

**Community Viewer (CV) 3.1**  
**Deployment, Installation, Backout,**  
**and Rollback (DIBR) Guide**



**September 2019**

**Version 1.4**

**Department of Veterans Affairs (VA)**

**Office of Information and Technology (OIT)**

## Revision History

Date	Version	Description	Author
09/16/2019	1.4	Corrected previously deployed filenames in section 4.8.2 steps 5c and 5f	AbleVets
09/13/2019	1.3	Updated filenames with final build number	AbleVets
08/22/2019	1.2	Received VA PM Approval	AbleVets
08/19/2019	1.2	Submitted for VA PM Approval	AbleVets
08/15/2019	1.1	Implemented client feedback	AbleVets
08/08/2019	1.0	Delivered for review	AbleVets
04/02/2019	0.1	Initial draft of document from last approved	AbleVets

## Artifact Rationale

This document describes the Deployment, Installation, Backout, and Rollback Guide for Community Viewer 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 Deployment, Installation, Backout, and Rollback (DIBR) Guide is required to be completed prior to Critical Decision Point 2 (CD2), with the expectation that it is updated throughout the life cycle of the project for each build, as needed.

## Table of Contents

<b>1. Introduction .....</b>	<b>1</b>
1.1. Purpose.....	1
1.2. Dependencies.....	1
1.3. Constraints .....	1
<b>2. Roles and Responsibilities .....</b>	<b>2</b>
<b>3. Deployment.....</b>	<b>3</b>
3.1. Timeline.....	3
3.2. Site Readiness Assessment .....	3
3.2.1. Deployment Topology (Targeted Architecture) .....	3
3.2.2. Site Information (Locations, Deployment Recipients) .....	5
3.2.3. Site Preparation.....	6
3.3. Resources.....	6
3.3.1. Facility Specifics .....	6
3.3.2. Hardware.....	6
3.3.3. Software .....	7
3.3.4. Communications.....	7
3.3.4.1. Deployment/Installation/Backout Checklist .....	8
<b>4. Installation .....</b>	<b>8</b>
4.1. Preinstallation and System Requirements .....	8
4.2. Platform Installation and Preparation .....	8
4.3. Download and Extract Files .....	9
4.4. DB Creation .....	9
4.5. Installation Scripts.....	9
4.6. Cron Scripts.....	9
4.7. Access Requirements and Skills Needed for the Installation .....	9
4.8. Installation Procedures .....	9
4.8.1. Preinstallation Procedures.....	10
4.8.2. Installation at AITC (Cloud Environment).....	10
4.9. Installation Verification Procedures.....	17
4.10. System Configuration.....	19
4.11. DB Tuning .....	19
<b>5. Backout Procedures.....</b>	<b>19</b>
5.1. Backout Strategy .....	19
5.2. Backout Considerations.....	19
5.2.1. Load Testing.....	19
5.2.2. User Acceptance Testing (UAT) .....	19

5.3.	<b>Backout Criterion</b> .....	19
5.4.	<b>Backout Risks</b> .....	20
5.5.	<b>Authority for Backout</b> .....	20
5.6.	<b>Backout Procedures</b> .....	20
5.7.	<b>Backout Verification Procedures</b> .....	20
<b>6.</b>	<b>Rollback Procedures</b> .....	<b>20</b>
6.1.	<b>Rollback Considerations</b> .....	20
6.2.	<b>Rollback Criteria</b> .....	20
6.3.	<b>Rollback Risks</b> .....	20
6.4.	<b>Authority for Rollback</b> .....	21
6.5.	<b>Rollback Procedures</b> .....	21
6.6.	<b>Rollback Verification Procedures</b> .....	22
<b>Appendix A. Acronyms and Abbreviations</b> .....		<b>23</b>

### Table of Figures

Figure 1: CV VA Staff Production Architecture Deployed in AITC .....	4
Figure 2: CV CCP Production Architecture Deployed in AITC.....	5
Figure 3: QoS Validation Expected Result .....	17
Figure 4: jMeadows Validation Expected Result.....	18
Figure 5: VDS Validation Expected Result .....	18

### Table of Tables

Table 1: Project Roles .....	2
Table 2: Deployment, Installation, Backout, and Rollback Roles and Responsibilities .....	2
Table 3: Site Preparation.....	6
Table 4: Virtual Machine (VM) Hardware Specifications.....	6
Table 5: Software Specifications .....	7
Table 6: Deployment/Installation/Backout Checklist .....	8
Table 7: Implementation Plan Summary.....	8
Table 8: Acronyms and Abbreviations .....	23

# 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) 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 (DIBR) Guide 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 to be completed at the two VA data centers, located at the Austin Information Technology Center (AITC).

System design specifications and diagrams can be found in the [CV Design, Engineering, and Architecture \(DE&A\) Compliance Requirements collection](#) in the International Business Machines Corporation (IBM) Rational Tool Suite<sup>1</sup>.

[Figure 1](#) and [Figure 2](#) illustrate CV as deployed in the AITC Production environment.

## 1.2. Dependencies

CV is dependent on ancillary services that connect the application to specific data sources which are listed in the *CV 3.1 Production Operations Manual (POM)*. If any of these sources encounter a disruption in data services, the data is not pulled into CV.

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 held at AITC, 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.

---

<sup>1</sup> **NOTE:** Access to IBM Rational is restricted and must be requested.

## 2. Roles and Responsibilities

[Table 1](#) and [Table 2](#) list the project and DIBR roles and responsibilities.

**Table 1: Project Roles**

Name	Title/Group	Company
REDACTED	JLV/CV Program Manager	VA
REDACTED	Health Portfolio, OIT/Enterprise Project Management Division (EPMD) Community Viewer Project Manager (PM)	VA
REDACTED	Contract PM	AbleVets
REDACTED	Contract Deputy PM	AbleVets
REDACTED	CV Operations Lead	AbleVets
REDACTED	System Engineer	AbleVets
REDACTED	System Administrator	AbleVets
REDACTED	System Administrator	AbleVets
REDACTED	System Administrator	AbleVets
REDACTED	System Administrator	AbleVets
REDACTED	System Administrator	HRG
REDACTED	System Administrator	HRG
REDACTED	System Administrator	HRG
REDACTED	System Administrator	HRG
REDACTED	System Administrator	HRG
REDACTED	Technical Lead/Application Architect	HRG
REDACTED	System Engineer	HRG
REDACTED	Application Support/Sr. System Engineer, CV Integration Lead	HRG
REDACTED	System Engineer/Data Center	Lockheed Martin

Please note that references to the CV Support indicate Team AbleVets 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
EPMO	Approval for Release to Production	Review the Release Readiness Report (RRR) for CD2 with the CV Triad for approval; review and approve the Planning and Online Activity/Release Integration Scheduler (POLARIS) board entry
CV Support	Deployment	<ul style="list-style-type: none"> <li>Plan and schedule deployments (including orchestration with vendors)</li> <li>Determine and document the roles and responsibilities of those involved in deployments</li> <li>Test for operational readiness</li> <li>Execute deployments</li> </ul>

Team	Phase/Role	Tasks
CV Support	Installation	<ul style="list-style-type: none"> <li>Plan and schedule installations</li> <li>Ensure that the Authority to Operate (ATO) and certificate authority security documentation is in place</li> <li>Validate through facility Points of Contact (POC) that Information Technology (IT) equipment has been accepted using the asset inventory processes</li> <li>Coordinate training</li> </ul>
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	Hardware, software, and system support

### 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, 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 at the AITC Production environments.

#### 3.2. Site Readiness Assessment

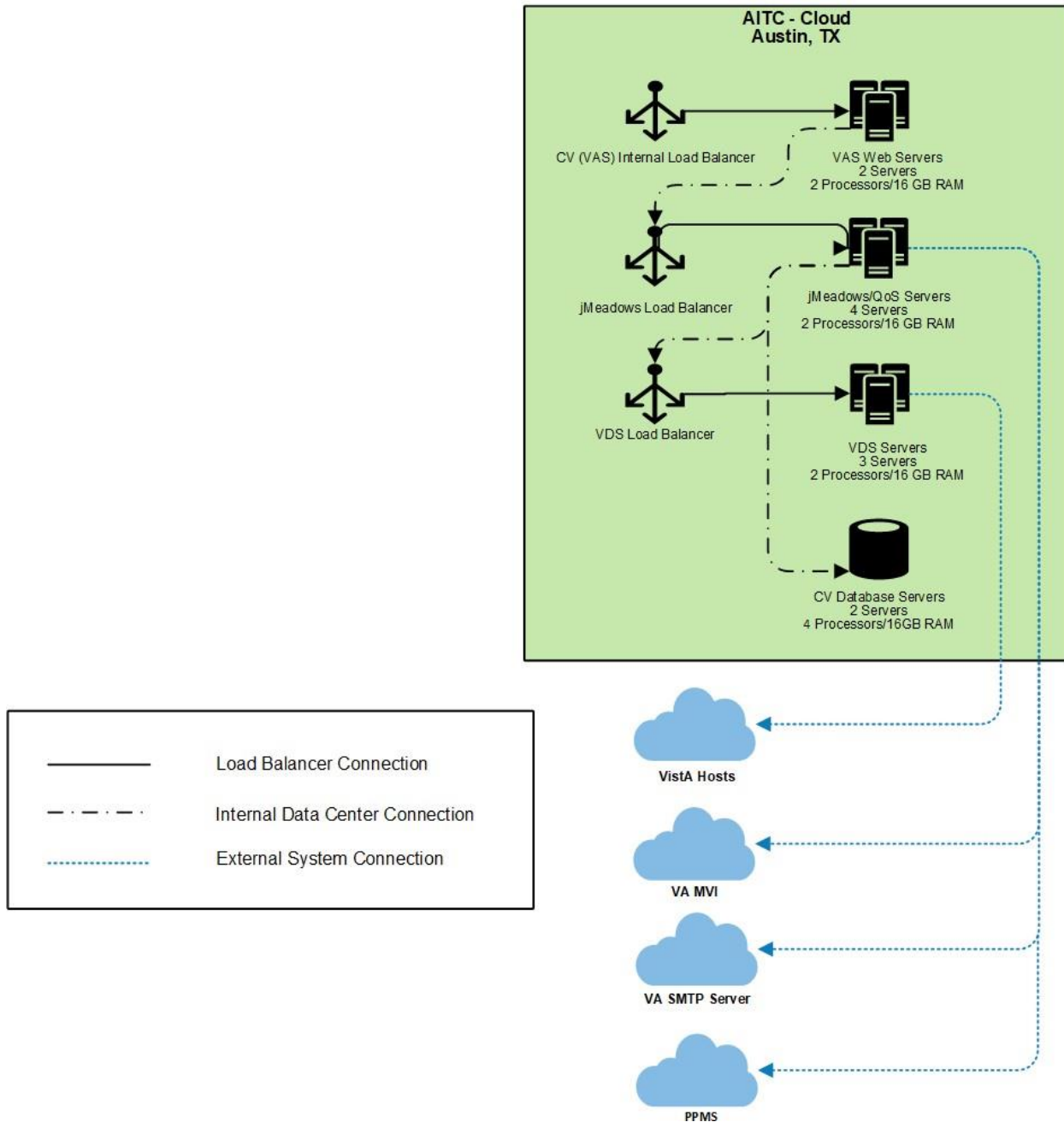
CV servers deployed in the AITC Production environments (cloud and non-cloud) are utilized to host the CV web application and its associated services.

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)

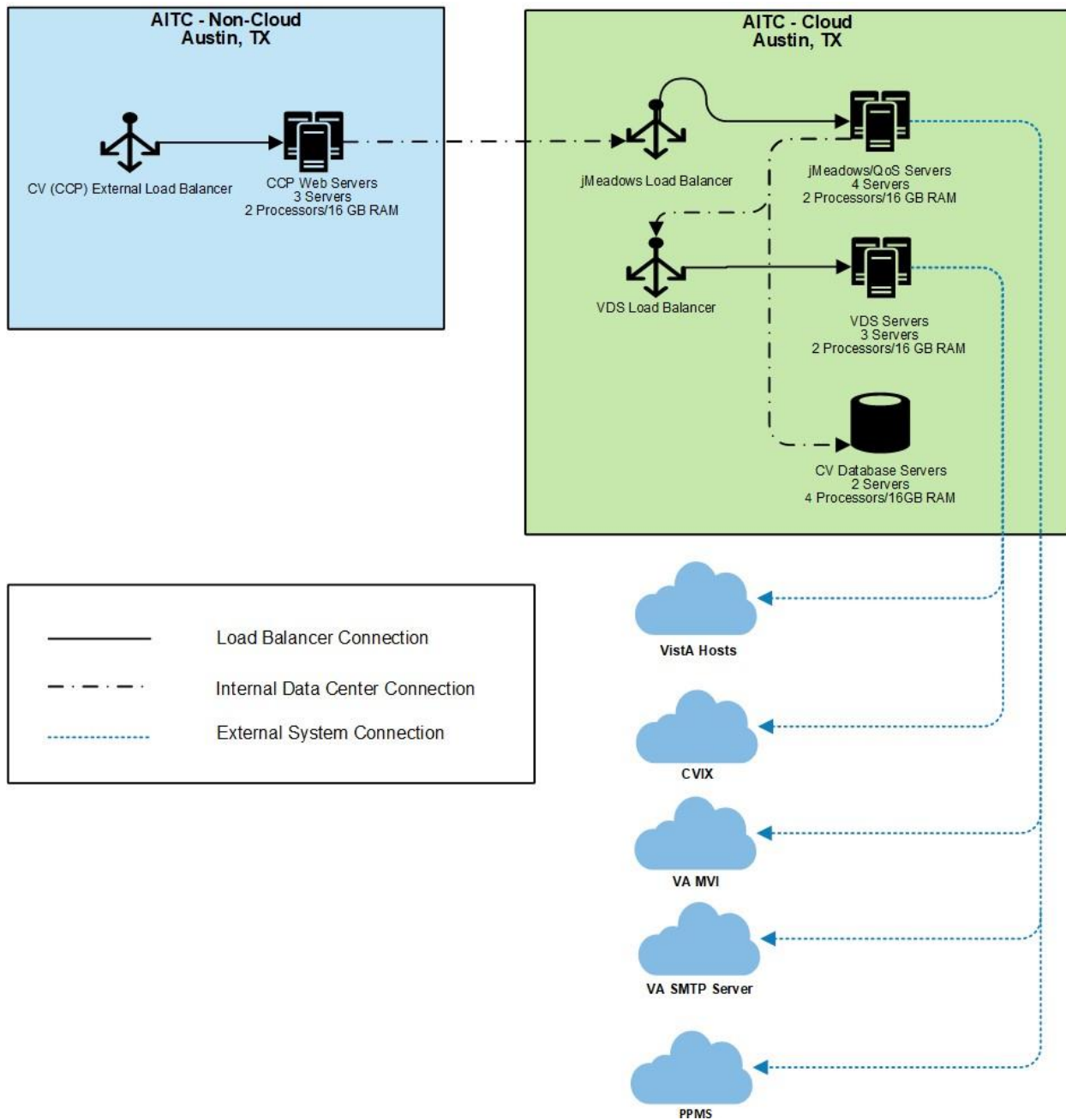
[Figure 1](#) and [Figure 2](#) represent the targeted VA Staff and CCP architectures for the CV web application. System design specifications and diagrams can be found in the CV DE&A Compliance Requirements collection in the IBM Rational Tool Suite. See [Purpose](#) for the link to the collection.

**Figure 1: CV VA Staff Production Architecture Deployed in AITC  
Community Viewer – VAS Production**





**Figure 2: CV CCP Production Architecture Deployed in AITC  
Community Viewer – CCP Production**



### 3.2.2. Site Information (Locations, Deployment Recipients)

The VA AITC hosts the CV web application and its system components.

### 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	Security Patches	None identifiable	Implement/Verify	IO
AITC	Program Updates	None identifiable	Implement/Verify	IO

### 3.3. Resources

The installation and deployment process for CV components in the AITC cloud environment is performed by the CV Support team.

The installation and deployment process for the CV web application in the AITC non-cloud 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 the cloud and non-cloud environments at AITC.

#### 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 6.9 (Santiago)	2 Central Processing Units (CPUs), 16 Gigabytes (GB) Random Access Memory (RAM)	Virtual	2 Servers
CV Web Application (for CCP users)	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	3 Servers
VDS Servers	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	3 Servers

Required Hardware	Model	Configuration	Manufacturer	Server Count
jMeadows/ Quality of Service (QoS) Service Servers	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	4 Servers
CV DB Servers	Microsoft (MS) Windows Server 2012 R2 Standard	4 CPUs, 16 GB RAM	Virtual	2 Servers

### 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 2012 R2	N/A	2012	MS	N/A
Oracle WebLogic Server Version 12.1.3	N/A	12.1.3	Oracle	N/A

### 3.3.4. Communications

IO performs the installation and deployment activities in the virtualized environment at AITC, utilizing the release-ready package provided by Team AbleVets. 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 POLARIS
2. Plan system downtime and change notifications:
  - a. Notify the CV PM and the OIT PM/COR
  - b. Submit a Request for Change Order (RFCO) for the web application deployment in the non-cloud environment:
    - i. E-mail the RFCO form and updated documentation to VA IT Service Delivery Engineering (SDE) and VA CV Operations Support (VACommunityviewopsup.va.gov); include the requested date and time of installation activities on the RFCO form
    - ii. Receive approval from AITC SDE and confirm the date/time
    - iii. AITC sends an approval request to the PM/COR
    - iv. The PM/COR approves the request
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 cloud installation

- b. Verify the non-cloud 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 [Project Joint Legacy Viewer \(JLV\)/CV SharePoint site](#)<sup>2</sup>.

**Table 7: Implementation Plan Summary**

Considerations	Associated Details	
What systems are affected?	<b>Component:</b>	<b>Deployed to:</b>
	CV Web Application (for VA Staff users)	AITC Cloud Environment
	CV Web Application (for CCP users)	AITC Non-Cloud Environment
	jMeadows Data Service	AITC Cloud Environment
	CV DB	AITC Cloud Environment
	VistA Data Service (VDS)	AITC Cloud Environment
	CV QoS	AITC Cloud Environment
Who is impacted by the change?	CV users	
What is the estimated timeframe for restoring service?	8 hours total for installation activities.	

<sup>2</sup> **NOTE:** Access to the Project JLV/CV SharePoint site is restricted and must be requested.

Considerations	Associated Details
What preimplementation 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. 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. 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 CV DE&A Compliance Requirements collection in the IBM Rational Tool Suite. See [Purpose](#) for the link to the collection.

### 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 AITC cloud environment.

IO performs the same preinstallation and installation procedures in the AITC non-cloud environment.

A detailed list of the servers referenced in the installation procedures can be found in the International Business Machines Corporation (IBM) [Rational Source Control Repository](#).<sup>3</sup>

<sup>3</sup> **NOTE:** Access to IBM Rational is restricted and must be requested.

### 4.8.1. Preinstallation Procedures

Prior to executing the installation procedures detailed in [Installation at AITC \(Cloud Environment\)](#), the CV Support team completes the following procedures in the AITC cloud environment.

IO performs the same preinstallation procedures in the AITC non-cloud environment.

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

 **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 3.1 POM*. (See [Platform Installation and Preparation](#) for the link to 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 AITC (Cloud Environment)

The following installation steps are completed by the CV Support team in the AITC cloud environment.

IO performs these same installation procedures in the AITC non-cloud environment.

1. Update the CV DB in the AITC cloud environment (15-minute time estimate)
  - a. Remote desktop into the DB server
  - b. Open MS SQL SSMS
  - c. Connect to *localhost* in SSMS
  - d. Open the SQL Script, *CV\_3.1.0.0.5\_update.sql*, provided with the CV 3.1 Source code package submission
  - e. Execute the SQL script *CV\_3.1.0.0.5\_update.sql*
  - f. Repeat steps a–e on the backup DB server
2. Install jMeadows-VAS in AITC cloud environment (30-minute time estimate)
  - a. Access the server using Remote Secure Access or Citrix
  - b. Secure Shell (SSH) into the jMeadows and CV QoS server
  - c. Upload the *CVjMeadowsVAS-3.1.0.0.6-production.war* build to /u01/CV\_HOME/builds/target directory on the jMeadows server
  - d. Copy the previously deployed *CVjMeadowsVAS-3.0.0.0.5-production.war* build as a backup in the /u01/CV\_HOME/builds/archive directory

- e. Validate that the following external endpoint web service is available by testing connectivity using curl on the jMeadows servers:
    - i. **Example:** Run the command (Note: This is the load balancer URL): `curl -k https://vaausgtdvapprd43.aac.va.gov/jMeadows_VAS/jMeadowsDataService?wsdl`
    - ii. The installer should expect to see the endpoint URL page with no errors
  - f. Log in to the WebLogic Admin console on the jMeadows server
  - g. Undeploy the previously deployed *CVjMeadowsVAS-3.0.0.5-production.war* build through the WebLogic Admin console
    - i. Click the **Deployments** link
    - ii. Click **Lock & Edit**
    - iii. Click the checkbox next to the previous jMeadows deployment
    - iv. Click **Delete**
    - v. Click **OK** to confirm removal
    - vi. Once removal is complete, click **Activate Changes**
  - h. Install the *CVjMeadowsVAS-3.1.0.6-production.war* build through the WebLogic Admin console
    - i. The .war files are staged in the `/u01/CV_HOME/builds/target` directory
    - ii. Click the **Deployments** link
    - iii. Click **Lock & Edit**
    - iv. Click **Install**
    - v. Type in the path to the location of the .war file in `/u01/CV_HOME/builds/target` on the next page
    - vi. Click the radio button next to the jMeadows build to be deployed, and click **Next**
    - vii. Set the application name to *CVjMeadowsVAS-3.1.0.6*
    - viii. Click **Finish** to complete installation to the jMeadows cluster
    - ix. Once the deployment is complete, click **Activate Changes**
  - i. Start the application, and verify its state is active using the **Monitoring** tab
    - i. Click the **Deployments** link in the **Domain Structure** window of the WebLogic Admin console
    - ii. Click the recently installed application, and select **Start**
    - iii. Once started, the **State** column indicates “Active”
  - j. 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:
    - i. **Example:** Run the command: `curl -k https://[Fully Qualified Domain Name (FQDN)];port/jMeadows_VAS/jMeadowsDataService?wsdl`
3. Install jMeadows-CCP in AITC cloud environment (30-minute time estimate)
    - a. Access the server using Remote Secure Access or Citrix
    - b. SSH into the jMeadows and CV QoS server

- c. Upload the *CVjMeadowsCCP-3.1.0.0.5-production.war* build to /u01/CV\_HOME/builds/target directory on the jMeadows server
- d. Copy the previously deployed *CVjMeadowsCCP-3.0.0.0.5-production.war* build as a backup in the /u01/CV\_HOME/builds/archive directory
- e. Validate that the following external endpoint web service is available by testing connectivity using curl on the jMeadows servers:
  - i. **Example:** Run the command (Note: This is the load balancer URL): `curl -k https://vaausgtdvapprd43.aac.va.gov/jMeadows_CCP/JMeadowsDataService?wsdl`
  - ii. The installer should expect to see the endpoint URL page with no errors
- f. Log in to the WebLogic Admin console on the jMeadows server
- g. Undeploy the previously deployed *CVjMeadowsCCP-3.0.0.0.5-production.war* build through the WebLogic Admin console
  - i. Click the **Deployments** link
  - ii. Click **Lock & Edit**
  - iii. Click the checkbox next to the previous jMeadows deployment
  - iv. Click **Delete**
  - v. Click **OK** to confirm removal
  - vi. Once removal is complete, click **Activate Changes**
- h. Install the *CVjMeadowsCCP-3.1.0.0.5-production.war* build through the WebLogic Admin console
  - i. The .war files are staged in the /u01/CV\_HOME/builds/target directory
  - ii. Click the **Deployments** link
  - iii. Click **Lock & Edit**
  - iv. Click **Install**
  - v. On the next page, type in the path to the location of the .war file in /u01/CV\_HOME/builds/target
  - vi. Click the radio button next to the jMeadows build to be deployed, and click **Next**
  - vii. Set the application name to *CVjMeadowsCCP-3.1.0.0.5*
  - viii. Click **Finish** to complete installation to the jMeadows cluster
  - ix. Once the deployment is complete, click **Activate Changes**
- i. Start the application, and verify its state is active using the **Monitoring** tab
  - i. Click the **Deployments** link in the **Domain Structure** window of the WebLogic Admin console
  - ii. Click the recently installed application, and select **Start**
  - iii. Once started, the **State** column indicates “Active”
- j. 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:
  - i. **Example:** Run the command: `curl -k https://[Fully Qualified Domain Name (FQDN)];port/jMeadows_CCP/JMeadowsDataService?wsdl`



4. Install Report Builder in AITC cloud environment (30-minute time estimate)
  - a. Copy *setupReportBuilder-3.1.0.0.5-production.zip* onto the target jMeadows using WinSCP to /tmp directory
  - b. SSH into the jMeadows server
  - c. Execute the following commands from the command line:
    - i. `cd /tmp`
    - ii. `unzip setupReportBuilder-3.1.0.0.5-production.zip`
    - iii. `dzdo nano setuprb.sh`
    - iv. `dzdo ./setuprb.sh`
  - d. Using WinSCP, copy *reportbuilder-3.1.0.0.5-production.jar* into /var/reportbuilder on the target server.
  - e. Execute the following commands from the command line:
    - i. `dzdo ln -s /var/reporbuilder/reportbuilder-3.1.0.0.5-production.jar /etc/rc/d/init.d/reportbuilder`
    - ii. `dzdo service reportbuilder restart`
  - f. Verify the service is running by executing the following command:
    - i. `ps aux | grep reportbuilder | grep -v grep`
  - g. Verify the port is listening by executing the following command:
    - i. `netstat -an | grep LISTEN | grep 7012`
5. Install the CV application for VA Staff users in the AITC cloud environment (30-minute time estimate)
  - a. SSH into the Web server
  - b. Upload the *CV-VAS-3.1.0.0.6-production.war* build to /u01/CV\_HOME/builds/target directory on the Web server
  - c. Copy the previously deployed *CV-VAS-3.0.0.0.5-production.war* build as a backup in the /u01/CV\_HOME/builds/archive directory
  - d. Validate that the following external endpoint web service is available by testing connectivity using curl on the web servers:
    - i. **Example:** Run the command (Note: This is the load balancer URL): `curl -k https://vaausgtdvwbprd44.aac.va.gov/VACV`
    - ii. The installer should expect to see the endpoint URL page with no errors
  - e. Log in to the WebLogic Admin console on the Web server
  - f. Undeploy the previously deployed *CV-VAS-3.0.0.0.5-production.war* build through the WebLogic Admin console
    - i. Click the **Deployments** link
    - ii. Click **Lock & Edit**
    - iii. Click the checkbox next to the previous CV-VAS deployment
    - iv. Click **Delete**
    - v. Click **OK** to confirm removal
    - vi. Once removal is complete, click **Activate Changes**

- g. Deploy the *CV-VAS-3.1.0.0.6-production.war* build through the WebLogic Admin console
    - i. The .war files are staged in the /u01/CV\_HOME/builds/target directory
    - ii. Click the **Deployments** link
    - iii. Click **Lock & Edit**
    - iv. Click **Install**
    - v. Type the path to the location of the .war file (/u01/CV\_HOME/builds/target) on the next page
    - vi. Click the radio button next to the CV-VAS build to be deployed, and click **Next**
    - vii. Set the application name to *CV-VAS-3.1.0.0.6*
    - viii. Click **Finish** to complete installation to the CV-VAS cluster
    - ix. Once the deployment is complete, click **Activate Changes**
  - h. Start the application, and verify its state is active using the **Monitoring** tab
    - i. Click the **Deployments** link in the **Domain Structure** window of the WebLogic Admin console
    - ii. Click the recently installed application, and select **Start**
    - iii. Once started, the **State** column indicates “Active”
  - i. Validate that the CV web portal is available by testing connectivity through a web browser outside of the CV servers, using the internal VA URL from step d
6. Install the CV application for CCP users in the AITC non-cloud environment (30-minute time estimate)
- a. SSH into Web server
  - b. Upload the *CV-CCP-3.1.0.0.5-production.war* build to /u01/CV\_HOME/builds/target directory on the Web server
  - c. Copy the previously deployed *CV-CCP-3.0.0.0.5-production.war* build as a backup in the /u01/CV\_HOME/builds/archive directory
  - d. Validate that the following external endpoint web service is available by testing connectivity using curl on the web servers:
    - i. **Example:** Access the public webpage using a web browser to the following URL: <https://www.communityviewer.va.gov/Community>
    - ii. The installer should expect to see the endpoint URL page with no errors
  - e. Log in to the WebLogic Admin console on the Web server
  - f. Undeploy the previously deployed *CV-CCP-3.0.0.0.5-production.war* build through the WebLogic Admin console
    - i. Click the **Deployments** link
    - ii. Click **Lock & Edit**
    - iii. Click the checkbox next to the previous CV-CCP deployment
    - iv. Click **Delete**
    - v. Click **OK** to confirm removal
    - vi. Once removal is complete, click **Activate Changes**

- g. Deploy the *CV-CCP-3.1.0.0.5-production.war* build through the WebLogic Admin console
    - i. The .war files are staged in the /u01/CV\_HOME/builds/target directory
    - ii. Click the **Deployments** link
    - iii. Click **Lock & Edit**
    - iv. Click **Install**
    - v. Type the path to the location of the .war file (/u01/CV\_HOME/builds/target) on the next page
    - vi. Click the radio button next to the CV-CCP build to be deployed, and click **Next**
    - vii. Set the application name to *CV-CCP-3.1.0.0.5*
    - viii. Click **Finish** to complete the installation to the CV-CCP cluster
    - ix. Once the deployment is complete, click **Activate Changes**
  - h. Start the application, and verify its state is active using the **Monitoring** tab
    - i. Click the **Deployments** link in the **Domain Structure** window of the WebLogic Admin console
    - ii. Click the recently installed application, and select **Start**
    - iii. Once started, the **State** column indicates “Active”
  - i. 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
7. Install VDS in AITC cloud environment (15-minute time estimate)
- a. SSH into VDS server
  - b. Upload the *CVVistaDataService-3.1.0.0.5-production.war* build to /u01/CV\_HOME/builds/target directory on the VDS server
  - c. Copy the previously deployed *CVVistaDataService-3.0.0.0.5-production.war* build as a backup in the /u01/CV\_HOME/builds/archive directory
  - d. Validate that the following external endpoint web service is available by testing connectivity using curl on the VDS servers:
    - i. **Example:** Run the command (Note: This is the load balancer URL): `curl -k https://[FQDN]:port/VistaDataService/VistaDataService?wsdl`
    - ii. The installer should expect to see the endpoint URL page with no errors
  - e. Log in to the WebLogic Admin console on the VDS server
  - f. Undeploy the previously deployed *CVVistaDataService-3.0.0.0.5-production.war* build through the WebLogic Admin console
    - i. Click the **Deployments** link
    - ii. Click **Lock & Edit**
    - iii. Click the checkbox next to the previous VistaDataService deployment
    - iv. Click **Delete**
    - v. Click **OK** to confirm removal
    - vi. Once removal is complete, click **Activate Changes**

- g. Deploy the *CVVistaDataService-3.1.0.0.5-production.war* build through the WebLogic Admin console
  - i. The .war files are staged in the /u01/CV\_HOME/builds/target directory
  - ii. Click the **Deployments** link
  - iii. Click **Lock & Edit**
  - iv. Click **Install**
  - v. Type the path to the location of the .war file (/u01/CV\_HOME/builds/target) on the next page
  - vi. Click the radio button next to the VistaDataService build to be deployed, and then click **Next**
  - vii. Set the application name to *CVVistaDataService-3.1.0.0.5*
  - viii. Click **Finish** to complete installation to the VistaDataService cluster
  - ix. Once the deployment is complete, click **Activate Changes**
- h. Start the application, and verify its state is active using the **Monitoring** tab
  - i. Click the **Deployments** link in the **Domain Structure** window of the Admin Console
  - ii. Click the recently installed application, and select **Start**
  - iii. Once started, the **State** column indicates “Active”
  - i. 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:
    - i. **Example:** Run the command (Note: This is the load balancer URL): curl -k https://[FQDN]:port/VistaDataService/VistaDataService?wsdl
- 8. Install CV QoS Service in the AITC cloud environment (15-minute time estimate)
  - a. SSH into the jMeadows and CVQoS server
  - b. Upload the *CVQoS-3.1.0.0.5-production.war* build to /u01/CV\_HOME/builds/cv-qos directory on the jMeadows server
  - c. Copy the previously deployed *CVQoS-3.0.0.0.5-production.war* build as a backup in the /u01/CV\_HOME/builds/archive directory
  - d. Log in to the WebLogic Admin console on the jMeadows server
  - e. Undeploy the previously deployed *CVQoS-3.0.0.0.5-production.war* build through the WebLogic Admin console
    - i. Click the **Deployments** link
    - ii. Click **Lock & Edit**
    - iii. Click the checkbox next to the previous CV QoS deployment
    - iv. Click **Delete**
    - v. Click **OK** to confirm removal
    - vi. Once removal is complete, click **Activate Changes**
  - f. Deploy the *CVQoS-3.1.0.0.5-production.war* build through the WebLogic Admin console
    - i. The .war files are staged in the /u01/CV\_HOME/builds/cv-qos directory

- ii. Click **Deployments** link
- iii. Click **Lock & Edit**
- iv. Click **Install**
- v. Type the path to the location of the .war file (/u01/CV\_HOME/builds/cv-qos) on the next page
- vi. Click the radio button next to the CV QoS build to be deployed, and then click **Next**
- vii. Set the application name to *CVQoS-3.1.0.0.5*
- viii. Click **Finish** to complete installation to the CV QoS server
- ix. Once the deployment is complete, click **Activate Changes**
- g. Validate that the following external endpoint web service is available by testing connectivity using curl on the jMeadows server using environment-specific servers and ports found in the WebLogic Admin console:
  - i. **Example:** Run the command: `curl -k https://[FQDN]:port/CVQoS/CVQoSDataService?wsdl`

#### 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 IBM Rational Source Control. See [Installation Procedures](#) for the link to the repository.

1. 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 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 3: QoS Validation Expected Result**

Results		Messages				
	date	service	status	message	id	env
1		PPMSService	OK	Running as expected.		
2		VIXService	OK	Running as expected.		
3		MVIService	OK	Running as expected.		
4		JMeadowsDataServiceVAS	OK	Running as expected.		
5		VistaDataService	OK	Running as expected.		
6		JMeadowsDataServiceCCP	OK	Running as expected.		
7		MVIService	OK	Running as expected.		
8		PPMSService	OK	Running as expected.		
9		JMeadowsDataServiceVAS	OK	Running as expected.		

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 4: 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 5: VDS Validation Expected Result**

```

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

```

5. Validate 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)
  - 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)

8. Validate that VA data displays within the CV widgets, using text patients CHDR 1 and CHDR 2 (internal)
9. Validate that VA terminology mapping occurs (internal)
  - 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)

## 4.10. System Configuration

[Table 4](#) describes the server configuration for CV Production infrastructure, hosted at AITC.

## 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

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

### 5.2.1. Load Testing

Load testing is currently being coordinated.

### 5.2.2. User Acceptance Testing (UAT)

When all testing cycles, including UAT, are complete, the data is delivered to the [Quality Management](#) module of the IBM Rational Tool Suite<sup>4</sup>.

## 5.3. Backout Criterion

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

---

<sup>4</sup>NOTE: Access to IBM Rational is restricted and must be requested.

## **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 criterion 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 in the AITC environment.

A detailed list of the servers referenced in the installation verification procedures can be found in IBM Rational Source Control. See [Installation Procedures](#) for the link to the repository.

1. Roll back jMeadowsVAS in the AITC cloud environment
  - a. SSH into the jMeadows server
  - b. Log into WebLogic Admin console on the jMeadows server
  - c. Undeploy the *CVjMeadowsVAS-3.1.0.0.6-production.war* build; WebLogic also undeploys the build from the clustered server(s)
  - d. Deploy *CVjMeadowsVAS-3.0.0.0.5-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: `curl -k https://vaausgtdvapprd43.aac.va.gov/jMeadows_VAS/jMeadowsDataService?wsdl`
2. Roll back jMeadowsCCP in the AITC cloud environment
  - a. SSH into the jMeadows server
  - b. Log into WebLogic Admin console on the jMeadows server
  - c. Undeploy the *CVjMeadowsCCP-3.1.0.0.5-production.war* build; WebLogic also undeploys the build from the clustered server(s)
  - d. Deploy *CVjMeadowsCCP-3.0.0.0.5-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: `curl -k https://vaausgtdvapprd43.aac.va.gov/jMeadows_CCP/JMeadowsDataService?wsdl`
3. Roll back the CV application for VA Staff users in the AITC cloud environment
  - a. SSH into the Web server
  - b. Log into WebLogic Admin console on the Web server
  - c. Undeploy the *CV-VAS-3.1.0.0.6-production.war* build; WebLogic also undeploys it from the clustered server(s)
  - d. Deploy *CV-VAS-3.0.0.0.5-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 internal VA URL

4. Roll back the CV application for CPP users in AITC non-cloud environment
  - a. SSH in to the Web server
  - b. Log into WebLogic Admin console on the Web server
  - c. Undeploy the *CV-CCP-3.1.0.0.5-production.war* build; WebLogic also undeploys it from the clustered server(s)
  - d. Deploy *CCV-CCP-3.0.0.0.5-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
5. Roll back VDS in AITC cloud environment
  - a. SSH into the VDS server
  - b. Log into the WebLogic Admin console on the VDS server
  - c. Undeploy the *CVVistaDataService-3.1.0.0.5-production.war* build; WebLogic also undeploys the build from the clustered server(s)
  - d. Deploy *CVVistaDataService-3.0.0.0.5-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: curl -k https://vaausgtdvappr44.aac.va.gov/VistaDataService/VistaDataService?wsdl
6. Re-create CV DB in AITC cloud environment (15-minute time estimate)
  - a. Remote desktop into the DB server
  - b. Open SSMS
  - c. Connect to *localhost*
  - d. Restore the CV.mdf and CV\_log.ldf files using SSMS
    - i. The CV DB backups created prior to installation include the .mdf and .ldf files
    - ii. See [Preinstallation Procedures](#)

## 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**

<b>Acronym</b>	<b>Definition</b>
<b>AITC</b>	Austin Information Technology Center
<b>ATO</b>	Authority to Operate
<b>CCP</b>	Community Care Provider
<b>CD2</b>	Critical Decision Point 2
<b>COR</b>	Contracting Officer's Representative
<b>CV</b>	Community Viewer
<b>CVIX</b>	Central Vista Imaging Exchange
<b>DB</b>	Database
<b>DE&amp;A</b>	Design, Engineering, and Architecture
<b>DIBR</b>	Deployment, Installation, Backout, and Rollback
<b>EP</b>	Elevated Privilege
<b>ePAS</b>	Electronic Permission Access System
<b>EPMO</b>	Enterprise Program Management Office
<b>FQDN</b>	Fully Qualified Domain Name
<b>GB</b>	Gigabyte
<b>IBM</b>	International Business Machines Corporation
<b>IO</b>	Infrastructure Operations
<b>IT</b>	Information Technology
<b>JLV</b>	Joint Legacy Viewer
<b>MS</b>	Microsoft
<b>MVI</b>	Master Veteran Index
<b>OIT</b>	Office of Information and Technology
<b>PM</b>	Program Manager or Project Manager
<b>POC</b>	Point of Contact
<b>POLARIS</b>	Planning and Online Activity/Release Integration Scheduler
<b>POM</b>	Production Operations Manual
<b>PPMS</b>	
<b>QoS</b>	Quality of Service
<b>RAM</b>	Random Access Memory
<b>RFCO</b>	Request for Change Order
<b>RRR</b>	Release Readiness Report
<b>SDE</b>	Service Delivery Engineering
<b>SMS</b>	Systems Made Simple
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SQL</b>	Structured Query Language

<b>Acronym</b>	<b>Definition</b>
<b>SSH</b>	Secure Shell
<b>SSMS</b>	SQL Server Management Studio
<b>UAT</b>	User Acceptance Testing
<b>VA</b>	Department of Veterans Affairs
<b>VAS</b>	VA Staff
<b>VDS</b>	VistA Data Service
<b>VIP</b>	Veteran-focused Integrated Process
<b>VistA</b>	Veterans Information Systems and Technology Architecture
<b>VM</b>	Virtual Machine
<b>WSDL</b>	Web Service Description Language