Community Viewer (CV) 3.7

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

June 2021

Version 1.0

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
06/01/2021	1.0	Addressed feedback and submitting the document for approval	Liberty ITS
05/27/2021	0.2	Comments addressed and updates included	Liberty ITS
05/03/2021	0.1	Initial draft of document from last approved	Liberty ITS

Artifact Rationale

This document describes the Deployment, Installation, Backout, and Rollback Guide (DIBRG) for Community Viewer (CV) releases going into the VA Enterprise. The Guide 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 it should be structured appropriately to reflect the particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the DIBRG is required to be completed prior to production deployment, 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

Community Viewer (CV) is a browser-based software application that facilitates the secure exchange of data between Department of Veterans Affairs (VA) systems and non-VA providers, known as Community Care Providers (CCPs). The exchange of data improves the coordination of care and continuity of care for VA patients receiving treatment outside of the VA network.

CV pulls information from VA health care systems in real time for viewing within a web browser. Through CV, VA Administrative Staff (VA Staff [VAS]) assign patients to CCPs and provision CCP use within the CV system, allowing CCPs access to view consolidated patient data from multiple Veterans Information Systems and Technology Architecture (VistA) systems.

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 CV 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 CV as deployed in the AITC and PITC Production environments.

1.2. Dependencies

CV is dependent on ancillary services that connect the application to specific data sources which are listed in the *CV 3.7 Production Operations Manual (POM)*. If any of these sources encounter a disruption in data services, the data is not pulled into CV.

ℹ **NOTE:** Additional functionality was added to align with the Joint Longitudinal Viewer (JLV) version 2.9.3 product release. In particular, CV now connects to the JLV Electronic Health Record Modernization (EHRM) Service which adds Cerner Millennium to the set of external data sources that CV can retrieve clinical data from. This set of data, known collectively as the Federal Electronic Health Record (FEHR) includes Department of Defense (DoD) medical treatment facilities and VA sites that have transitioned from VistA to Cerner Millennium. At the time of the CV v3.7 release, required approvals were not in place to allow CV to display DoD data to its Community Care Provider users. Therefore, all data from Cerner Millennium are turned off.

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

The physical environment, which provides security and environmental control over the CV servers, is restricted by Elevated Privilege (EP) access. Project personnel request EP access by submitting the *CV 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 CV.

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	Health Portfolio, OIT/Enterprise Project Management Division (EPMD) Joint Longitudinal Viewer (JLV)/CV Program Manager (PgM)	VA
REDACTED	CV Project Manager (PM)	VA
REDACTED	Contract Program Manager	Liberty ITS
REDACTED	Contract Project Manager	Liberty ITS
REDACTED	Contract Project Manager	Liberty ITS
REDACTED	CV Operations	Liberty ITS
REDACTED	CV DevOps Lead	Liberty ITS
REDACTED	CV Operations	Liberty ITS
REDACTED	CV Operations Lead	Liberty ITS
REDACTED	CV Development Lead	Liberty ITS
REDACTED	CV Java Developer	Liberty ITS
REDACTED	CV Java Developer	Liberty ITS
REDACTED	System Architect	Liberty ITS
REDACTED	System Engineer/Data Center	Seawolf

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

Table 2: DIBRG Roles and Responsibilities

Team	Phase/Role	Tasks
Enterprise Project Management Office (EPMO)/EPMD	Approval for Release to Production	Review the Release Readiness Report (RRR) with CV PM and Health Product Support (HPS) for approval; review and approve the ServiceNow (SNOW) board entry

Team	Phase/Role	Tasks
CV Support	Deployment	• Plan and schedule deployments (including orchestration with vendors) • Determine and document the roles and responsibilities of those involved in deployments • Test for operational readiness • Execute deployments
CV Support	Installation	• Plan and schedule installations • Ensure that the Authority to Operate (ATO) and certificate authority security documentation is in place • Validate through facility Points of Contact (POC) that Information Technology (IT) equipment has been accepted using the asset inventory processes • Coordinate training
CV Support	Backout	• Confirm the availability of backout instructions and backout strategy • Identify the criteria that triggers a backout
CV Support	Rollback	• Confirm the availability of rollback instructions and rollback strategy • Identify the criteria that triggers a rollback
CV Support	Post-Deployment	Provide hardware, software, and system support
CV Support	Post-Deployment	Production testing is verified

3. Deployment

The CV deployment workflow is outlined below.

1. Once EPMO approval is complete, the CV Support Team schedules the deployment with Infrastructure Operations (IO)
2. Once CV is deployed to the Production environment, Production testing is verified by the CV Support Team; please see Access Requirements and Skills Needed for the Installation for additional information
3. If there is an issue with the deployment, the project 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.

3.2. Site Readiness Assessment

CV servers deployed in the AITC and PITC Production environments (cloud and non-cloud) are utilized to host the CV web application and its associated services.

IO assesses the non-cloud, public-facing servers; CV Support Team assesses the internal servers, also referred to as cloud servers.

3.2.1. Deployment Topology (Targeted Architecture)

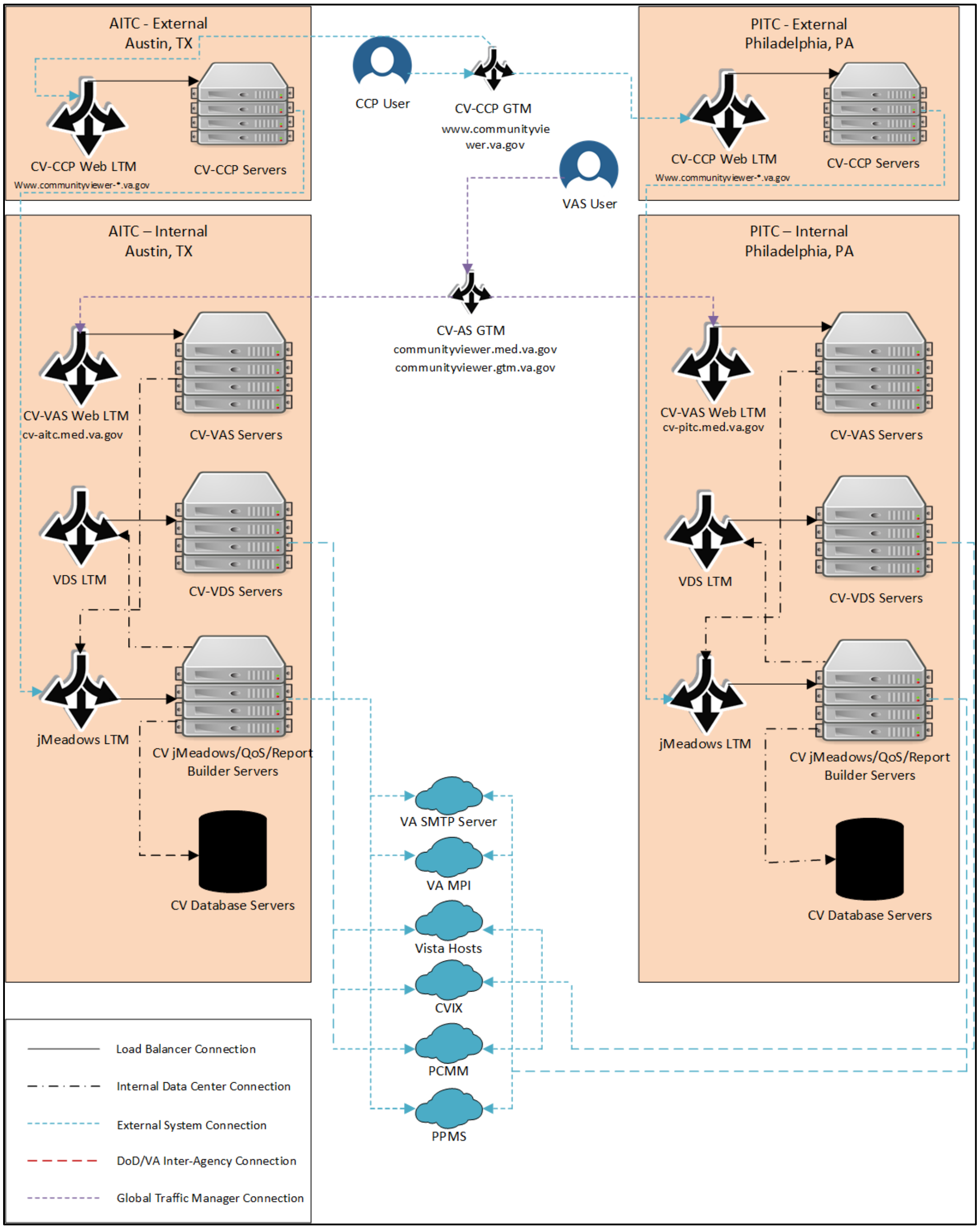
CV has environments at the PITC and AITC data centers. The primary operating environment is at PITC, with AITC serving as the failover site. Server details are documented in Table 4.

Figure 1 represents the targeted VAS and CCP architectures for the CV web application. System design specifications and diagrams can be found in the REDACTED on GitHub. See Purpose for information on the repository.

NOTE: Additional functionality was added to align with the JLV version 2.9.3 product release. In particular, CV now connects to the JLV EHRM Service which adds Cerner Millennium to the set of external data sources that CV can retrieve clinical data from. This set of data, known collectively as the Federal Electronic Health Record (FEHR) includes DoD medical treatment facilities and VA sites that have transitioned from VistA to Cerner Millennium. At the time of the CV v3.7 release, required approvals were not in place to allow CV to display DoD data to its CCP users. Therefore, all data from Cerner Millennium are turned off.

The figure below reflects the use of the EHRM Service server at both AITC and PITC. The figure also depicts the connection to the Cerner Fast Healthcare Interoperability Resources (FHIR) API. For the CV v3.7 release, as noted above, this functionality has been disabled, therefore Cerner FHIR data will not display.

Figure 1: CV Production Hardware Architecture[1]



3.2.2. Site Information (Locations, Deployment Recipients)

VA AITC and PITC host the CV web application and its system components.

[1] Central VistA Imaging Exchange (CVIX), Global Traffic Manager (GTM), Local Traffic Manager (LTM), Master Person Index (MPI), Patient-Centered Management Module (PCMM), Provider Profile Management System (PPMS), Quality of Service (QoS), Simple Mail Transfer Protocol (SMTP), VistA Data Service (VDS)

3.2.3. Site Preparation

Servers have the latest program updates and security patches. These updates are performed on a regular, monthly patching schedule.

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

Table 3: Site Preparation

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

3.3. Resources

The installation and deployment process for:

- CV components in the cloud environment is performed by the CV Support Team.
- CV web application in the non-cloud (on prem) environment is performed and managed by IO.

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

3.3.1. Facility Specifics

The CV application is deployed in PITC as the primary production site, with AITC serving as the failover site. See Figure 1 above for additional details.

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) Hardware Specifications

Required Hardware	Model	Configuration	Manufacturer	Server Count
CV Web Application (for VA Staff users)	Red Hat Enterprise Linux Server release 7 (Maipo)	2 Central Processing Units (CPUs), 16 Gigabytes (GB) Random Access Memory (RAM)	Virtual	2 Servers for AITC
	Red Hat Enterprise Linux Server release 7 (Maipo)	4 CPUs, 16 GB RAM	Virtual	2 Servers for PITC

Required Hardware	Model	Configuration	Manufacturer	Server Count
CV Web Application (for CCP users)	Red Hat Enterprise Linux Server release 7 (Maipo)	2 CPUs, 16 GB RAM	Virtual	3 Servers for AITC
	Red Hat Enterprise Linux Server release 7 (Maipo)	4 CPUs, 16 GB RAM	Virtual	3 Servers for PITC
VDS Servers	Red Hat Enterprise Linux Server release 7 (Maipo)	2 CPUs, 16 GB RAM	Virtual	3 Servers for AITC
	Red Hat Enterprise Linux Server release 7 (Maipo)	8 CPUs, 16 GB RAM	Virtual	4 Servers for PITC
jMeadows/ QoS/ Report Builder Servers	Red Hat Enterprise Linux Server release 7 (Maipo)	2 CPUs, 16 GB RAM	Virtual	4 Servers for AITC
	Red Hat Enterprise Linux Server release 7 (Maipo)	8 CPUs, 16 GB RAM	Virtual	4 Servers for PITC
CV DB Servers	Microsoft (MS) Windows Server 2012 R2 Standard	2 CPUs, 16 GB RAM	Virtual	2 Servers for AITC
	Microsoft (MS) Windows Server 2012 R2 Standard	8 CPUs, 28 GB RAM	Virtual	2 Servers 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	Other
MS Structured Query Language (SQL) Server	N/A	2012 R2	MS	N/A
Oracle WebLogic Server	N/A	12.1.3	Oracle	N/A
Apache	N/A	2.2.15/	Apache	N/A
SiteMinder	N/A	12.51	Computer Associates (CA) Technologies	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

IO performs the installation and deployment activities in the virtualized environments, 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 communication during the implementation process is as follows:

1. Submit a CV release notification via SNOW /Change (CHG) Order
2. Plan system downtime and change notifications:
   a. Notify the CV 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
5. Validate installation:
   a. Verify the IO cloud installation
   b. Verify the IO non-cloud (on prem) installation
6. Notify the stakeholders and Product Team that systems are online

3.3.4.1. Deployment/Installation/Backout Checklist

Table 6 gives details for the deployment, installation, and backout checklist.

Table 6: Deployment/Installation/Backout Checklist

Activity	Day	Time	Task Owner
Deployment	Joint decision between VA PMs	Deployment is dependent on a planned maintenance ticket	CV Support / IO
Installation	Coordinated with IO	Coordinated with IO	CV Support
Backout	As needed	As needed, with a time estimate to be communicated to stakeholders when determined	CV Support / 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/CV Software Configuration Management (CM) Plan* for more information about CV installation and deployment. 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:**
	CV Web Application (for VA Staff and RM users)	Cloud Environment
	CV Web Application (for CCP users)	Non-Cloud Environment
	CV Report Builder	Cloud Environment
	jMeadows Data Service	Cloud Environment
	CV DB	Cloud Environment
	VDS	Cloud Environment
	CV QoS	Cloud Environment
Who is impacted by the change?	CV users	
What is the estimated timeframe for restoring service?	8 hours total for installation activities	
What pre-implementation work is required?	Download installation files	

4.3. Download and Extract Files

All software installation files for this release will be staged in the /u01/CV_HOME/builds/target. Installation file 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 CV DB is created with a restore DB schema. The DB is a SQL Server 2012 DB, used to store community provider account information, patient assignments to community providers, user profile information, and audit records.

System design specifications and diagrams can be found in the REDACTED. See Purpose for information on the repository.

4.5. Installation Scripts

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

4.6. Cron Scripts

Not applicable to CV.

4.7. Access Requirements and Skills Needed for the Installation

EP access is required for installation activities. CV 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 and Linux operating systems, Oracle WebLogic, and SQL Server, in addition to a general understanding of web-based applications and familiarity with networking and basic troubleshooting, such as Telnet and ping.

4.8. Installation Procedures

The subsections below detail the preinstallation and installation procedures performed by the CV Support Team in the cloud environment. IO performs the same preinstallation and installation procedures in the non-cloud (on prem) environment.

A detailed list of the servers referenced in the installation procedures can be found in the REDACTED. See Purpose for information on the repository.

4.8.1. Preinstallation Procedures

Prior to executing the installation procedures detailed in Installation at Primary and Failover Operating Environments, the CV Support Team completes the following procedures in the cloud environment. IO performs the same preinstallation procedures in the non-cloud environment.

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

ℹ **NOTE:** IO generates nightly snapshots for each of the Production servers.

Manually generate a backup of the CV DBs by running the *Backup DB* task through SQL Server Management Studio (SSMS) using D:\DBBackups as the default save point:

1. Back up CV DBs
2. Archive the backup files per IO procedures and the *CV 3.7 POM* (See Platform Installation and Preparation for information on the repository)
   a. Archived application .war files are stored in: D:\builds\archive
3. Record the CV 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 IO and the CV Support Team

4.8.2. Installation at Primary and Failover Operating Environments

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

The following installation steps are completed by the CV Support Team. IO performs these same installation procedures in the non-cloud (on prem) environment.

4.8.2.1. Update the CV Database (DB) (~15 minutes)

1. Remote desktop into the DB server
2. Open MS SQL Management Studio (SSMS)

3. Connect to *localhost* in SSMS
4. Open the SQL Script, *CV_3.7.0.0.0_update.sql*, provided with the CV 3.x Source code package submission
5. Execute the SQL script *CV_3.7.0.0.0_update.sql*
6. Repeat steps 1–5 on the backup DB server

4.8.2.2. Install jMeadows-Community Care Provider (CCP) (~30 minutes)

1. Access the server using Remote Secure Access or Citrix
2. SSH in to the jMeadows and CV QoS server
3. Upload the *CVjMeadowsCCP-3.7.0.0.0-production.war* build to /u01/CV_HOME/builds/target directory on the jMeadows server
4. Copy the previously deployed *CVjMeadowsCCP-3.6.0.0.1-production.war* build as a backup in the /u01/CV_HOME/builds/archive directory
5. Validate that the following external endpoint web service is available by testing connectivity using curl on the jMeadows servers:
    a. **Example:** Run the command (Note: This is the load balancer URL): REDACTED.
    b. The installer should expect to see the endpoint URL page with no errors
6. Log in to the WebLogic Admin console on the jMeadows server
7. Undeploy the previously deployed *CVjMeadowsCCP-3.6.0.0.1-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 jMeadows deployment
    d. Click **Delete**
    e. Click **OK** to confirm removal
    f. Once removal is complete, click **Activate Changes**
8. Install the *CVjMeadowsCCP-3.7.0.0.0-production.war* build through the WebLogic Admin console
    a. The .war files are staged in the /u01/CV_HOME/builds/target directory
    b. Click the **Deployments** link
    c. Click **Lock & Edit**
    d. Click **Install**
    e. On the next page, type in the path to the location of the .war file in /u01/CV_HOME/builds/target
    f. Click the radio button next to the jMeadows build to be deployed, and click **Next**
    g. Set the application name to *CVjMeadowsCCP-3.7.0.0.0*
    h. Click **Finish** to complete installation to the jMeadows cluster
    i. Once the deployment is complete, click **Activate Changes**
9. 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"*
10. Validate that the following external endpoint web service is available by testing connectivity using curl on the jMeadows servers using the environment-specific servers and ports found in the WebLogic Admin console:
    a. **Example:** Run the command: REDACTED.

4.8.2.3. Install the CV application for CCP users (~30 minutes)

1. SSH into Web server
2. Upload the *CV-CCP-3.7.0.0.0-production.war* build to /u01/CV_HOME/builds/target directory on the Web server
3. Copy the previously deployed *CV-CCP-3.6.0.0.1-production.war* build as a backup in the /u01/CV_HOME/builds/archive directory
4. Validate that the following external endpoint web service is available by testing connectivity using curl on the web servers:
   a. **Example:** Access the public webpage using a web browser to the following URL: REDACTED.
   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. Undeploy the previously deployed *CV-CCP-3.6.0.0.1-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 CV-CCP deployment
   d. Click **Delete**
   e. Click **OK** to confirm removal
   f. Once removal is complete, click **Activate Changes**
7. Deploy the *CV-CCP-3.7.0.0.0-production.war* build through the WebLogic Admin console
   a. The .war files are staged in the /u01/CV_HOME/builds/target directory
   b. Click the **Deployments** link
   c. Click **Lock & Edit**
   d. Click **Install**
   e. Type the path to the location of the .war file (/u01/CV_HOME/builds/target) on the next page
   f. Click the radio button next to the CV-CCP build to be deployed, and click **Next**
   g. Set the application name to *CV-CCP-3.7.0.0.0*
   h. Click **Finish** to complete the installation to the CV-CCP 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 CV web portal is available by testing connectivity through a web browser, outside of the CV servers, using the public URL from step d

4.8.2.4. Install VistA Data Service (VDS) (~15 minutes)

1. SSH in to VDS server
2. Upload the *CVVistaDataService-3.7.0.0.0-production.war* build to /u01/CV_HOME/builds/target directory on the VDS server
3. Copy the previously deployed *CVVistaDataService-3.6.0.0.1-production.war* build as a backup in the /u01/CV_HOME/builds/archive directory
4. Validate that the following external endpoint web service is available by testing connectivity using curl on the VDS servers:
    a. **Example:** Run the command (Note: This is the load balancer URL): REDACTED.
    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. Undeploy the previously deployed *CVVistaDataService-3.6.0.0.1-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 *CVVistaDataService-3.7.0.0.0-production.war* build through the WebLogic Admin console
    a. The .war files are staged in the /u01/CV_HOME/builds/target directory
    b. Click the **Deployments** link
    c. Click **Lock & Edit**
    d. Click **Install**
    e. Type the path to the location of the .war file (/u01/CV_HOME/builds/target) on the next page
    f. Click the radio button next to the VistaDataService build to be deployed, and then click **Next**
    g. Set the application name to *CVVistaDataService-3.7.0.0.0*
    h. Click **Finish** to complete 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 Admin Console
    b. Click the recently installed application, and select **Start**
    c. Once started, the **State** column indicates *"Active"*
9. Validate that the following external endpoint web service is available by testing connectivity using curl on the VDS servers using the environment-specific servers and ports found in the WebLogic Admin console:
    a. **Example:** Run the command (Note: This is the load balancer URL): REDACTED.

4.8.2.5. Install Report Builder (~30 minutes)

1. Copy *setupReportBuilder-3.7.0.0.0-production.zip* onto the target jMeadows using WinSCP to /tmp directory
2. SSH in to the jMeadows server
3. Copy the previously deployed reportbuilder-3.6.0.0.1-production.jar build as a backup in the /u01/CV_HOME/builds/archive directory.
4. Execute the following commands from the command line:
    a. cd /tmp
    b. unzip setupReportBuilder-3.7.0.0.0-production.zip
    c. dzdo nano setuprb.sh
    d. dzdo ./setuprb.sh
5. Using WinSCP, copy *reportbuilder-3.7.0.0.0-production.jar* into /var/reportbuilder on the target server.
6. Execute the following commands from the command line:
    a. dzdo ln -s /var/reportbuilder/reportbuilder-3.7.0.0.0-production.jar /etc/rc/d/init.d/reportbuilder
    b. dzdo service reportbuilder restart
7. Verify the service is running by executing the following command:
    a. ps aux | grep reportbuilder | grep -v grep
8. Verify the port is listening by executing the following command:
    a. netstat -an | grep LISTEN | grep 7012

4.9. Installation Verification Procedures

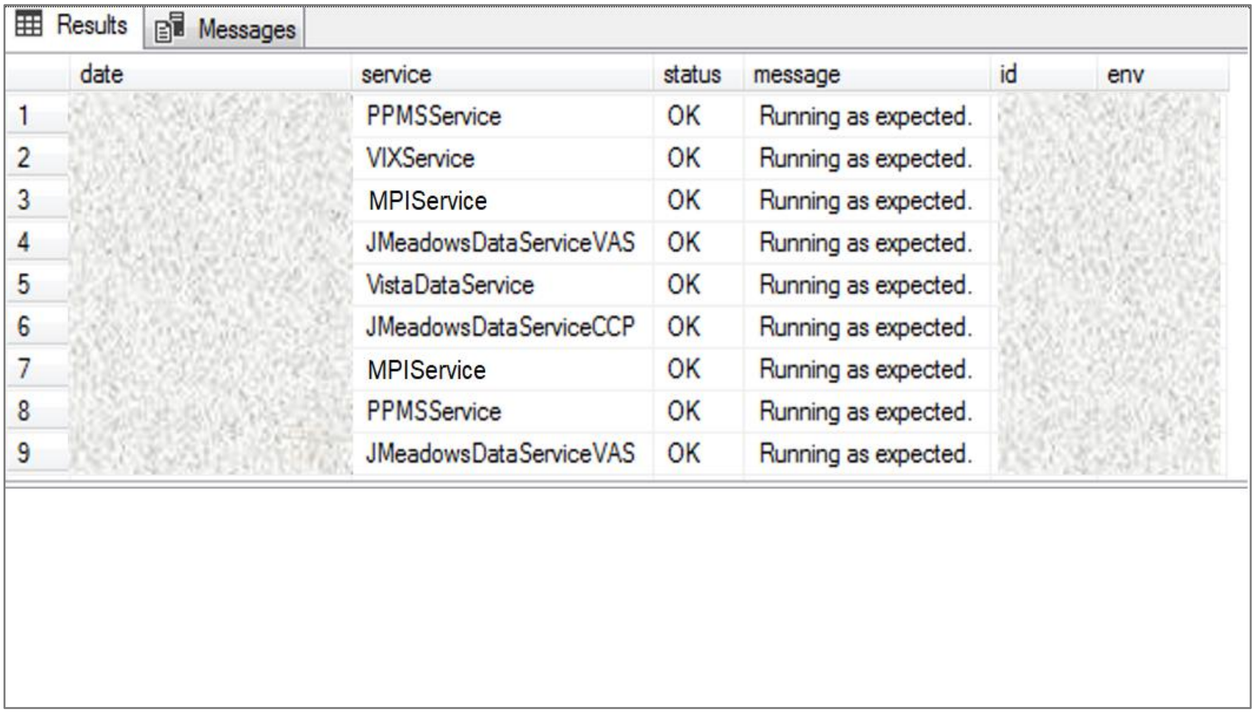
After completing the installation process detailed in Installation Procedures, perform a manual smoke test. Use the steps below to test each module as an end user to validate the installation, deployment, and functionality of all CV applications and services.

A detailed list of the servers referenced in the installation verification procedures can be found in REDACTED. See Purpose for information on the repository.

1. Validate that Quality of Service (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 cv.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

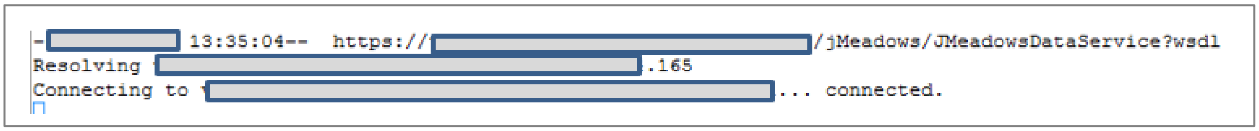
Figure 2: QoS Validation Expected Result



	date	service	status	message	id	env
1	[redacted]	PPMSService	OK	Running as expected.	[redacted]	[redacted]
2	[redacted]	VIXService	OK	Running as expected.	[redacted]	[redacted]
3	[redacted]	MPIService	OK	Running as expected.	[redacted]	[redacted]
4	[redacted]	JMeadowsDataServiceVAS	OK	Running as expected.	[redacted]	[redacted]
5	[redacted]	VistaDataService	OK	Running as expected.	[redacted]	[redacted]
6	[redacted]	JMeadowsDataServiceCCP	OK	Running as expected.	[redacted]	[redacted]
7	[redacted]	MPIService	OK	Running as expected.	[redacted]	[redacted]
8	[redacted]	PPMSService	OK	Running as expected.	[redacted]	[redacted]
9	[redacted]	JMeadowsDataServiceVAS	OK	Running as expected.	[redacted]	[redacted]

2. Validate that jMeadows is running by testing the connection to the Web Service Description Language (WSDL) on a Linux machine
    a. Run the wget command to confirm the download of the wsdl
    b. Wget –no-check-certificate https://<hostname>:<443> /jMeadows/JMeadowsDataService?wsdl
        i. **Expected Result:** The wsdl shows in the terminal window
        ii. If the wsdl does not show in the terminal window, double check the installation steps

Figure 3: jMeadows Validation Expected Result



```
-[redacted] 13:35:04--  https://[redacted]/jMeadows/JMeadowsDataService?wsdl
Resolving [redacted].165
Connecting to [redacted]... connected.
```

3. Validate Report Builder:
    a. Verify the service is running by executing the following command:

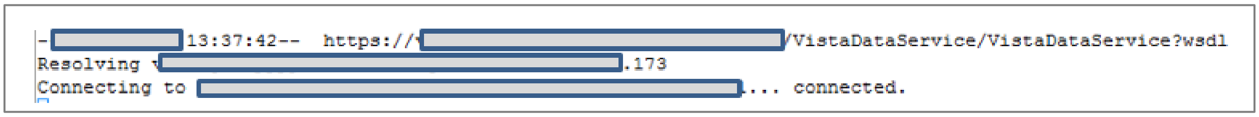
        i. ps aux | grep reportbuilder | grep -v grep

   b. Verify the port is listening by executing the following command:

        i. netstat -an | grep LISTEN | grep 7012

4. Validate that VDS is running by testing the connection to WSDL on a Linux machine
   a. Run the wget command to confirm the download of the wsdl
   b. Wget –no-check-certificate https://<hostname>:<443> /VistaDataService/VistaDataService?wsdl
        i. **Expected Result:** The wsdl shows in the terminal window
        ii. If the wsdl does not show in the terminal window, double check the installation steps

Figure 4: VDS Validation Expected Result



```
-[redacted]13:37:42--  https://[redacted]/VistaDataService/VistaDataService?wsdl
Resolving [redacted].173
Connecting to [redacted]... connected.
```

5. Validate HTTP Strict Transport Security (HSTS) compliance at the following address: https://securityheaders.com/?q=https%3A%2F%2Fwww.communityviewer.va.gov%2F&hide=on
   a. **Expected Result:** The Strict Transport Security will be in a green dialog box with a checkmark.
6. Validate that the system status appears on the CV Login page (internal [VAS])
   a. **Expected Result:** The system status should show a circular, green icon with a checkmark
7. Validate the ability to log in with VA credentials (internal [VAS])
8. Validate that VA data displays within the CV widgets using test patients Clinical/Health Data Repository (CHDR) 1 and CHDR 2 (internal [VAS])
9. Validate that VA terminology mapping occurs (internal [VAS])
   a. **Expected Result:** VA terminology is properly mapped in the CV widgets
10. Validate that the system status displays on the CV Login page (external)
    a. **Expected Result:** The system status should show a circular, green icon with a checkmark
11. Validate the ability to log in with CCP credentials (external [CCP])
    a. Check for no Cerner connection status icon
    b. Verify that no Cerner data is displaying.

4.10. System Configuration

Table 4 describes the server configuration for CV Production infrastructure.

4.11. DB Tuning

Not applicable to CV.

5. Backout Procedures

A backout is performed before a rollback. The backout procedures remove the newly installed components if the CV deployment did not pass the installation verification procedures. Both backout and rollback are performed consecutively for each CV 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 CV system components and restore the previously deployed version of CV.

5.2. Backout Considerations

There are no considerations for backing out of the current installation of CV.

5.3. Backout Criteria

The criteria for backing out the current installation is that CV does not operate as intended when tested by VA OIT and the CV Project Ops Team.

5.4. Backout Risks

The risks for executing the backout are minimal, because a backout is performed during a previously announced downtime when users are not accessing the system. When 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 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.

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 CV.

6.1. Rollback Considerations

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

6.2. Rollback Criteria

The criteria for performing a rollback is that the CV application does not operate as intended when tested by the CV Support Team.

6.3. Rollback Risks

The rollback procedures restore the previously deployed version of CV. Rollback is performed after a backout. 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 CV 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 current VA PM.

6.5. Rollback Procedures

Perform the following steps to uninstall the newly deployed CV components and restore the previous installation.

A detailed list of the servers referenced in the installation verification procedures can be found in the REDACTED. See Purpose for information on the repository.

1. Roll back jMeadowsCCP
   a. SSH in to the jMeadows server
   b. Log in to WebLogic Admin console on the jMeadows server
   c. Undeploy the *CVjMeadowsCCP-3.7.0.0.0-production.war* build; WebLogic also undeploys the build from the clustered server(s)
   d. Deploy *CVjMeadowsCCP-3.6.0.0.1-production.war* build located in the *Builds* directory /u01/CV_HOME/builds to the targeted cluster
   e. Start the application
   f. Validate all external endpoint web services are available by testing connectivity through a curl command on the jMeadows servers: REDACTED.
2. Roll back the CV application for CCP users
   a. SSH into the Web server
   b. Log into WebLogic Admin console on the Web server

   c. Undeploy the *CV-CCP-3.7.0.0.0-production.war* build; WebLogic also undeploys it from the clustered server(s)
   d. Deploy *CCV-CCP-3.6.0.0.1-production.war* build located in the *Builds* directory /u01/CV_HOME/builds to the targeted cluster.
   e. Start the application
   f. Validate that the CV web portal is available by testing connectivity through a web browser, outside of the CV servers, using the public URL
3. Roll back VDS
   a. SSH in to the VDS server
   b. Log in to the WebLogic Admin console on the VDS server
   c. Undeploy the *CVVistaDataService-3.7.0.0.0-production.war* build; WebLogic also undeploys the build from the clustered server(s)
   d. Deploy *CVVistaDataService-3.6.0.0.1-production.war* build located in the *Builds* directory /u01/CV_HOME/builds to the targeted cluster
   e. Start the application
   f. Validate that the following external endpoint web service is available by testing connectivity using curl on the VDS servers: REDACTED.
4. Roll back Report Builder
   a. SSH in to the jMeadows server
   b. Log in to the WebLogic Admin console on the jMeadows server
   c. Undeploy the *reportbuilder-3.7.0.0.0-production.jar;* WebLogic also undeploys the build from the build from the clustered server(s)
   d. Deploy *reportbuilder-3.6.0.0.1-production.jar* build located in the *Builds* directory /u01/CV_HOME/builds to the targeted cluster
   e. Start the application

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 VM snapshots taken prior to the upgrade.

Appendix A. Acronyms and Abbreviations

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

Table 8: Acronyms and Abbreviations

Acronym	Definition
AITC	Austin Information Technology Center
ATO	Authority to Operate
CA	Computer Associates
CCP	Community Care Provider
CD2	Critical Decision Point 2
CHDR	Clinical/Health Data Repository
CHG	Change Order
COR	Contracting Officer's Representative
CV	Community Viewer
CVIX	Central VistA Imaging Exchange
DB	Database
DIBRG	Deployment, Installation, Backout, and Rollback Guide
EP	Elevated Privilege
ePAS	Electronic Permission Access System
EPMO	Enterprise Program Management Office
FEHR	Federal Electronic Health Record
FHIR	Fast Healthcare Interoperability Resources
FQDN	Fully Qualified Domain Name
GB	Gigabyte
GTM	Global Traffic Manager
HSTS	HTTP Strict Transport Security
IAM	Identity and Access Management
IO	Infrastructure Operations
IT	Information Technology
JLV	Joint Longitudinal Viewer
LTM	Local Traffic Manager
MHS	Military Health System
MPI	Master Person Index
MS	Microsoft
OIT	Office of Information and Technology
PCMM	Patient-Centered Management Module
PgM	Program Manager
PITC	Philadelphia Information Technology Center
PM	Project Manager
POC	Point of Contact

Acronym	Definition
POM	Production Operations Manual
PPMS	Provider Profile Management System
QoS	Quality of Service
RAM	Random Access Memory
RRR	Release Readiness Report
SDE	Service Delivery Engineering
SMS	Systems Made Simple
SMTP	Simple Mail Transfer Protocol
SNOW	Service Now
SQL	Structured Query Language
SSH	Secure Shell
SSMS	SQL Server Management Studio
UAT	User Acceptance Testing
VA	Department of Veterans Affairs
VAS	VA Administrative Staff
VDS	VistA Data Service
VIP	Veteran-focused Integrated Process
VistA	Veterans Information Systems and Technology Architecture
VM	Virtual Machine
WSDL	Web Service Description Language