      - Click Checkbox next to previous JLV deployment.
      - Click Delete.
      - Click OK to confirm removal.
      - Once removal is complete, click Activate Changes.

7. 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. Undeploy the new version of the VistaDataService build through the WebLogic Admin Console.

      - Click Deployments link.
      - Click Lock & Edit.
      - Click Checkbox next to previous VistaDataService deployment.
      - Click Delete.
      - Click OK to confirm removal.
      - Once removal is complete, click Activate Changes.

d. Deploy the previous version of VistaDataService, VistaDataService -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to VistaDataService build to be deployed, click Next.
- Set application name to 'VistaDataService_-[JLV version]'.
- Click Finish to complete installation to the VistaDataService cluster.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the clustered servers (VAAUSJLVWEB205, VAAUSJLVWEB206, VAAUSJLVWEB207, VAAUSJLVWEB208) and stages it in the directory path ${VistaDataService_DOMAIN}\servers\${SERVER_NAME}\stage.

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.

8. Uninstall VDS in PITC-EO Cloud environment.

a. Remote desktop into *VAPHIJLVWEB205* server.

b. Log into WebLogic Server Administration Console on *VAPHIJLVWEB205* server.

c. Undeploy the new version of the VistaDataService build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous VistaDataService deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

d. Deploy the previous version of VistaDataService, VistaDataService-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to VistaDataService build to be deployed, click Next.
- Set application name to 'VistaDataService_[JLV version]'.

- Click Finish to complete installation to the VistaDataService cluster.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the clustered servers (VAPHIJLVWEB205, VAPHIJLVWEB206, VAPHIJLVWEB207, VAPHIJLVWEB208) and stages it in the directory path ${VistaDataService_DOMAIN}\servers\${SERVER_NAME}\stage.

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.

9. Recreate JLV database in AITC-EO Cloud environment (15-minute time estimate).
   a. Remote desktop into VAAUSSQLJLV405.
   b. Open Microsoft SQL Server Management Studio (SSMS)
   c. In SSMS, connect to 'localhost'
   d. Recreate the tables of the previous version of the JLV database using the JLV.mdf and JLV_log.ldf files through restoral of database backups.
10. Recreate JLV database in PITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into VAPHISQLJLV405.
    b. Open Microsoft SQL Server Management Studio (SSMS)
    c. In SSMS, connect to 'localhost'
    d. Recreate the tables of the previous version of the JLV database using the JLV.mdf and JLV_log.ldf files through restoral of database backups.
11. 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. Log in to the WebLogic Server Administration Console on *VAAUSJLVWEB209* server.
    e. Undeploy new version of the JLVPrintService build through the WebLogic Admin Console.
       - Click Deployments.
       - Click Lock & Edit.
       - Click Checkbox next to previous JLVPrintService deployment.
       - Click Delete.

- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

f. Deploy the previous version of JLVPrintService, JLVPrintService -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLVPrintService build to be deployed, click Next.
- Set application name to 'JLVPrintService_[JLV version]'.
- Click Finish to complete installation to the JLVPrintService server.
- Once deployment completes, click Activate Changes.

g. WebLogic distributes the .war file to the VAAUSJLVWEB210 server and stages it in the directory path ${ JLVPrintService_Server}\servers\${SERVER_NAME}\stage.

h. Start application.

12. 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 new version of the JLVPrintService build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLVPrintService deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

e. Deploy the previous version of JLVPrintService, JLVPrintService -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLVPrintService build to be deployed, click Next.
- Set application name to 'JLVPrintService_[JLV version]'.
- Click Finish to complete installation to the JLVPrintService server.

- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the VAPHIJLVWEB210 server and stages it in the directory path ${ JLVPrintService_Server}\servers\${SERVER_NAME}\stage.

f. Start application.

13. 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 the new version of the JLVQoS build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLVQoS deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

e. Deploy the previous version of JLVQoS, JLVQoS -[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file ‘d:\builds’.
- Click Radio next to JLVQoS build to be deployed, click Next.
- Set application name to ‘JLVQoS_[JLV version]’.
- Click Finish to complete installation to the JLVQoS server.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the VAAUSJLVWEB209 server and stages it in the directory path ${ JLVQoS_Server}\servers\${SERVER_NAME}\stage.

f. Start application.

14. 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 the new version of the JLVQoS build through the WebLogic Admin Console.

- Click Deployments link.
- Click Lock & Edit.
- Click Checkbox next to previous JLVQoS deployment.
- Click Delete.
- Click OK to confirm removal.
- Once removal is complete, click Activate Changes.

e. Deploy the previous version of JLVQoS, JLVQoS-[JLV version]-production.war build through the WebLogic Admin Console.

- War files are staged in the D:\builds\ directory.
- Click Deployments link.
- Click Lock & Edit.
- Click Install.
- At the next page, type in path to location of war file 'd:\builds'.
- Click Radio next to JLVQoS build to be deployed, click Next.
- Set application name to 'JLVQoS_[JLV version]'.
- Click Finish to complete installation to the JLVQoS server.
- Once deployment completes, click Activate Changes.
- WebLogic distributes the .war file to the VAPHIJLVWEB209 server and stages it in the directory path ${ JLVQoS_Server}\servers\${SERVER_NAME}\stage.

f. Start application.

5.7 Backout Verification Procedures

Validate the backout procedures by completing the steps below.

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

1. Log in as VA user to JLV application.
   a. Expected Result: Successful login
2. Validate VA Master Veteran Index (MVI).
   a. Expected Result: Successful patient search, and patient correlation.
3. Validate Patient Search Patient Discovery Web Service (PDWS).
   a. Expected Result: Successfully able to view DoD patient demographics.
4. Validate the VistA Data Service.
   a. Expected Result: VA data is being returned.
5. Validate that the jMeadows interface with the Relay Service is functional.
   a. Expected Result: DoD data is being returned.

6. Validate that VA Terminology mapping is occurring.
    a. Expected Result: VA terminology is properly being mapped in JLV widgets.
7. Validate that DoD Terminology mapping is occurring.
    a. Expected Result: DoD terminology is properly being mapped in JLV widgets.
8. Validate the Health Monitor (QoS).
    a. Expected Result: QoS Service is sending email alerts, System status is displaying.
9. Validate the JLV Print Service.
    a. Expected Result: User is able to add items to report builder and generate a printable PDF file.
10. Validate the RTF Conversion Service.
    a. Expected Result: DoD notes are being displayed in PDF format (when source data is RTF)

6 Rollback Procedures

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 procedures. The rollback procedures restore 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 a rollback is necessary, approval for the rollback comes from the current VA PM, Renae Facundus.

6.5 Rollback Procedures

Refer to Section 5.6, Backout Procedures.

6.6 Rollback Verification Procedures

Refer to Section 5.7, Backout Verification Procedures.

A. Appendix A: Acronyms and Abbreviations

Table 9 lists the acronyms and abbreviations are used throughout this document.

Table 9: Acronyms and Abbreviations

Acronym	Definition
AITC	Austin Information Technology Center
ANR	Automated Notification Request
CD	Critical Decision
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
IP	Internet Protocol
IT	Information Technology
JLV	Joint Legacy Viewer
MESOC	Military Health System Enterprise Services Operations Center
MVI	Master Veteran Index
OI&T	Office of Information and Technology
PDWS	Patient Discovery Web Service
PITC	Philadelphia Information Technology Center
PMP	Program Manager or Project Manager
POC	Point of Contact
POM	Production Operations Manual
QoS	Quality of Service
RAM	Random Access Memory

Acronym	Definition
REST	REpresentational State Transfer
RTF	Rich Text Format
SOAP	Simple Object Access Protocol
SDD	System Design Document
SSMS	SQL Server Management Studio
SSOi	Single Sign On Internal
SQL	Structured Query Language
TCP	Transmission Control Protocol
TSPR	Technical Services Project Repository
URL	Universal Resource Locator
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