Joint Longitudinal Viewer (JLV) 3.0

Deployment, Installation, Backout, and Rollback Guide (DIBRG)

March 2022

Version 2.0

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
02/28/2022	2.0	Draft for approval	Liberty ITS
02/09/2022	1.1	Updated from last approved to include hot patch updates	Liberty ITS
01/18/2022	1.0	Final Version after adjudication meeting	Liberty ITS
12/28/2021	0.1	Initial creation of document from last approved	Liberty ITS

Artifact Rationale

This document serves as the Deployment, Installation, Backout, and Rollback Guide (DIBRG) for Joint Longitudinal Viewer (JLV) releases going into the Department of Veterans Affairs (VA) Enterprise. The Guide includes information about system support, issue tracking, and escalation processes, and it identifies the 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 this artifact should be structured appropriately to reflect the particulars of these procedures at a single or at multiple locations.

The Deployment, Installation, Backout, and Rollback Guide is required to be completed with the expectation that it is updated throughout the life cycle of the project for each build as needed.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

Born from a joint Department of Defense (DOD)–Department of Veterans Affairs (VA) venture called JANUS, Joint Longitudinal Viewer was directed by the Secretary of the VA and the Secretary of Defense in early 2013 to further support interoperability between the two departments. JLV is a centrally hosted, Java-based web application managed as two similar but distinct products - one tailored for DOD use and another tailored for VA use. Each JLV product is deployed to its respective DOD and VA hosting environments. Although separately hosted, the respective applications use several shared data services. The browser-based, Graphical User Interface (GUI) provides an integrated, read-only view of Electronic Health Record (EHR) data from VA, DOD, and community partners within a single application.

JLV eliminates the need for VA and DOD clinicians to access disparate viewers. The GUI retrieves clinical data from several native data sources and systems, then presents it to the user via widgets, each corresponding to a clinical data domain.

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 blue circle indicates VA data; an orange square indicates DOD data; a purple hexagon indicates community partner data; and a green triangle indicates Cerner Millennium Federal Electronic Health Record (FEHR) data.

1.1. Purpose

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

System design specifications and diagrams can be found in the REDACTED.

Figure 1 illustrates the three tiers (presentation, abstraction, and data/storage) of the JLV architecture, the location of JLV system components within the tiers, the external systems that JLV communicates with in Enterprise environments, and the communication protocols and authentication methods used. In the diagram, components of JLV are shaded blue; external systems are shaded grey.

Figure 1: JLV Architecture and Components[1]
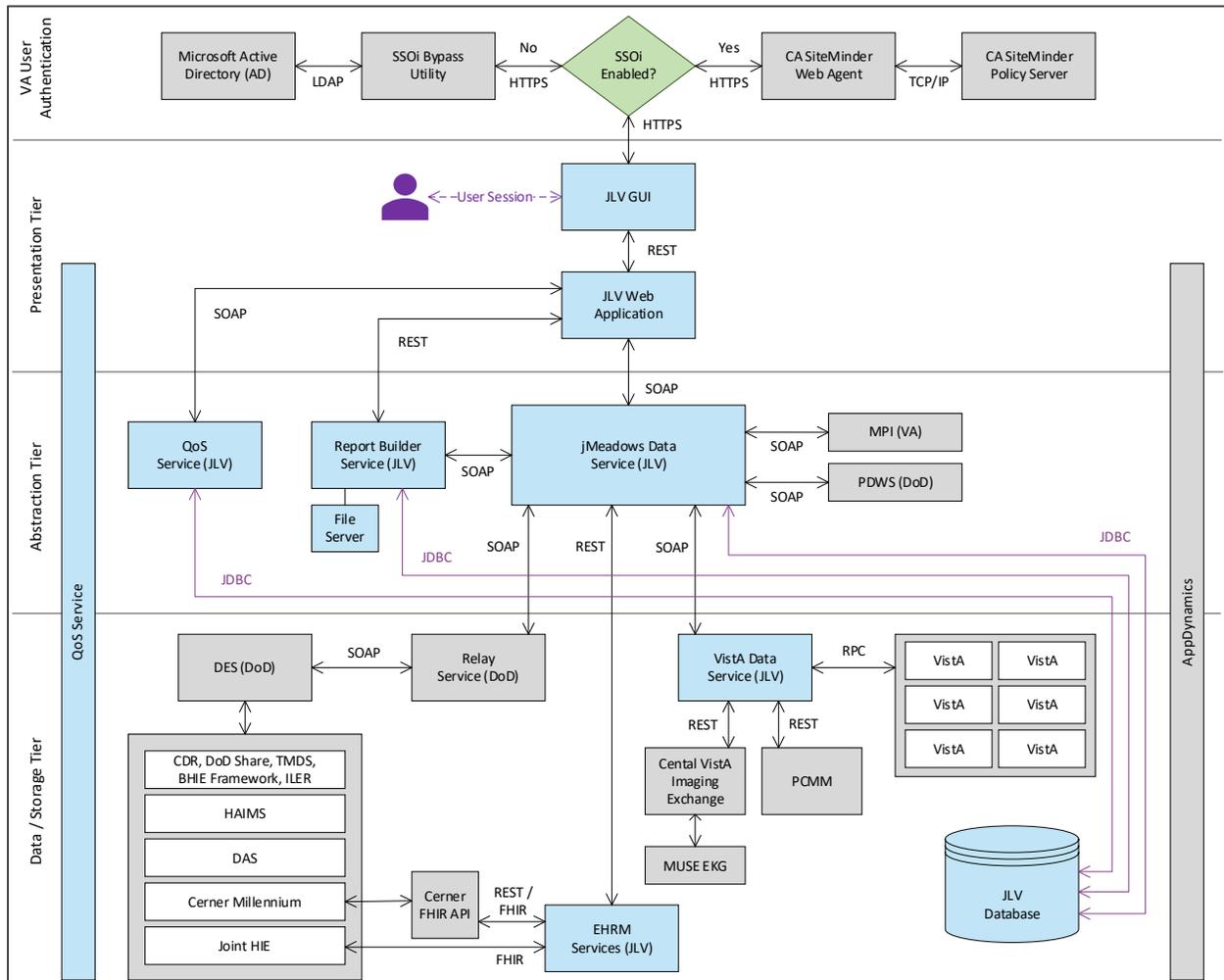
1.2. Dependencies

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 into JLV.

JLV is also dependent on internal VA update requirements, including DB flips, server updates, and security patches. If any of the VA Enterprise operational procedures disrupt the normal operation of JLV, the application is not fully functional.

---

[1] Active Directory (AD), Application Program Interface (API), Bidirectional Health Information Exchange (BHIE), Central VistA Imaging Exchange (CVIX), Clinical Data Repository (CDR), Computer Associates (CA), Data Access Service (DAS), Data Exchange Service (DES), , Electronic Health Record Modernization (EHRM), Fast Healthcare Interoperability Resources (FHIR), Healthcare Artifact and Image Management Solution (HAIMS), Health Information Exchange (HIE) HyperText Transfer Protocol Secure (HTTPS), Internet Protocol (IP), Java Database (DB) Connectivity (JDBC), Lightweight Directory Access Protocol (LDAP), Master Person Index (MPI), Military Health System (MHS), Patient Discovery Web Service (PDWS), Quality of Service (QoS), Remote Procedure Calls (RPCs), REpresentational State Transfer (REST), Single Sign On Internal (SSOi), Simple Object Access Protocol (SOAP), Theater Medical Data Store (TMDS), Transmission Control Protocol (TCP), Veterans Health Information Systems and Technology Architecture (VistA) Data Service (VDS)

The physical environments held at AITC and PITC provide security and environmental control over the JLV servers and are restricted by Elevated Privilege (EP) access. Project personnel request EP access by submitting the *JLV Linux (Centrify) and Windows Access Requirements* spreadsheet to the VA Project Manager (PM) / Contracting Officer's Representative (COR) for approval via the Electronic Permission Access System (ePAS). Any delay in granting initial EP access hinders the ability to respond to technical impacts to the servers.

1.3. Constraints

Not applicable to JLV.

2. Roles and Responsibilities

Table 1 and Table 2 list the project and DIBRG roles and responsibilities.

Table 1: Project Roles

Name	Title/Group	Company
REDACTED	JLV Program Manager	VA
REDACTED	JLV Project Manager	VA
REDACTED	OIT Software Test Lead	VA
REDACTED	Contract Program Manager	Liberty ITS
REDACTED	Contract Project Manager	Liberty ITS
REDACTED	Contract Project Manager	Liberty ITS
REDACTED	Contract Project Manager	Liberty ITS
REDACTED	JLV Operations Lead	Liberty ITS
REDACTED	JLV DevOps	Liberty ITS
REDACTED	JLV DevOps Lead	Liberty ITS
REDACTED	JLV Java Developer	Liberty ITS
REDACTED	JLV Java Developer	Liberty ITS
REDACTED	JLV Java Developer	Liberty ITS
REDACTED	Test Lead	Liberty ITS
REDACTED	Tester	Liberty ITS
REDACTED	Tester	Liberty ITS
REDACTED	Tester	Liberty ITS
REDACTED	JLV Incident Triage	Liberty ITS
REDACTED	JLV Incident Triage	Liberty ITS
REDACTED	IT Operations and Services (ITOPS), Infrastructure Operations (IO)	Seawolf

Please note that references to JLV Support in the table below indicate Liberty Team Operations and Engineers. See Table 6 for additional details regarding the Phase/Role column of Table 2.

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

Team	Phase/Role	Tasks
Enterprise Project Management Office (EPMO)	Approval for Release to Production	Review the Release Readiness Report (RRR) with JLV PM and Health Product Support (HPS) for approval; review and approve the Service Now (SNOW) Change Control Board (CCB) entry.
JLV Support	Deployment Coordination	• Plan and schedule deployments (including orchestration with vendors) • Determine and document the roles and responsibilities of those involved in deployments • Test for operational readiness
JLV Support	Installation	• Schedule installations with ITOPS IO • Ensure that the Authority to Operate (ATO) and certificate authority security documentation is in place • Validate through facility Points of Contact (POCs) to ensure that Information Technology (IT) equipment has been accepted using the asset inventory processes • Coordinate training
JLV Support	Backout	• Confirm the availability of backout instructions and backout strategy • Identify the criteria that triggers a backout
JLV Support	Rollback	• Confirm the availability of rollback instructions and rollback strategy • Identify the criteria that triggers a rollback
JLV Support	Post-Deployment	Provide hardware, software, and system support

3.   Deployment

The JLV deployment workflow is as follows.

1. Once EPMO approval is complete, the JLV Support team schedules the deployment in coordination with ITOPS IO
2. JLV Support completes a SNOW Change Order (CHG) prior to the known effective downtime
3. Once the deployment is complete in each of the Production environments, Production testing is verified by the JLV Support team; please see Access Requirements and Skills Needed for Installation for additional information
4. If there is an issue with the deployment in any Production environment, the JLV Support team and project management may decide to proceed with a backout; refer to Backout Strategy for more information

3.1.   Timeline

The deployment and installation have a duration of 8 hours per environment, simultaneously.

3.2.   Site Readiness Assessment

JLV is a Production, Enterprise-wide application hosted at PITC and AITC. All site readiness assessments are completed by ITOPS IO.

3.2.1.   Deployment Topology (Targeted Architecture)

JLV has environments at the PITC and AITC data centers. The primary operating environment is at PITC, with AITC serving as the failover site. Server details are documented in Table 4.

3.2.2.   Site Information (Locations, Deployment Recipients)

The host sites for JLV are the VA PITC and AITC data centers.

3.2.3.   Site Preparation

JLV is a Production, Enterprise-wide application hosted at PITC and AITC. All site preparation is completed by ITOPS IO.

PITC and AITC servers have the latest program updates and security patches. These updates are performed on a regular, monthly patching schedule determined by ITOPS IO. An additional update performed previous to this iteration was the upgrade

Table 3 describes the 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
PITC/AITC	Security Patches/Program Updates	None identifiable	Implement/Verify	ITOPS IO
PITC/AITC	Upgrade to Java 8 and WebLogic 12 to support JLV 3.0	Install on all JLV Web layer servers	Verify	ITOPS IO

3.3.   Resources

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

3.3.1.   Facility Specifics

JLV is deployed in the virtualized environments at both the PITC and AITC data centers.

3.3.2.   Hardware

Table 4 describes the hardware specifications required at each site prior to deployment. Please see Table 2 for details about the party(ies) responsible for preparing the site to meet the hardware specifications.

Table 4: Virtual Machine (VM) Production Hardware Specifications

Required Hardware	Model	Configuration	Manufacturer	Other
Windows Server	Windows Server 2012 Enterprise R2 (64-bit)	4 processors, 16 GB RAM (JLV)	Virtual	18 servers for AITC 18 servers for PITC
		4 processors, 16 GB RAM (jMeadows)	Virtual	25 servers for AITC 25 servers for PITC
		4 processors, 16 GB RAM (VDS)	Virtual	25 servers for AITC 24 servers for PITC
		5 processors, 16 GB RAM (VDS)	Virtual	1 server for PITC
		4 processors, 8 GB RAM (Report Builder)	Virtual	6 servers for AITC 6 servers for PITC
		2 processors,16 GB RAM (Report Builder File Server)	Virtual	1 server for AITC 1 server for PITC
Linux Server	Red Hat 7, Apache 2.4	4 processors, 8 GB RAM Single Sign on Internal (SSOi)	Virtual	18 servers for AITC 18 servers for PITC
		4 processors, 16 GB RAM (EHRM Service)	Virtual	6 servers for AITC 6 servers for PITC
DB Server	Windows Server 2012 Enterprise R2 (64-bit) Microsoft (MS) Structured Query Language (SQL) Server 2012	8 processors,16 GB RAM	Virtual	1 server for PITC
		4 processors, 16 GB RAM	Virtual	1 server for AITC
		16 processors, 28 GB RAM	Virtual	1 server for AITC 1 server for PITC

3.3.3.　Software

Table 5 describes the software specifications required at each site prior to deployment. Please see Table 2 for details about the party(ies) responsible for preparing the site to meet the software specifications.

Table 5: Software Specifications

Required Software	Make	Version	Manufacturer	Tier	Other
MS SQL Server 2012	N/A	2012	MS	Data / Storage Tier	N/A
Windows Server 2012	N/A	2012	MS	Data / Storage Tier	N/A
Oracle WebLogic Server 11G	N/A	10.3.6	Oracle	Abstraction Tier	N/A
Oracle WebLogic Server 12c	N/A	12.2.1.4.0	Oracle	Abstraction Tier	N/A
Red Hat Linux	N/A	7	Red Hat	Presentation Tier	N/A
Apache	N/A	2.4	Apache	Presentation Tier	N/A
SiteMinder	N/A	12.51	CA Technologies	VA User Authentication Tier	N/A
Tomcat	N/A	9.0.12	Apache	Presentation Tier	N/A

More information about SSOi server installation can be found in the *CA SiteMinder Apache Web Agent Install & Configuration Guide,* maintained by Identity and Access Management (IAM).

3.3.4.   Communications

ITOPS IO performs JLV installation and deployment activities in the virtualized environments at PITC and AITC, utilizing the release-ready package provided by the Liberty project team. When possible, the installation is performed during 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 a JLV release notification via SNOW /Change (CHG) Order
2. Plan the system downtime and change notifications:
    a.   Notify the JLV PM and the OIT PM/COR
3. Back up the systems and/or current deployment
4. Perform the installation/deployment:
    a.   Remove the current installation from service and deploy the new version
    b.   Validate the installation of the new version
5. Notify the stakeholders and Product team that systems are online

3.3.4.1.   Deployment/Installation/Backout Checklist

Table 6 captures the coordination effort and documents the day/time/individual when each activity (deploy, install, back-out) is completed for a project.

Table 6: Deployment, Installation, and Backout Checklist

Activity	Day	Time	Completed By
Deployment	Decision by VA OIT	Deployment dependent on a planned maintenance ticket	ITOPS IO
Installation	Coordinated with IO	Coordinated with IO	ITOPS IO
Backout	As needed	As needed, with a time estimate to be communicated to stakeholders when determined	ITOPS IO

4. Installation

4.1. Preinstallation and System Requirements

Please see the Hardware and Software sections for information regarding preinstallation system requirements.

4.2. Platform Installation and Preparation

Refer to the *JLV Change Management (CM) Plan* for more information about the installation and deployment of JLV. Once approved, all project documentation is available on the REDACTED.

Table 7: Implementation Plan Summary

Considerations	Associated Details	
What systems are affected?	**Component:**	**Deployed to:**
	JLV Web Application	PITC/AITC Cloud Environment
	JLV Report Builder	PITC/AITC Cloud Environment
	jMeadows Data Service	PITC/AITC Cloud Environment
	EHRM Service	PITC/AITC Cloud Environment
	JLV DB	PITC/AITC Cloud Environment
	VDS	PITC/AITC Cloud Environment
	JLV QoS	PITC/AITC Cloud Environment
Who is impacted by the change?	JLV users	
What is the estimated timeframe for restoring service?	8 hours total for installation activities.	
What pre-**i**mplementation work is required?	Download installation files	

4.3. Download and Extract Files

All software installation files are in the D:\builds\ directory on the ITOPS IO Software Delivery Server. Their locations, and the chronological steps for downloading and extracting the software prior to installation, are held in a VA development location, accessible via EP access. Refer to Installation Procedures for more information.

4.4.   Database (DB) Creation

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

System design specifications and diagrams can be found in the VA JLV Product Repository on GitHub. See Purpose for the link to the repository.

4.5.   Installation Scripts

There are no installation scripts used in the deployment of JLV. The application is installed manually, with oversight by the JLV Support team.

4.6.   Cron Scripts

Cron scripts are Linux-based events. There are currently no cron scripts run for JLV.

The singular, regularly scheduled event is the hourly server health check, a Windows-based event.

4.7.   Access Requirements and Skills Needed for Installation

EP access is required for installation activities. JLV System Engineers have been granted VA EP, and they are designated to access the application servers for deployment, maintenance, and backout activities. This document assumes the installer has knowledge and experience with the Windows operating system, MS SQL Server, Linux, Apache, and Oracle WebLogic, in addition to a general understanding of the web-based applications and familiarity with networking and basic troubleshooting, such as Telnet and ping.

4.8.   Installation Procedures

The subsections below detail failover to avoid downtime, preinstallation, and installation procedures. A detailed list of the servers referenced in the installation procedures can be found in the VA JLV Product Repository on GitHub. See Purpose for the link to the repository.

4.8.1.   Installation Order to Avoid Downtime

Perform the installation steps (detailed in Installation Procedures) in the following order to avoid JLV system downtime:

1. Install the updated JLV product at the failover site
    a.   This step does not impact JLV users
2. Validate the installation at the failover site
3. ITOPS IO routes JLV users to the failover site via the Global Traffic Manager (GTM)
4. Install the updated JLV product at the primary site
    a.   This step does not impact JLV users
5. Validate the installation at the primary site
6. ITOPS IO routes JLV users to the primary site via the GTM

4.8.2.   Preinstallation Procedures

Before deploying the new release, verify that IO created a backup of the currently deployed JLV systems:

> 🛈   **NOTE:** ITOPS IO generates nightly snapshots for each of the Production servers.

1. Manually generate a backup of the JLV DBs by running the *Backup DB* task through SQL Server Management Studio (SSMS) using E:\DBBackups as the default save point:
2. Back up the JLV DBs the primary and failover environments
3. Archive the backup files per ITOPS IO procedures and the *JLV 3.0 Production Operations Manual (POM)* (See Platform Installation and Preparation for the link to the repository.)
   a. Archived application .ear files are stored in: D:\builds\archive
4. Record the JLV software version number to be installed (for reference), as well as the software version number of the previous installation
   a. These numbers are detailed in the installation checklist used by PITC, AITC, and the JLV Support team

> 🛈   **NOTE:** Should any problems arise from the deployment of the updated JLV application, the backup snapshots and DB files are used to back out of the deployment and restore the previous JLV installation.

Once the preinstallation activities are complete, the installation of JLV system components begins in the primary and failover environments.

4.8.3.   Installation at Primary and Failover Operating Environments

Complete these installation steps at the failover site first, validate the installation according to the steps in Installation Verification Procedures, route JLV users to the failover site, then perform these installation steps at the primary site. See Deployment Topology for identification of primary and failover sites.

4.8.3.1.   Update the JLV DBs (~15 Minutes)

1. Remote desktop into the DB server
2. Open MS SSMS
3. Connect to *localhost* in SSMS
4. Open the SQL script *JLV_3.0.0.0_update.sql*, provided with the JLV 3.0.0.0 source code package submission
5. Execute the SQL script *JLV_3.0.0.0_update.sql*

4.8.3.2.   Install jMeadows (~30 Minutes)

1. Remote desktop into the jMeadows server
2. Upload the *jMeadows-3.0.0.0.(PITC/AITC)-PROD.ear*build to the D:\builds\ directory on the jMeadows server

3. Copy the previously deployed *jMeadows-2.9.6.0.3-production.ear* build as a backup into the D:\builds\archive directory

4. Validate that the following external endpoint web service is available by testing connectivity through a web browser on the jMeadows servers:

   a. **Example:** Copy the endpoint Universal Resource Locator (URL) (either https://jlvmds-aitc.med.va.gov/jMeadows/jMeadowsDataService?wsdl or https://jlvmds-pitc.med.va.gov/jMeadows/jMeadowsDataService?wsdl) into the address bar of a web browser

   b. The installer should expect to see the endpoint URL page with no errors

5. Log in to the WebLogic Admin console on the jMeadows server

6. Stop the previously deployed *jMeadows-2.9.6.0.3-production.ear* build through the WebLogic Admin console

   a. Click the **Deployments** link

   b. Click **Lock & Edit**

   c. Click checkbox next to the previous jMeadows deployment

   d. Click **Delete**

   e. Click **OK** to confirm removal

   f. Once the removal is complete, click **Activate Changes**

7. Deploy the *jMeadows-3.0.0.0 (PITC/AITC)-PROD.ear* build through the WebLogic Admin console

   a. The .ear files are staged in the D:\builds\ directory

   b. Click the **Deployments** link

   c. Click **Lock & Edit**

   d. Click **Install**

   e. Type the path to the location of the .ear file in D:\builds\ on the next page

   f. Click the radio button next to the jMeadows build to be deployed, and click **Next**

   g. Set the application name to *jMeadows-3.0.0*

   h. Click **Finish** to complete the installation to the jMeadows cluster

   i. Once the deployment is complete, click **Activate Changes**

8. Start the application, and verify its state is active using the **Monitoring** tab

   a. Click the **Deployments** link in the **Domain Structure** window of the WebLogic Admin console

   b. Click the recently installed application, and select **Start**

   c. Once started, the **State** column indicates *"Active"*

9. Validate that the jMeadows endpoint web service (either https://jlvmds-aitc.med.va.gov/jMeadows/JMeadowsDataService?wsdl or https://jlvmds-pitc.med.va.gov/jMeadows/jMeadowsDataService?wsdl) is available by testing connectivity through a web browser on the jMeadows servers using the environment-specific servers and ports found in the WebLogic admin console

4.8.3.3. Install the JLV application (~30 Minutes)

1. Remote desktop into the Web server
2. Upload the *JLV-3.0.0.0.(PITC/AITC)-PROD.ear* build to D:\builds\ directory on the Web server
3. Copy the previously deployed *JLV-2.9.6.0.3-production.ear* build as a backup into the D:\builds\archive directory
4. Validate that the following JLV web service is available by testing connectivity through a web browser on the JLV web server
   a. Example: User copies the endpoint URL (either https://jlv-aitc.med.va.gov.va.gov/JLV or https://jlv-pitc.med.va.gov.va.gov/JLV) into a web browser
   b. The installer should expect to see the endpoint URL page with no errors
5. Log in to the WebLogic Admin console on the Web server
6. Stop the previously deployed *JLV-2.9.6.0.3-production.ear* build through the WebLogic Admin console
   a. Click the **Deployments** link
   b. Click **Lock & Edit**
   c. Click the checkbox next to the previous JLV deployment
   d. Click **Delete**
   e. Click **OK** to confirm removal
   f. Once removal is complete, click **Activate Changes**
7. Deploy the *JLV-3.0.0.0.(PITC/AITC)-PROD.ear* build through the WebLogic Admin console
   a. The .ear files are staged in the D:\builds\ directory
   b. Click the **Deployments** link
   c. Click **Lock & Edit**
   d. Click **Install**
   e. Type the path to the location of the .ear file in D:\builds\ on the next page
   f. Click the radio button next to the JLV build to be deployed, and click **Next**
   g. Set the application name to *JLV_3.0.0*
   h. Click **Finish** to complete the installation to the JLV cluster
   i. Once the deployment is complete, click **Activate Changes**
8. Start the application, and verify its state is active using the **Monitoring** tab
   a. Click **Deployments** link in the **Domain Structure** window of the WebLogic Admin console
   b. Click the recently installed application, and select **Start**
   c. Once started, the **State** column indicates *"Active"*
9. Validate that the JLV web portal is available by testing connectivity through a web browser, outside of the JLV servers, using the public URL

4.8.3.4. Install VDS (~15 Minutes)

1. Remote desktop into the VDS server

2. Upload the *VistaDataService-3.0.0.0.(PITC/AITC)-PROD.war* build to D:\builds\ directory on the VDS server

3. Copy the previously deployed *VistaDataService-2.9.6.0.3-production.war* build as a backup into the D:\builds\archive directory

4. Validate that the following VDS endpoints are available by testing connectivity through a web browser on the VDS servers

   a. Example: User copies the endpoint URL (either https://jlvvds-aitc.med.va.gov/VistaDataService/VistaDataService?wsdl or https://jlvvds-pitc.med.va.gov/VistaDataService/VistaDataService?wsdl) into a web browser

   b. The installer should expect to see the endpoint URL page with no errors

5. Log in to the WebLogic Admin console on the VDS server

6. Stop the previously deployed *VistaDataService-2.9.6.0.3-production.war* build through the WebLogic Admin console

   a. Click the **Deployments** link

   b. Click **Lock & Edit**

   c. Click the checkbox next to the previous VistaDataService deployment

   d. Click **Delete**

   e. Click **OK** to confirm removal

   f. Once removal is complete, click **Activate Changes**

7. Deploy the *VistaDataService-3.0.0.0.(PITC/AITC)-PROD.war* build through the WebLogic Admin console

   a. The .war files are staged in the D:\builds\ directory

   b. Click the **Deployments** link

   c. Click **Lock & Edit**

   d. Click **Install**

   e. Type the path to the location of the .war file in D:\builds on the next page

   f. Click the radio button next to the VistaDataService build to be deployed, and click **Next**

   g. Set the application name to *VistaDataService_3.0.0*

   h. Click **Finish** to complete the installation to the VistaDataService cluster

   i. Once the deployment is complete, click **Activate Changes**

8. Start the application, and verify its state is active using the **Monitoring** tab

   a. Click the **Deployments** link in the **Domain Structure** window of the WebLogic Admin console

   b. Click the recently installed application, and select **Start**

   c. Once started, the **State** column indicates *"Active"*

9. Validate that the VDS endpoint (either https://jlvvds-aitc.med.va.gov/VistaDataService/VistaDataService?wsdl or https://jlvvds-pitc.med.va.gov/VistaDataService/VistaDataService?wsdl) is available by testing connectivity through a web browser on the VDS servers; if the VDS endpoint is not available, check and validate the deployment

4.8.3.5.   Install Report Builder (~15 Minutes)

1. Remote desktop into the server hosting the AdminServer

2. Upload *reportbuilder-3.0.0.0-production_VA.ear* to the **Report Builder** domain of the directory D:\builds on the server hosting the AdminServer

3. Copy the previously deployed *reportbuilder-2.9.6.0.3-production_VA.ear* build as a backup into the D:\builds\archive directory

4. Remotely log in to the server hosting the AdminServer via Remote Desktop Protocol

5. Open Internet Explorer and log in to the WebLogic Server Administration Console

6. Stop the previously deployed *reportbuilder-2.9.6.0.3-production_VA.ear* build through the WebLogic Admin console

   a. Click **Deployments** link

   b. Click **Lock & Edit**

   c. Select the checkbox next to the previous Report Builder deployment

   d. Click **Delete**

   e. Click **OK** to confirm removal

   f. Once removal is complete, click **Activate Changes**

7. Deploy the *reportbuilder-3.0.0.0-production.ear* build through the WebLogic Admin console

   a. The .ear files are staged in the D:\builds directory

   b. Click **Deployments** link

   c. Click **Lock & Edit**

   d. Click **Install**

   e. At the next page, type in path to location of .ear file d:\builds

   f. Click radio button next to Report Builder file name to be deployed, click **Next**

   g. Select the radio button next to the text *"Install this deployment as an application"* to deploy the .ear file as an application

   h. Set application name to *reportbuilder-3.0.0*

   i. Click **Finish** to complete the installation to the JLVRB_Cluster

   j. Once the deployment is complete, click **Activate Changes**

8. Start the application

9. Validate that the Report Builder endpoint is available by testing connectivity to the website (either https://jlvrb-aitc.med.va.gov/reportbuilder/systemInfo or https://jlvrb-pitc.med.va.gov/reportbuilder/systemInfo) via web browser

   a. The expected result is a json file will open in the browser (or a prompt to download the file will appear)

4.8.3.6.   Install EHRM Service

1. SSH into the EHRM server

2. Backup the current 2.9.6.0.3 ehrm.war file on /u01/app/apache/tomcat/latest/webapps/ and rename to ehrm.war.backup

3. Copy the provided 3.0.0 ehrm.war file to /u01/app/apache/tomcat/latest/webapps/

4.9. Installation Verification Procedures

After completing the installation processes detailed in [Installation Procedures](#) perform a manual smoke test. Use the steps below to test each module as an end user to validate the installation, deployment, and functionality of all JLV applications and services.

A detailed list of the servers referenced in the installation verification procedures can be found in the VA JLV Product Repository on GitHub. See [Purpose](#) for the link to the repository.

1. Validate that JLV is running
   a. Access the JLV application web page using the following URL: https://jlv-pitc.med.va.gov/JLV

      ℹ️ **NOTE:** This endpoint is also tested for the AITC environment using the following URL: REDACTED.

2. Validate that VA PIV and PIN are accepted by SSOi
3. Validate that the system status appears on the JLV **Login** page
   a. **Expected Result:** The system status should show a circular, green icon with a white checkmark
4. Validate the ability to log in with VA credentials
5. Validate that VA data displays within the JLV widgets, using test patients CHDR 1 and CHDR 2
6. Validate that FEHR data displays within the JLV widgets
7. Validate that community partner data displays within the JLV widgets
8. Validate that VA terminology mapping occurs
   a. **Expected Result:** VA terminology is properly mapped in the JLV widgets
9. Validate that DOD terminology mapping occurs
   a. **Expected Result:** DOD terminology is properly mapped in the JLV widgets
10. Validate that QoS is running by verifying that QoS is writing updates to the DB in the QoS_LOGS table
    a. Run the following command in SSMS on the active MSSQL server: select top 100 * from jlv.dbo.QOS_LOGS and order by date desc
       i. **Expected Result:** The select top 100* results will be displayed and indicate a time stamp of within 5 minutes of the time the query was run
       ii. If the top rows do not show, double check the installation steps
11. Validate that Report Builder is running
    a. **Expected Result:** The user can add items to the Report Builder and generate a printable Portable Document Format (PDF) file
12. Once all verification steps are complete, JLV users are rerouted back to the primary Production operating environment

4.10.   System Configuration

Table 4 describes the server configurations for JLV Enterprise Production infrastructure hosted at the AITC and PITC data centers.

4.11.   DB Tuning

JLV Engineering and Development and EPMO engineering ensure DB indexing for each release. Existing performance-based jobs are collaboratively reviewed, managed, and implemented (if changes are needed) with ITOPS IO database administrators (DBAs). The DB schema is validated with ITOPS IO DBAs for the deployment of each release.

5.   Backout Procedures

A backout is performed before a rollback. The backout procedures remove the newly installed components if the JLV deployment did not pass the installation verification procedures. Both backout and rollback are performed consecutively for each JLV component to return to the last known good operational state of the software and platform settings.

5.1.   Backout Strategy

The backout strategy is to uninstall the currently deployed JLV system components and restore the previously deployed version of JLV using the instructions listed in Rollback Procedures.

5.2.   Backout Considerations

The following subsections detail the considerations for backing out of the current installation of JLV.

5.2.1.   Load Testing

Load testing is currently being coordinated with the VA Enterprise Testing Service (ETS) team.

5.2.2.   User Acceptance Testing (UAT)

UAT results were not available at the time of this writing. When all testing cycles, including UAT, are complete, the data is made available in the VA JLV Product Repository on GitHub. See Purpose for the link to the repository.

5.3.   Backout Criterion

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

5.4.   Backout Risks

The risks for executing the backout are minimal because a backout is performed during planned downtime when users are not accessing the system. Once the restored system is online and validated, user access continues.

If a backout is initiated later in the deployment window, restoration time may exceed the downtime planned 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 VA PM, REDACTED.

5.6.   Backout Procedures

Because backout and rollback are performed consecutively, the backout and rollback procedures are combined in Rollback Procedures.

5.7.   Backout Verification Procedures

See Installation Verification Procedures.

6.   Rollback Procedures

A rollback is performed after a backout. The rollback procedures restore the previously deployed version of JLV.

6.1.   Rollback Considerations

The consideration for performing a rollback is that the JLV application does not operate as intended when tested by the JLV Support team.

6.2.   Rollback Criterion

The criterion for performing a rollback is that the JLV application does not operate as intended when tested by the JLV Support team.

6.3.   Rollback Risks

The risks for executing a rollback are minimal because the procedure is performed during a planned and announced downtime when users are not accessing the system. Therefore, users would not have accessed the newly deployed version of JLV and changes to user configuration files would not have occurred. When the system is online and validated, user access continues.

If a 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 VA PM, REDACTED.

6.5.   Rollback Procedures

Perform the following steps to uninstall the newly deployed JLV components and restore the previous installation in the PITC and AITC environments.

A detailed list of the servers referenced in the installation verification procedures can be found in VA JLV Product Repository on GitHub. See Purpose for the link to the repository.

1. Roll back jMeadows
   a. Remote desktop into the jMeadows server
   b. Log into the WebLogic Admin console on the jMeadows server
   c. Stop the *jMeadows-3.0.0.0.(PITC/AITC)-PROD.ear*build; WebLogic also undeploys the build from the clustered server(s)
   d. Deploy the *jMeadows-2.9.6.0.3-production.ear* build, located in the builds directory D:\builds\archive; WebLogic also deploys the build to the clustered servers(s) (See Installation Procedures and Installation Verification Procedures for more information.)
   e. Start the application

2. Roll back the JLV application
   a. Remote desktop into the Web server
   b. Log into the WebLogic Admin console on the Web server
   c. Stop the *JLV-3.0.0.0.(PITC/AITC)-PROD.ear*build; WebLogic also undeploys it from the clustered server(s)
   d. Deploy the *JLV-2.9.6.0.3-production.ear* build, located in the builds directory D:\builds\archive; WebLogic also deploys it to the clustered server(s)
   e. Start the application

3. Roll back VDS
   a. Remote desktop into the VDS server
   b. Log into the WebLogic Admin console on the VDS server
   c. Stop the *VistaDataService-3.0.0.0.(PITC/AITC)-PROD.war*build; WebLogic also undeploys the build from the clustered server(s)
   d. Deploy the *VistaDataService-2.9.6.0.3-production.war* build, located in the builds directory D:\builds\archive; WebLogic also deploys the build to the clustered server(s)
   e. Start the application

4. Roll back the JLV DB (15-minute time estimate)
   a. Remote desktop into DB
   b. Open SSMS
   c. Connect to *localhost*
   d. Restore the JLV DB using SSMS, using the backup files created prior to installation (See Installation Procedures.)

5. Roll back Report Builder
   a. Remote desktop into jMeadows
   b. Log into the WebLogic Admin console
   c. Stop the *reportbuilder-3.0.0.0-production_VA.ear* build; WebLogic also undeploys the build from the clustered server(s)
   d. Deploy the *reportbuilder-2.9.6.0.3-production_VA.ear* build, located in the builds directory D:\builds\archive; WebLogic also deploys the build to the clustered server(s)

      e. Start the application

6. Roll back EHRM Service

      a. SSH into the EHRM server

      b. Remove the 3.0.0 ehrm.war located in /u01/app/apache/tomcat/latest/webapps

      c. Rename ehrm.war.backup to ehrm.war located in /u01/app/apache/tomcat/latest/webapps

6.6.   Rollback Verification Procedures

After completing the rollback procedures, perform the validation steps in [Installation Verification Procedures](#). If all else fails, restore the servers from the nightly VM snapshots taken prior to the installation.

A. Acronyms and Abbreviations

Table 8 lists the acronyms and abbreviations are used throughout this document.

Table 8: Acronyms and Abbreviations

Acronym	Definition
AD	Active Directory
AITC	Austin Information Technology Center
API	Application Programming Interface
ATO	Authority to Operate
BHIE	Bidirectional Health Information Exchange
CA	Computer Associates
CAC	Common Access Card
CD2	Critical Decision Point 2
CDR	Clinical Data Repository
CM	Change Management
CHG	Change Order
COR	Contracting Officer's Representative
CVIX	Central VistA Imaging Exchange
DAS	Data Access Service
DB	Database
DBA	Database Administrator
DES	Data Exchange Service
DIBRG	Deployment, Installation, Backout, and Rollback Guide
DOD	Department of Defense
EHR	Electronic Health Record
EHRM	Electronic Health Record Modernization
eHX	eHealth Exchange
EP	Elevated Privilege
ePAS	Electronic Permission Access System
EPMO	Enterprise Program Management Office
FEHR	Federal Electronic Health Record
FHIR	Fast Healthcare Interoperability Resources
GB	Gigabyte
GTM	Global Traffic Manager
GUI	Graphical User Interface
HAIMS	Healthcare Artifact and Image Management Solution
HIE	Health Information Exchange
HRG	Hawaii Resources Group
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IP	Internet Protocol
ITOPS IO	IT Operations and Services (ITOPS),Infrastructure Operations (IO)
IT	Information Technology

Acronym	Definition
JDBC	Java Database Connectivity
JLV	Joint Longitudinal Viewer
LDAP	Lightweight Directory Access Protocol
MHS	Military Health System
MS	Microsoft
MPI	Master Person Index
OEHRM	Office of Electronic Health Record Modernization
OIT	Office of Information and Technology
PCMM	Patient Centered Management Module
PDWS	Patient Discovery Web Service
PDF	Portable Document Format
PITC	Philadelphia Information Technology Center
PM	Program Manager or Project Manager
POC	Point of Contact
POM	Production Operations Manual
QoS	Quality of Service
RAM	Random Access Memory
REST	Representational State Transfer
RPC	Remote Procedure Calls
RRR	Release Readiness Report
SOAP	Simple Object Access Protocol
SMS	Systems Made Simple
SNOW	Service Now
SSMS	SQL Server Management Studio
SSOi	Single Sign on Internal
SQL	Structured Query Language
TCP	Transmission Control Protocol
TMDS	Theater Medical Data Store
UAT	User Acceptance Testing
URL	Universal Resource Locator
VA	Department of Veterans Affairs
VDS	VistA Data Service
VIP	Veteran-Focused Integration Process
VistA	Veterans Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
VM	Virtual Machine