Community Viewer (CV) 3.2

Production Operations Manual

November 2019

Version 1.2

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
12/02/2019	1.2	Approved by VA PM	AbleVets
11/27/2019	1.2	Updated following adjudication meeting and submitted for approval	AbleVets
11/27/2019	1.1	Addressed reviewer feedback	AbleVets
11/18/2019	1.0	Submitted for review	AbleVets
10/23/2019	0.1	Initial draft of document from the last approved and integrated content from the April 2019 CV Downtime Notification and Outage Triage Process version 1.4	AbleVets

Artifact Rationale

The Production Operations Manual (POM) provides the information needed by the Production Operations team to maintain and troubleshoot the product. The POM must be provided prior to release of the product.

Table of Contents

1. Introduction 1
2. Routine Operations 1
2.1. Administrative Procedures 1
2.1.1. System Startup 2
2.1.1.1. System Startup from Emergency Shutdown 4
2.1.2. System Shutdown 4
2.1.2.1. Emergency System Shutdown 4
2.1.3. Backup and Restore 4
2.1.3.1. Backup Procedures 4
2.1.3.2. Restore Procedures 5
2.1.3.3. Backup Testing 6
2.1.3.4. Storage and Rotation 7
2.2. Security/Identification (ID) Management 7
2.2.1. Identity Management 8
2.2.2. Access Control 8
2.3. User Notifications 9
2.3.1. User Notification Points of Contact 10
2.3.2. CV QoS Mail Groups 11
2.3.3. Scheduled Downtime Notifications 11
2.3.3.1. Planning and Online Activity/Release Integration Scheduler (POLARIS) Process 14
2.3.3.2. Patch Release Notification E-mail (Example) 15
2.3.4. Unscheduled Outage Notifications 15
2.3.4.1. Initial Response to Issues Within 30 Minutes of Alert 15
2.3.4.1.1. Initial Outage Response Notification E-Mail (Example) 16
2.3.4.2. Outage Escalation to External Teams 16
2.3.4.2.1. Outage Escalation to External Teams E-Mail (Example) 16
2.3.4.2.2. Outage Update E-Mail (Example) 17
2.3.5. Announcement Banners 18
2.3.5.1. Placing Announcement Banners 19
2.3.5.2. Removing Announcement Banners 20
2.3.5.2.1. Manual Removal 20
2.3.5.2.2. Automatic Expiration 21
2.3.5.2.3. Announcement Banner Extensions 21
2.4. System Monitoring, Reporting, and Tools 21
2.4.1. Dataflow Diagram 21
2.4.2. VistA Imaging (VI) Data Retrieval 22

2.4.3. PPMS Data Web Service (DWS) Retrieval 23
2.4.4. Availability Monitoring 24
2.4.4.1. Domain-Level Availability Monitoring 26
2.4.5. Performance/Capacity Monitoring 26
2.4.6. Critical Metrics 27
2.5. Routine Updates, Extracts, and Purges 27
2.5.1. Routine Updates 27
2.5.2. Quarterly Update of the VistA Site List 28
2.5.3. Extracts 28
2.5.4. Purges 28
2.6. Scheduled Maintenance 28
2.7. Unscheduled Outage Triage Process 29
2.7.1. Outage Triage Timeline 29
2.7.2. Escalation 30
2.7.3. Issue Resolution and After Action 31
2.8. Capacity Planning 31
2.8.1. Initial Capacity Plan 31
3. Exception Handling 32
3.1. Routine Errors 32
3.1.1. Security Errors 32
3.1.2. Login Errors 32
3.1.3. Timeouts 32
3.1.3.1. Application Timeout 32
3.1.3.2. Connection Errors 33
3.1.4. Concurrency 34
3.2. Significant Errors 34
3.2.1. Application Error Logs 34
3.2.2. Application Error Codes and Descriptions 36
3.2.3. Infrastructure Errors 36
3.2.3.1. DB 36
3.2.3.2. Web Server 40
3.2.3.3. Application Server 40
3.2.3.4. Network 40
3.2.3.5. Authentication and Authorization (A&A) 40
3.2.3.6. Logical and Physical Descriptions 41
3.3. Dependent System(s) 41
3.4. Troubleshooting 42
3.5. System Recovery 42
3.5.1. Restart After Unscheduled System Interruption 42

3.5.2. Restart After DB Restore 42
3.5.3. Backout Procedures 42
3.5.4. Rollback Procedures 42
4. Operations and Maintenance Responsibilities 42
5. Approval Signatures 45
A. Acronyms and Abbreviations 46

Table of Figures

Figure 1: Database Names Tree 5
Figure 2: Source/Device/Database Dialog Box 5
Figure 3: Restore Plan Dialog Box 6
Figure 4: Mockup of Regularly Scheduled Downtimes 12
Figure 5: Scheduled Downtime Notification Process 14
Figure 6: POLARIS Tool on the VA Intranet 15
Figure 7: User-facing Banner on the CV Login Page 20
Figure 8: Data Retrieval from VA Systems 22
Figure 9: PPMS DWS Retrieval 23
Figure 10: System Status Check Sequence 25
Figure 11: Connection Status Details 26
Figure 12: Patching Process for CV Components 28
Figure 13: Scheduled Downtime and Unscheduled Outage Overview 29
Figure 14: Outage Event Activities and Timeline 31
Figure 15: Session Timeout Notification 33
Figure 16: Session Timeout 33
Figure 17: Connection Error 34
Figure 18: jMeadows Log Output 35
Figure 19: CV Architecture and Components 37
Figure 20: Audit Log 39

Table of Tables

Table 1: Virtual Machine (VM) Hardware Specifications 1
Table 2: Access Control Design 9
Table 3: CV Scheduled Downtime Notification List (VA Stakeholders) 10
Table 4: Announcement Banner Content for Maintenance Events Impacting End Users 19
Table 5: Database Table Entry Prior to Manual Removal 20
Table 6: Database Table Entry After Manual Removal 20
Table 7: Database Table Entry for a Planned Maintenance Announcement Banner 21
Table 8: Database Table Entry, as Initially Posted 21
Table 9: Database Table Entry, After a Date Extension Update 21
Table 10: Services Monitored by QoS 24
Table 11: Response Time Log Location 35
Table 12: User Authentication Sequence Overview 40
Table 13: CV External Dependent Systems 41
Table 14: Operations and Maintenance Responsibility Matrix 42
Table 15: Acronyms and Abbreviations 46

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 authorized non-VA providers, known as Community Care Providers (CCPs) or Provider Profile Management System (PPMS) providers. 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 Staff (VAS) assign patients to CCPs and Risk Management (RM) users, allowing them access to view consolidated patient data from multiple Veterans Information Systems and Technology Architecture (VistA) systems.

2. Routine Operations

Routine operations are performed by System Administrators to ensure the upkeep, configuration, and reliable operation of computer systems. System Administrators also ensure that the uptime, performance, resources, and security of the systems meet the needs of the end users.

2.1. Administrative Procedures

The current Production environment is held at the Austin Information Technology Center (AITC). A detailed list of the servers referenced throughout the system startup procedures can be found in the International Business Machines Corporation (IBM) Rational Source Control Repository.[1] Table 1 lists server counts and configurations.

Table 1: 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
jMeadows Quality of Service (QoS) Servers	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	4 Servers
CV DB Servers	MS Windows Server 2012 R2 Standard	4 CPUs, 16 GB RAM	Virtual	2 Servers

[1] **NOTE:** Access to IBM Rational is restricted and must be requested.

2.1.1. System Startup

The start of the CV database (DB) servers is performed by Team AbleVets Operations.

> **NOTE:** The following procedures apply to both the VA Staff and CCP modules of CV.

1. Start the CV DB servers in AITC
   a. The DB server processes are configured to run as system services and are automatically started with the DB servers
   b. Validation
      i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the DB servers are up and operational
      ii. The Operations team logs in to each DB server to validate that the Microsoft (MS) Structured Query Language (SQL) Server service has started; if the service has started, it signifies that the DB servers are up and operational
      iii. The Operations team logs in to each DB server, opens SQL Server Management Studio (SSMS) and connects to the DB; the connection is successful if the DB servers are up and operational
2. Start the VistA Data Service (VDS) servers in AITC
   a. The service processes are configured to run as system services and are automatically started with the VDS servers
   b. Validation
      i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the servers are up and operational
      ii. If startup is unsuccessful, the Operations team investigates the server log files and determines the correct resolution, possibly server reboots
3. Start the jMeadows servers in AITC
   a. The service processes are configured to run as system services, which are automatically started with the servers
   b. Validation
      i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the servers are up and operational
      ii. If startup is unsuccessful, the Operations team investigates the server log files and determines the correct resolution, possibly server reboots
4. Start the CV web application servers (cloud)
   a. The service processes are configured to run as system services and are automatically started with the application servers
   b. Validation

i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the servers are up and operational (Detailed information can be found in the *Installation Verification Procedures* section of the *CV 3.2 Deployment, Installation, Backout and Rollback Guide [DIBR]*. Once approved, all project documentation is available on the Project Joint Legacy Viewer (JLV)/CV SharePoint site[2].)

ii. If startup is unsuccessful, the Operations team investigates the server log files and determines the correct resolution, possibly server reboots

5. Infrastructure Operations (IO) personnel start the CV web application servers for CCPs in AITC non-cloud environment
   a. The service processes are configured to run as system services and are automatically started with the servers
   b. Validation
      i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the DB is up and operational (Detailed information can be found in *Section 4.9* of the *CV 3.2 DIBR*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See 4.b.i, immediately above, for the repository link.
      ii. If startup is unsuccessful, IO investigates the server log files and determines the correct resolution, possibly server reboots
6. Log in with a VA Staff user test account:
   a. Use a Personal Identity Verification (PIV) card and Personal Identification Number (PIN), when prompted
      i. Community Viewer is compatible with PIV cards manufactured by USAccess
   b. Verify that the CV Login page for VA Staff displays as expected and that the system status indicates services are online and connected
   c. Enter Access/Verify codes
   d. Verify VA Staff Portal loads

NOTE: The CV Operations and Engineering teams run a script to ensure that all systems are operational. In addition, opening the Uniform Resource Locator (URL) for CV ensures that all CV context roots are successfully reached.

7. Log in to the CV web application with a CCP test username and password:
   a. Verify that the CV Login page for CCPs displays as expected and indicates that the system status indicates that services are online and connected
   b. Enter username (National Provider Identifier [NPI] or e-mail address) and password
   c. Verify Provider Portal loads

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

2.1.1.1. System Startup from Emergency Shutdown

If there is a power outage or other abrupt termination of the server operating systems, start up the servers as detailed in System Startup and allow the operating system to check the disks for corruption. Consult with IO to ensure that the DB successfully recovers.

2.1.2. System Shutdown

Shutdown procedures are performed during a published maintenance window, when there are few users accessing the system, to avoid impacting transactions in progress. Table 1 lists the AITC servers. A diagram of the CV Production environment can be found in the *CV 3.2 DIBR (Figure 1)*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See System Startup for the link to the repository.

1. Shut down the WebLogic services on the CV web application servers in AITC
2. Shut down the CV web application servers in AITC (cloud)
3. Shut down the CV web application servers in AITC (non-cloud)
4. Shut down the WebLogic services on the jMeadows servers in AITC
5. Shut down the jMeadows servers in AITC
6. Shut down the WebLogic services on the VDS servers in AITC
7. Shut down the VDS servers in AITC
8. Shut down the CV DB servers in AITC

2.1.2.1. Emergency System Shutdown

The emergency system shutdown procedure is to shut down all servers (CV web applications in both cloud and non-cloud environments, jMeadows, VDS, and the CV DB) in AITC, in any order.

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See Administrative Procedures for the link to the repository.

2.1.3. Backup and Restore

This section provides a high-level description of the backup and restore strategy, including all components that require backup and the devices or infrastructure that perform the backup and restore procedures.

IO manages the platform and installation of both the operating systems and the baseline installation of the MS SQL Server in the VA Production environment.

2.1.3.1. Backup Procedures

Backups of the CV DB are configured to run, automatically, at midnight daily. The DB servers are backed up at the IO data center by the AITC Systems Administrators using IO's backup solution. The DB servers also have a MS SQL DB maintenance that automatically backs up each DB to the following location on each server:

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See Administrative Procedures for the link to the repository.

- D:\DBBackups
- D:\DBBackups\TransactionLogs

2.1.3.2. Restore Procedures

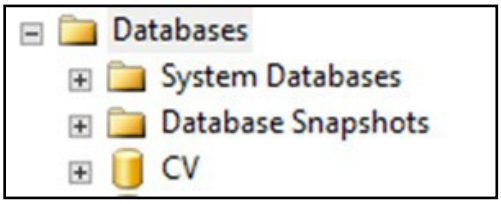
The items necessary for the recovery of the DBs are:

- DB backup (.bak) file for the CV DB
- Encryption keys for the DB

Restore a full DB backup:

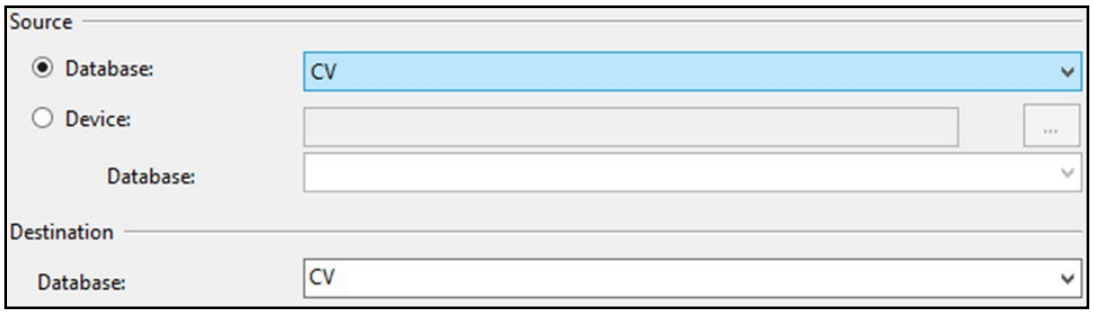
1. Connect to the appropriate instance of the MS SQL Server DB Engine in SSMS
2. Click the server name to expand the server tree
3. Right-click **Databases**

Figure 1: Database Names Tree



4. Click **Restore Database**
5. Use the **Source** section on the **General** page to specify the source and location of the backup sets to restore; select the following options:
   a. Click the **Browse** (...) button to open the **Select Backup Devices** dialog box
   b. Select **File** in the Backup Media Type box, then click **Add**
   c. Navigate to the location of the backup file (.bak) of the CV DB, then click **OK**
   d. After you add the devices you want to the **Backup Media Type** box, click **OK** to return to the **General** page
   e. Select the name of the DB to be restored (CV) in the **Source Device: DB List** box

Figure 2: Source/Device/Database Dialog Box



6. The **Database** box in the **Destination** section automatically populates with the name of the DB to be restored
   a. Select CV from the dropdown
7. Leave the default in the **Restore To** box as the last backup taken, or click **Timeline** to access the **Backup Timeline** dialog box to manually select a point in time to stop the recovery action
8. Select the backups to restore in the **Backup Sets to Restore** grid
   a. This grid displays the backups available for the specified location
   b. By default, a recovery plan is suggested; to override the suggested recovery plan, change the selections in the grid

Figure 3: Restore Plan Dialog Box

Restore plan

Backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position
☑	CV_backup_2018_12_13_000002_1596274	Database	Full	VAAUSGTDSQL200	CV	1

   c. Backups dependent upon the restoration of an earlier backup are automatically deselected when the earlier backup is deselected

> **NOTE:** Default options are not selected if an attribute necessary for restoration is not contained within the default backup.

9. Alternatively, click **Files** in the **Select a Page** pane to access the **Files** dialog box
   a. Restore the DB to a new location by specifying a new restore destination for each file in the **Restore the database files as** grid

2.1.3.3. Backup Testing

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See Administrative Procedures for the link to the repository.

1. Servers
   a. Backups of the VMs are done at the VA data center by AITC Systems Administrators
   b. Backups are performed daily
   c. Testing of the backups is performed by IO
   d. Validation of restorations are confirmed by:
      i. Validating that all software/configurations are restored from the expected configuration
      ii. Confirming that the configuration files contain server-specific settings
      iii. Validating that the application server starts as expected through logs and a smoke test of the application
2. DB

a. Backups are performed at midnight daily
b. Backups are periodically restored, on an ad hoc basis, to the backup DB servers to test the restore procedures and the integrity of the backup files
c. AITC System Administrators validate that data in the DB contains up-to-date entries for the user profiles and audit logging
d. Validation of operations is confirmed through a smoke test of the application

2.1.3.4. Storage and Rotation

IO manages the platform and any storage and rotation scheduling in the CV Production environment. IO ensures the system and storage arrays are operating properly, with daily inspections of CV QoS logs and system notifications.

Team AbleVets is responsible for ensuring that the partition structure in use is sufficient, which, in turn, ensures there is enough storage space.

2.2. Security/Identification (ID) Management

Access to CV is restricted to authorized VistA users within, and authorized providers outside of, the VA. Authorized VistA users are referred to as VA Staff. Authorized providers outside of the VA are referred to as CCPs (or PPMS providers). CV utilizes HTTP Strict Transport Security (HSTS) which is a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking.

Three tables within the CV DB are used for ID management; the PPMS_Provider table, the C_Provider table, and the VAS_UserRole table:

- The PPMS_Provider table within the CV DB lists CCPs' first names, last names, e-mail address, and their associated NPI numbers
- The C_Provider table within the CV DB lists CCPs' and RM users' first names, last names, and their associated e-mail addresses
- The VAS_UserRole table within the CV DB assigns roles to VA Staff users specific to their function (e.g., Tier 1 VA Staff, Tier 2 VA Staff, Risk Management Provider Manager [RMPM], or Service Desk User [SDU]) and stores their associated PIV information

The CV Login page guides VA Staff users through the login process, including, where necessary, fields to enter specific credentials. The CV Login page fields request the VA Staff user's Access/Verify Codes, Agency, and Site. VA Staff users must have their PIV card in place before entering the CV URL into the address bar of a supported browser.

SDUs must have their PIV card in place before entering the CV URL into the address bar of a supported browser. SDUs log in with their PIV card and PIN but are not required to have or use Access/Verify codes.

CCPs can use either the e-mail address associated with their account or their NPI, and a password to log in. CV queries PPMS during login to see if a provider has an NPI listed within PPMS. If they do, they are considered "active." If there is no NPI listed for a provider, they are not considered active, and will be unable to log in to CV.

NOTE: The *username* field of the CV Login page has been made a free text field to accommodate either an e-mail address or NPI entry.

A detailed overview of the login process, from the user's perspective, can be found in the *CV 3.2 VA Staff User Guide* and the *CV 3.2 Community Care Provider (CCP) User Guide*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See System Startup for the link to the repository.

2.2.1. Identity Management

Any VA user with VistA credentials can access either the Community Care PPMS Provider Management widget or the Risk Management Provider Management widget on the CV VA Staff portal page, depending on their role.

CCP user accounts are created by VA Staff or the Community Provider Technical Service Desk. Detailed instructions for creating CCP user accounts are found in the *CV 3.2 VA Staff User Guide*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See System Startup for the link to the repository.

2.2.2. Access Control

CV access control for CCPs consists of the validation of user credentials, retrieved from the Login page, against the CV DB. When the user's credentials are found in the PPMS_Provider table of the CV DB, the user is granted access to CV. CCPs may encounter a login error message if they attempt to access CV when their status is not set to *active* in PPMS: *There is an issue preventing your access to Community Viewer. Please contact your VA Contractor or VA Medical Center for assistance*.

VA Staff control CCP access to patient records by making assignments for a specified date range. A CCP can access only the records of the patient with whom they have an assigned consultation for the time period set by VA Staff.

SDUs must be added to the VAS_UserRole table as authorized users. Once authorized, they use their PIV card and PIN to gain access to the application.

VA Staff use their PIV card, PIN, and VistA credentials to access either the Community Care PPMS Provider Management widget or the Risk Management Provider Management widget on the VA Staff portal page, depending on their role.

Table 2 summarizes the CV system components and the settings utilized for access control.

Table 2: Access Control Design

Component	Description
DB	The PPMS_Provider table within the DB contains NPI values used as usernames for CCPs. The C_Provider table within the DB contains e-mail addresses used as usernames for CCPs and RM users. System design specifications and diagrams can be found in the CV Design, Engineering, and Architecture (DE&A) Compliance Requirements collection in the Rational Tool Suite [3].
DB script	A DB script is used to deliver changes or updates to the pertinent tables within the CV DB.
Configuration settings	A configuration setting within the appconfig-production.properties file that enables access control. • *Enable VA Access Control, On/Off:* This setting enables access control for VA Staff.
VAS_UserRole table	The VAS_UserRole table is the authorized user table for SDUs. Once added to the table, SDUs can gain access to CV.

2.3. User Notifications

CV is comprised of hardware and software, interfaces to the dependent partner systems such as PPMS and the Master Veteran Index (MVI), as well as other infrastructure necessary to deliver the CV application. Each of the individual components may undergo scheduled downtime for maintenance on a periodic basis. CV Support follows a notification process to alert VA stakeholders of pending downtime in advance of each known event.

NOTE: The Veterans Health Administration (VHA) CV team is responsible for crafting and approving outage notification messages before they are posted for end users.

Notifications are sent via e-mail to VA Stakeholders when there are scheduled or unscheduled changes in system state, including but not limited to: planned us, system upgrades, maintenance work, and any unexpected system outages. The Veterans Health Administration (VHA) CV team is responsible for crafting and approving outage notification messages before they are posted to the Announcements section of the CV Login page and banners within the application.

Notifications for planned outages are initiated 24 hours in advance of anticipated system downtime, and notification of an unscheduled outage occurs if an error does not clear within 15 minutes. The notification process for unscheduled outages is as follows:

1. The CV Support team monitors and evaluates all system issues
2. The QoS service alerts are e-mailed to the CV Support team and a defined list of contacts when a service disruption occurs
3. The CV Support team notifies Tier 2 Support of the Enterprise Service Desk (ESD) about any outage, and reports the same to VA users via e-mail, with an ESD ticket number, and the date and time of the outage

[3] **NOTE:** Access to IBM Rational is restricted and must be requested.

2.3.1. User Notification Points of Contact

Table 3 details the current notification list for alerting VA stakeholders of scheduled CV downtime. This list is maintained by Team AbleVets.

Table 3: CV Scheduled Downtime Notification List (VA Stakeholders)

Name	Organization	Email Address
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	AbleVets	REDACTED
REDACTED	AbleVets	REDACTED
REDACTED	AbleVets	REDACTED
REDACTED	AbleVets	REDACTED
REDACTED	HRG	REDACTED
REDACTED	HRG	REDACTED
REDACTED	HRG	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	RavenTek	REDACTED
REDACTED	Seawolf	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED

2.3.2. CV QoS Mail Groups

VA:

- REDACTED

Team AbleVets

- REDACTED
-

2.3.3. Scheduled Downtime Notifications

CV Support monitors the maintenance schedules of systems that provide notification of planned outages, then communicates the upcoming downtime to VA stakeholders.

> **NOTE:** CV Support depends on the receipt of timely information from dependent systems and infrastructure. Not all systems and/or infrastructure teams provide downtime notices to CV Support.

Figure 4 shows a typical calendar of regularly scheduled downtimes for CV and external systems. For a complete list of planned downtimes, refer to the detailed list following the calendar mockup.

Figure 4: Mockup of Regularly Scheduled Downtimes

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17 Linux	18	19	20 Windows
21	22	23	24	25	26	27
28	29	30	31			

Downtimes

Linux — 3rd week of each month, Wednesday @9 pm to 11 pm EDT Linux (ITOPS)

Windows — 3rd week, Sunday, Windows updates 8 am to 10 am EDT (ITOPS)

The following list details the downtime notices currently known to CV Support.

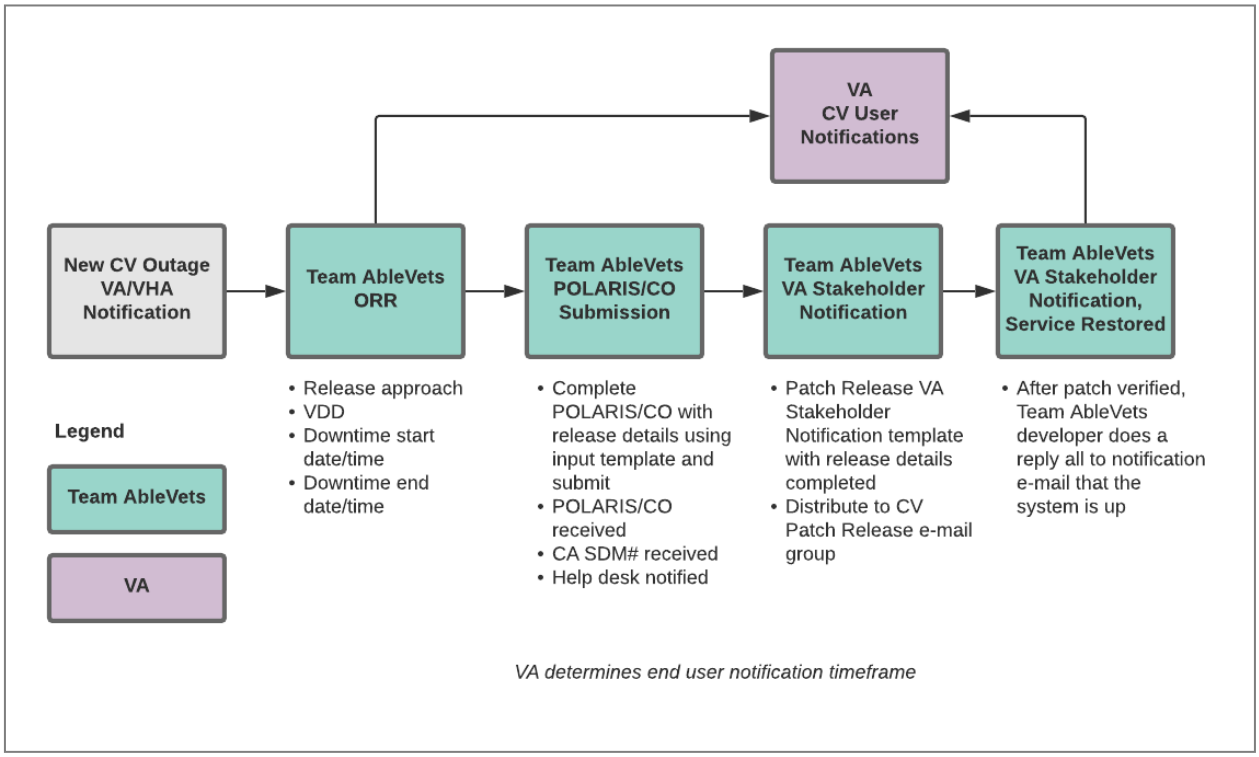
- **IO (AITC)**
  - Organization: VA
  - Frequency: Monthly, the 3rd week
    - 3rd Sunday of each month, Windows updates
    - 3rd Wednesday of each month, Linux updates
  - Time Frame: Sundays from 8:00 am to 10:00 am EST; Wednesdays from 9:00 pm to 11:00 pm EST
  - Email Subject: Monthly Security Patching
  - POC: REDACTED
- **VA Authentication Federation Infrastructure (VAAFI)**
  - Organization: VA
  - Frequency: As needed
  - Time Frame: Varies
  - Email Subject: VAAFI Datacenter flip Miami to Culpeper
  - POC: REDACTED
- **MVI**
  - Organization: VA
  - Frequency: As needed
  - Time Frame: Varies, typically the 3rd weekend and from 3:00 pm to 9:00 pm
  - Email Subject: VAAFI Data center flip Miami to Culpeper
  - POC: REDACTED

CV Support actively monitors all relevant system maintenance schedules and follows the planned downtime notification process for CV application code-driven patch releases (see Figure 5).

1. CV Support notifies VA stakeholders when CV is restored to service
2. The VHA CV team crafts and approves messages to notify CV users of estimated system downtime when CV is unavailable and when the system is restored

> **NOTE:** The process flow (shown in Figure 5) is designed primarily for *CV application code-driven patch releases*. It is also used as a guide for scheduled downtime notifications; however, not all steps may apply to downtimes triggered by scheduled maintenance/outages on external components that are outside the control of CV Support.

Figure 5: Scheduled Downtime Notification Process



While all CV scheduled downtime communications follow a similar format, each is tailored to the specific activity and system/service affected.

2.3.3.1. Planning and Online Activity/Release Integration Scheduler (POLARIS) Process

POLARIS (Figure 6) is a web-based tool, available on the VA Intranet, that is used to create notifications for scheduled system downtime events.

Figure 6: POLARIS Tool on the VA Intranet

Event ID: 24616	Title: CV (GTD) Patching - AITC	
Point of Contact Information		
Project Manager POC:	**Implementation Manager POC:**	**Post-Validation Tester POC:**
Name: Reed, Colleen	**Name:** Lukens, Richard K. (AbleVets)	**Name:** Stanton, Troy A. (AbleVets)
Phone number: (703) 402-8604	**Phone number:** 703-407-2623	**Phone number:** 703-583-6202
Phone number (alternate):	**Phone number (alternate):**	**Phone number (alternate):** 2
Email: Colleen.Reed@va.gov	**Email:** Richard.Lukens@va.gov	**Email:** troy.stanton@va.gov
Creator: Stanton, Troy A. (AbleVets)	**Created Date:** 10/9/2019	
Release Information		
Summary	CV Monthly Patching Windows Production in AITC on 20 October 2019, starting at 9a Eastern / 8a Central	

The Change Order (CO) notifies the Enterprise Service Desk (ESD) of the planned event. Once the form has been completed and submitted, the ESD responds via e-mail within approximately 15 minutes with the associated ESD ticket number. The CO and ESD ticket numbers are provided in the notification e-mail, as shown in Patch Release Notification E-mail (Example).

2.3.3.2. Patch Release Notification E-mail (Example)

All,

This is to notify you of the upcoming Production release of the CV Enterprise Patch x.x.x.x.x.

- The CO number is **CHGxxxxx**
- The ServiceNow Ticket number is **INCxxxxxxx**
- CV Enterprise Patch version x.x.x.x.x will be released to VA Production environments on <Day>, <Month> <Day>, <Year> starting at <Time 24-hour clock> (Time am/pm) ET. Patching is expected to be completed by <Time 24-hour clock> (Time am/pm) ET, <Day>, <Month> <Day>, <Year>. CV-Enterprise will be unavailable during this time.

2.3.4. Unscheduled Outage Notifications

2.3.4.1. Initial Response to Issues Within 30 Minutes of Alert

The following steps represent the response to a reported issue, to occur within 30 minutes of the initial alert:

1. If a QoS e-mail is received and errors have **not** been cleared within 30 minutes of receipt of the initial error alert, proceed to Step 2
2. Within 30 minutes of the initial error e-mail, CV Support (Table 14) will send an e-mail to the CV stakeholders (Table 3) to inform them that the Support team is investigating the issue
   a. Use the e-mail example below, tailored to the specific activity and the system(s)/service(s) that are affected

2.3.4.1.1. Initial Outage Response Notification E-Mail (Example)

Subject: CV Outage Notification

All,

CV is currently experiencing an error in the <Environment Name> environment.

The error detail is: <Error from QoS>

This error impacts <service impacted> (choose one from list below)

- MVI: the users' ability to retrieve VA records
- VDS: the users' ability for VA users to log in and retrieve VA records
- Database: the ability for the application to check the authorized users list, retrieve a user's profile, generate a site list for the log in, and the ability for CV to log auditing records
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to CV until service is restored.

Please stand by as we further investigate the error. You will be notified by e-mail as soon as the issue is rectified. If the issue persists longer than 90 minutes from now, you will be notified of the error status and resolution progress in another e-mail.

Thank you.

2.3.4.2. Outage Escalation to External Teams

The following information details the escalation process to external teams in the case of an issue caused by a service outside CV Support's purview. A status update is requested within 2 hours of the initial alert.

1. Send an e-mail to the applicable external service group, MVI, PPMS, VA Network Security Operations Center (NSOC), IO, etc., as specified in Table 14
2. Request the status of the issue within 2 hours of the initial alert
   a. Copy CV Support (Table 14)
   b. Use the e-mail example(s) below, tailored to the specific activity and system(s)/service(s) that are affected

2.3.4.2.1. Outage Escalation to External Teams E-Mail (Example)

Subject: CV Service Verification Request

All,

The CV application is currently experiencing an error in the <Environment Name> environment.

The error detail is: <Error from QoS>

This error impacts <service impacted> (choose one from list below)

- MVI: the users' ability to retrieve VA records
- VDS: the users' ability to authenticate and retrieve VA records
- PPMS: the ability for VA Staff to retrieve provider profiles

- VistA Host: the ability for CV to retrieve records for the specified VistA host
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to CV until service is restored.

CV Support would like to verify that <application/service> is up, running, and not experiencing any errors.

Optional: CV Support has verified that network connectivity is not the issue. Please verify and respond to CV Support with your findings.

Thank you for your assistance in troubleshooting this issue.

1. Generate a trouble ticket and assign it to the appropriate application team
2. Send a notification to the CV stakeholders (Table 3) with all pertinent information
   a. Use the e-mail example(s) below, tailored to the specific activity and system(s)/service(s) that are affected

2.3.4.2.2. Outage Update E-Mail (Example)

Subject: CV Outage Update

All,

The CV application is currently experiencing an error in the <Environment Name> environment.

The error detail is: <Error from QoS>

- MVI: the users' ability to retrieve VA records
- VDS: the users' ability to authenticate and retrieve VA records
- PPMS: the ability for VA Staff to retrieve provider profiles
- VistA Host: the ability for CV to retrieve records for the specified VistA host
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to CV until service is restored

The CV Engineering team has determined the following:

- Severity: Severity Level ONE
- Impact: <List impacted users, and state which services are impacted, and the functionality lost>
- Fault is isolated to: <Where the error resides (local CV servers, local CV database, network (provide details if possible) or external application>
- Estimated Time of Service Restoration: <Estimated time frame of restoration>
- CO Number: <CO number, only if applicable and approved by VA CV PM or VHA CV Team>
- Ticket Number: <Ticket number submitted to the VA service desk, only if the issue is with the network or an external application>

The CV Engineering team will continue to monitor and troubleshoot the issue. Updates will be provided every 2 hours until the issue is resolved.

Thank you.

1. Continue monitoring the issue
2. Provide updates every **2 hours** to the CV stakeholders (Table 3) until issue is resolved:
   a. AbleVets Emergency Contact: REDACTED
   b. AbleVets Alternate Contact: REDACTED
   c. AbleVets Alternate Contact: REDACTED
   d. HRG Emergency Contact: REDACTED
   e. HRG Alternate Contact: REDACTED
   f. CV Support Hours: 24x7x365

2.3.5. Announcement Banners

Announcement banners are provided for the end users' benefit and information. They appear in the Announcements section of the CV Login page, and within the CV application in the form of banners.

The primary goal of announcement banners is to inform end users of important information about their use of CV. The use of acronyms and IT jargon within announcement banners is minimized to clearly communicate any temporary limitations of CV.

It is important to note that the system maintenance notices shared among technical groups are different from the application-level announcement banners as they are not appropriate for end users.

Announcement banners are posted no more than 24 hours prior to a planned event and removed immediately upon completion of the planned event.

Announcement banners for an unplanned outage are posted immediately after the confirmation of the outage and are removed immediately upon resolution of the outage.

The following announcement banners are prioritized:

1. Patient Safety
2. Newly discovered defects/issues with broad impact
3. Unplanned outages or unexpected loss of data lasting more than 2 hours that are not already communicated by System Status notifications
4. Planned maintenance/outages with expected impacts or disruptions
   a. Maintenance events no or inconsequential impact should not be posted

End users can become desensitized to the important information in announcement banners when too many alerts are posted too often. The plan to minimize alert fatigue is as follows:

1. Display announcement banners by severity
   a. Add a prefix category (Patient Safety, Issue, Outage, Maintenance, etc.) to announcement banner titles and content to further differentiate context and priority
2. Post only those alerts that impact end users
   a. Informational announcement banners for maintenance events where there is no expected or an inconsequential impact should not be posted

3. Set an expiration date for announcement banners, and remove them as soon as possible after the event has completed or the issue has been corrected

The following groups have the authority to enable certain types of announcement banners:

- CV Support: Maintenance-related notifications that impact end users
- CV Business Team: Notifications regarding patient safety and other critical issues that impact end users

Table 4 lists the announcement banner content for maintenance events with expected user impact and for special events and issues.

Table 4: Announcement Banner Content for Maintenance Events Impacting End Users

Maintenance Event Titles (50-character limit)	"More" Hyperlink Expanded Content (255-character limit)
MAINTENANCE VA Patient Identity System -5/17 **More**	**Maintenance window:** 05/17/18 9pm ET -05/18/18 12pm ET **Impact:** Users may experience problems with patient search.
MAINTENANCE Community Partner System- 6/29 **More**	**Maintenance window:** 06/29/18 8pm ET - 06/29/18 11 pm ET **Impact:** CV will be available for use, but Documents widget may not retrieve records. If you experience this problem, please try again later.
PATIENT SAFETY Contrast Allergies **More**	CV is currently not displaying VA allergies for Contrast media entered through the Radiology option "Update Patient Record" [RA PTEDIT].
ISSUE Imaging not available **More**	VA images are not currently being displayed in CV. The issue is being analyzed and a patch to resolve the issue will be deployed as soon as possible.
OUTAGE Community Partner Records **More**	VA is currently unable to retrieve records from community partners (VLER/VHIE partners). Engineers are working to restore connections as quickly as possible. (add details on anticipated resolution, etc. if available).

2.3.5.1. Placing Announcement Banners

When there is a major system outage, service degradation or patient safety issue, an announcement banner will be placed on the Login page for the affected environment at the T+60-time frame. The announcement banner placement in any environment is accomplished via the database associated with that environment.

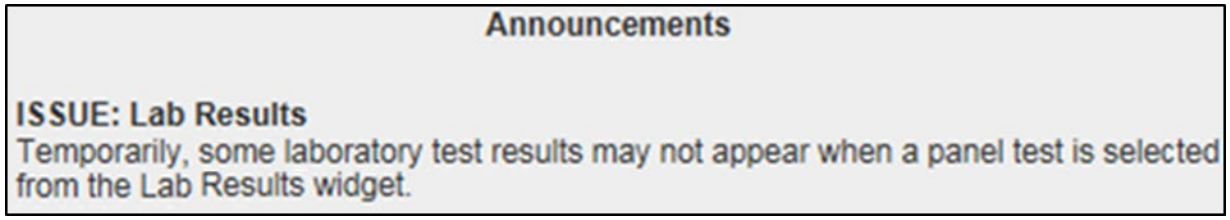
NOTE: Current functionality does not allow for a specific time frame, like 2:00 pm to 8:00 pm, to be provided. At present, the system only allows for an expiration date, formatted as Month/Day/Year.

An example of the script used to place an announcement banner is as follows:

```
execute dbo.createNotification
        @startDate='10/17/2018'
       ,@endDate='10/30/2018'
       ,@announcement=Lab Results'
       ,@userGroup='ALL'
       ,@description=Temporarily, some laboratory test results may not appear when a
panel test is selected from the Lab Results widget.'
```

The resulting announcement banner, as viewed on the application Login page, is shown in Figure 7.

Figure 7: User-facing Banner on the CV Login Page



2.3.5.2. Removing Announcement Banners

There are two methods used to remove a banner from the application Login page: manual and automatic expiration.

2.3.5.2.1. Manual Removal

The manual removal method is used when a system degradation has been resolved or the planned outage has been completed prior to the designated end date.

Manual removal is accomplished by accessing the database tables and manually changing the end date to match the start date associated with the announcement banner to be removed. Database entries demonstrating the announcement banner prior to (Table 5) and after (Table 6) manual removal follow.

Table 5: Database Table Entry Prior to Manual Removal

Start Date	End Date	Title	Announcement Banner Text
2018-10-17	2018-10-30	ISSUE: Lab Results	Temporarily, some laboratory test results may not appear when a panel test is selected from the Lab Results widget. If you encounter this problem, please refer to VistAWeb for the results.

Table 6: Database Table Entry After Manual Removal

Start Date	End Date	Title	Announcement Banner Text
2018-10-17	2018-10-17	ISSUE: Lab Results	Temporarily, some laboratory test results may not appear when a panel test is selected from the Lab Results widget.

2.3.5.2.2. Automatic Expiration

Automatic expiration of an announcement banner occurs when the designated end date of the announcement banner has been reached. Expiration dates are set based on when the issue can be resolved by an authorized member of CV Support. A database entry demonstrating a planned maintenance announcement banner as shown in Table 7.

Table 7: Database Table Entry for a Planned Maintenance Announcement Banner

Start Date	End Date	Title	Announcement Banner Text
2018-10-26	2018-10-27	ISSUE: System performance upgrades	System may temporarily be down for system performance upgrades between 8pm EST 26 October 2018 - 12am EST 27 October 2018.

2.3.5.2.3. Announcement Banner Extensions

If a service degradation or other event will exceed the planned end date of an existing announcement banner, CV Support can manually extend the duration of the announcement banner by changing the end date to a date in the future. Database entries demonstrating the announcement banner prior to (Table 8) and after (Table 9) a date extension.

Table 8: Database Table Entry, as Initially Posted

Start Date	End Date	Title	Announcement Banner Text
2018-10-26	2018-10-27	ISSUE: System performance upgrades	System may temporarily be down for system performance upgrades between 8pm EST-26 October 2018 – 12am EST 27 October 2018.

Table 9: Database Table Entry, After a Date Extension Update

Start Date	End Date	Title	Announcement Banner Text
2018-10-26	2018-10-29	ISSUE: System performance upgrades	System may temporarily be down for system performance upgrades between 8pm EST-26 October 2018 – 12am EST 29 October 2018.

2.4. System Monitoring, Reporting, and Tools

CV traces and audits actions that a user executes within the application. CV audits are provided through audit trails and audit logs that offer a backend view of system use, in addition to storing user views of patient data. Audit trails and logs record key activities (date and time of the event, patient identifiers, user identifiers, type of action, and access location) to show system threads of access and the views of patient records. Refer to Application Error Logs for more information about audit and server logs.

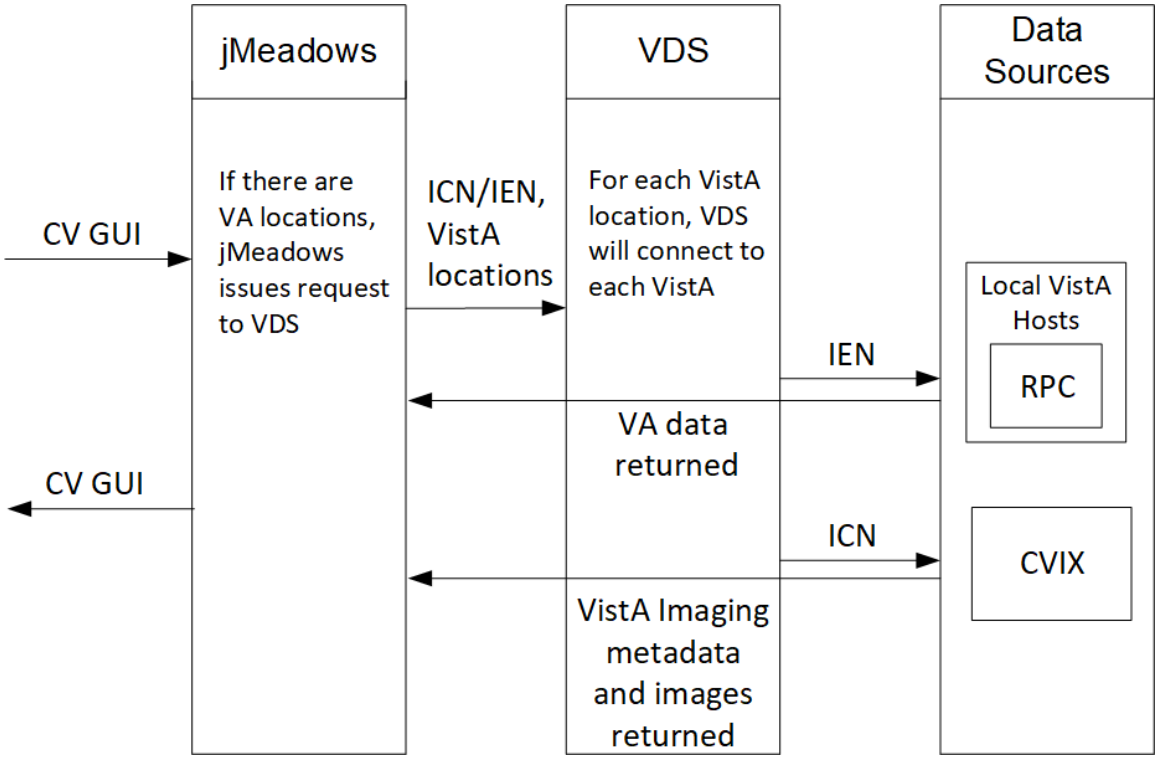
The CV QoS service monitors the availability of data sources. Refer to Availability Monitoring for more information.

2.4.1. Dataflow Diagram

The data retrieval sequence, depicted in Figure 8, occurs after a patient is selected:

1. jMeadows issues a request to VDS with the VA Integration Control Number (ICN)/Internal Entry Number (IEN) and VistA location for each VA location in the patient record; the ICN and VistA location information is received from the Master Veteran Index (MVI)
2. VDS connects to each VistA and returns the clinical data to jMeadows for each VistA location, detailed in VistA Imaging (VI) Data Retrieval
3. jMeadows aggregates the data and returns the data to the CV application

Figure 8: Data Retrieval from VA Systems



2.4.2. VistA Imaging (VI) Data Retrieval

CV utilizes the Central VistA Imaging Exchange (CVIX) Viewer Service Application Programming Interface (API) to retrieve and display nondiagnostic quality Joint Photographic Experts Group (JPEG) images and Portable Document Formats (PDFs). Images and/or PDFs are displayed in the Radiology Exams, Encounters, and Progress Notes widgets. Some progress notes that have images associated with them appear in the Pain Management widget.

The retrieval and display sequence involve three requests to CVIX.

1. A Station 200 service account is created for CV to communicate with the VI services
   a. When the user logs in to CV, a Broker Security Enhancement (BSE) token is retrieved for the service account to enable communication with the CVIX Viewer Study Query service
   b. The service account credentials and site information are used for the basic authentication when communicating with the VI Study and VI Image services
2. When the user clicks the camera icon, CV first makes a Study Query request to CVIX

3. jMeadowsCCP constructs the contextID needed by the CVIX API
   a. The accepted file types are identified in the VDS code
      i. **Example:** contentType=image/JPEG 2000 (j2k),image/jpeg.application/pdf
   b. The J2K file types are converted to JPEG format using GraphicsMagick
4. CV then makes a request to retrieve the study details
5. When the two requests to CVIX are complete, CV displays the list of study groups and images in a dialog
6. When the user clicks a study's image link, CV initiates a third request to CVIX for the image data
7. The image data is returned, and CV displays the image in a new browser tab
   a. The image quality is set in the CV CCP configuration file
      i. **Example:** grails.vixImageQuality=90

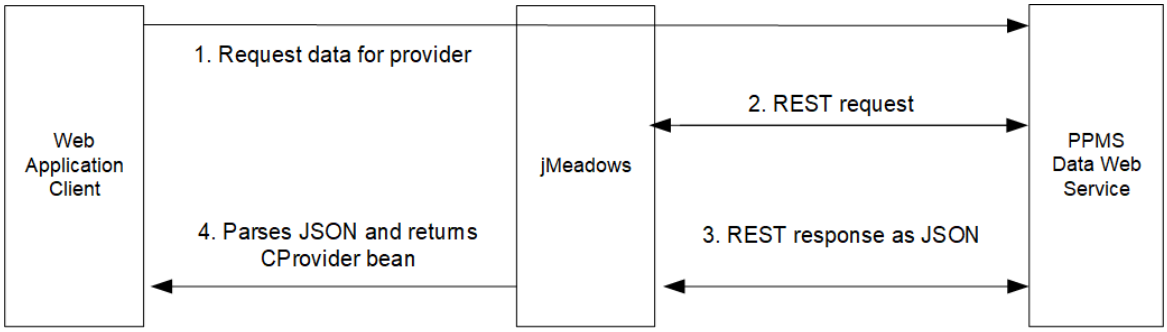
NOTE: If the image is not in JPEG or PDF format the error message, *"The current image is not a supported file type and cannot be displayed."* appears.

2.4.3. PPMS Data Web Service (DWS) Retrieval

The PPMS data retrieval sequence is depicted in Figure 9.

1. CV requests data for a provider from the jMeadows SOAP service
2. The jMeadows SOAP service layer makes the corresponding REST request and sends the security token to PPMS
3. PPMS returns a REST response as JSON to jMeadows
4. jMeadowsVAS parses the JSON and returns a CProvider bean
5. The CProvider bean is communicated back to the Graphical User Interface (GUI), which returns the response to the Manage PPMS Providers screen

Figure 9: PPMS DWS Retrieval



For detailed information, see the *PPMS Data Service Interface Control Document (ICD)*. The ICD can be found in Rational Source Control [4]. See Administrative Procedures for the link to the repository.

2.4.4. Availability Monitoring

The QoS monitors the health of the CV application and checks for the availability or disruption of dependent services within the systems in VA environments (Table 10).

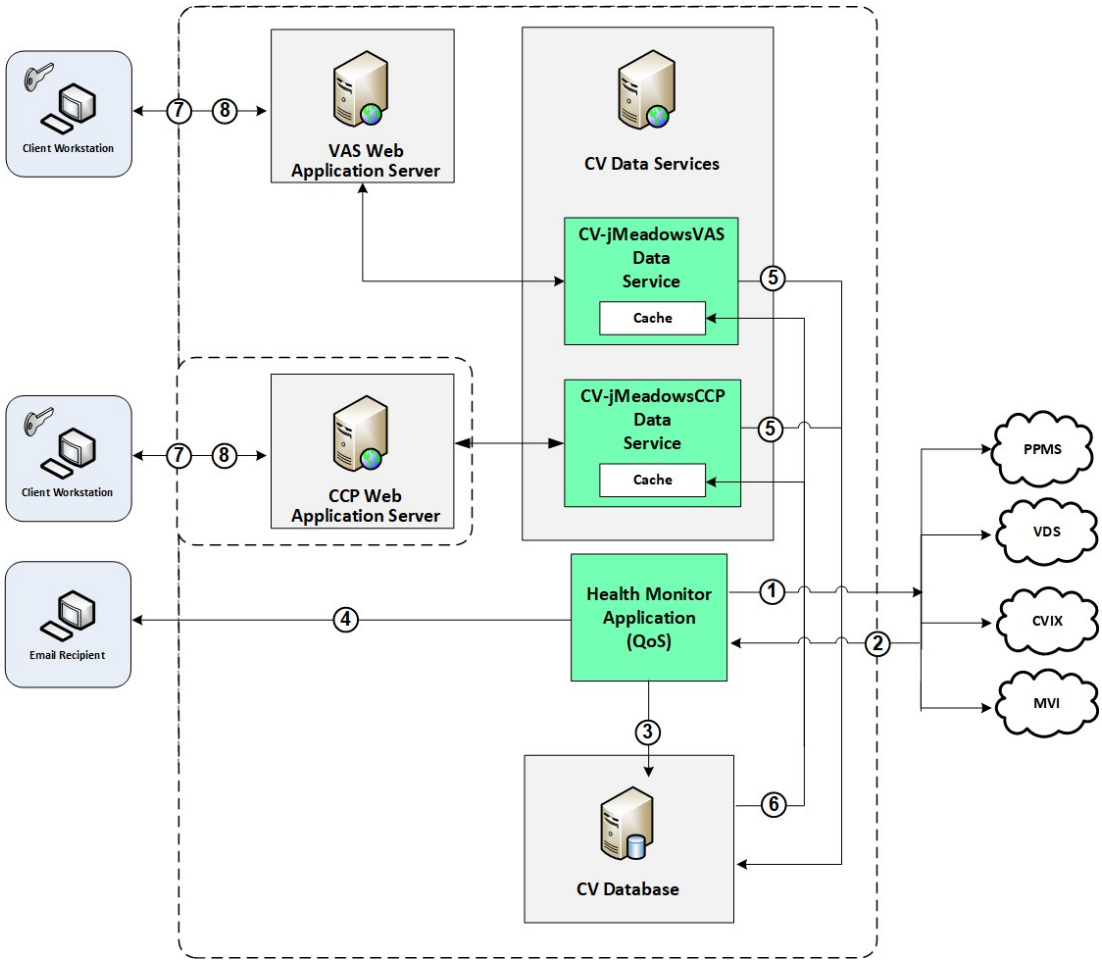
Table 10: Services Monitored by QoS

Service	Description
MVI (VA)	Retrieves VA patient ID
CV Database (DB) Server	Contains CV database information
jMeadows Data Service	Connects to MVI/DB/VDS
Veterans Information Systems and Technology Architecture (VistA) Data Service (VDS)	VA Log in/Data
PPMS	Retrieves CCP profile information

System status is displayed on the Login page and in the application when there is a degradation. System status events are logged to the CV DB, and users are notified of system status via the Login page.

[4] **NOTE**: Access to IBM Rational is restricted and must be requested.

Figure 10: System Status Check Sequence



System status checks (Figure 10) are performed as follows:

1. The Health Monitor pings the monitored services every 5 minutes
2. The Health Monitor receives a system status from each monitored service and reports the status of CV systems to CV Support via e-mail
3. System status events are written to the QOS_LOGS table, within the CV DB
4. The Health Monitor sends an automated e-mail notification every 6 hours, unless a status change is detected
   a. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset
   b. The next e-mail is generated after 6 hours, if no further system status changes are detected
   c. When all errors are cleared, an e-mail is sent stating that no errors are detected
5. The CV-jMeadowsVAS and CV-jMeadowsCCP Data Services ping the CV DB every 2 minutes for status checks

6. The CV-jMeadowsVAS and CV-jMeadowsCCP Data Services store the data returned from the CV DB in their internal caches, the CV-jMeadowsVAS or CV-jMeadowsCCP Data Services cache, respectively
7. When a user accesses the CV Login page, the CV application requests and receives system status data from either the CV-jMeadowsVAS or CV-jMeadowsCCP Data Service cache
8. Every 5 minutes of an active user session, CCP or VAS application server requests system status data from either the CV-jMeadowsCCP or CV-jMeadowsVAS Data Service cache
   a. Current system status is retrieved from either cache and sent to the CCP or VA Staff GUI

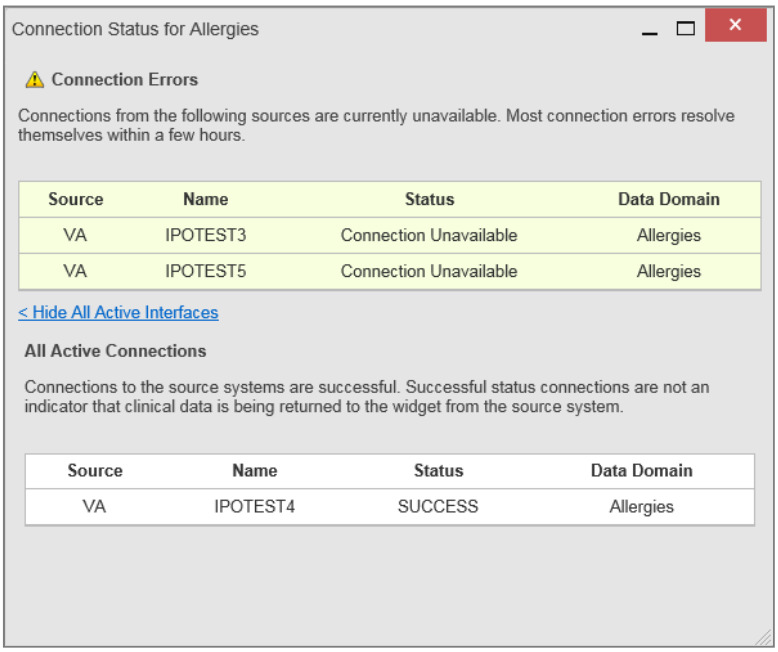
2.4.4.1. Domain-Level Availability Monitoring

CV displays interface status icons on the toolbars of multiple Patient Portal widgets to communicate the status of the data source for the widget's clinical domain. There are two conditions:

- The information icon indicates that all sources are available
- The warning icon indicates one or more data sources are unavailable

Both icons are used to provide status for data sources. Clicking the status icon opens interface status details in a separate window, as shown in Figure 11.

Figure 11: Connection Status Details



2.4.5. Performance/Capacity Monitoring

Query times for each web service call in to jMeadows and VDS are recorded to a file in the /u01/CV_HOME/logs/ directory on the server, where the services are installed. Performance monitoring data is collected by the AITC Monitoring group using the Computer Associates (CA) Application Performance Management (APM) suite.

Refer to Application Error Logs for more information on audit and server logs.

2.4.6. Critical Metrics

The CV Development team adds metric requirement reporting to the product backlog as metrics are defined. Current metrics considered critical are user metrics, core system metrics, user transactions, error logging, QoS metrics (service stability/availability), and other industry-standard system/performance metrics. The metric data is reported in the weekly Operations report and the weekly/monthly usage report.

Examples of the critical metrics listed above, and captured in the Operations and Usage reports, include:

- User Access: CV traces and audits the actions a user executes within the application
- Audit data is provided via audit trails and audit logs that offer a backend view of system use and store user views of patient data
- Interface with jMeadows: jMeadows retains user actions within CV
- Specific events (user transactions) are audited or captured in log files, including but not limited to user ID, date and time of the event, type of event, success or failure of the event, successful login, and the identity of the information system component where the event occurred

Each time an attempt is made to interface with jMeadows, whether it is a service communication or a user searching for a patient, the activity is logged and stored in the CV data store. The purpose of retention is for traceability; specifically, to show which calls/actions were made, where, by whom, and when they terminated. Each CV query for data is audited and has the user ID linked to it.

2.5. Routine Updates, Extracts, and Purges

CV system updates, and other routine actions on systems within the AITC cloud environment, are handled by the CV Support team, as needed.

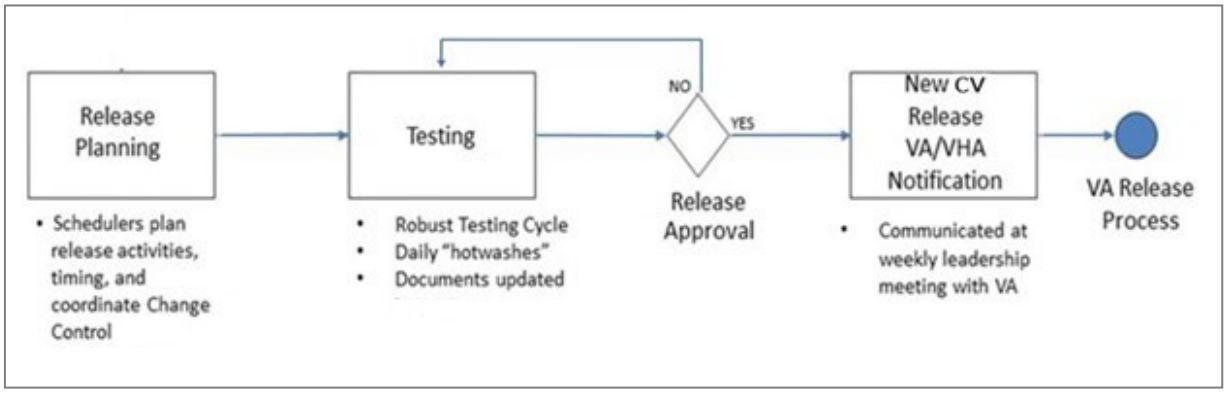
Updates to the CV web application servers within the AITC (non-cloud) environment are performed by AITC personnel.

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See Administrative Procedures for the link to the repository.

2.5.1. Routine Updates

Patches and other routine updates follow the CV patching process, shown in Figure 12.

Figure 12: Patching Process for CV Components



2.5.2. Quarterly Update of the VistA Site List

The CV Support Team monitors the VistA site list for any changes and updates the DB quarterly.

2.5.3. Extracts

Extracts of the CV audit logs and server logs are available by request only, on an as-needed. The VA Project Manager must approve requests for extracts. Approvals are dependent on the type of request and the organization of the requester. Once a request is approved, an authorized System Administrator extracts the requested data and sends it to the requestor, via an encrypted method. Refer to Application Error Logs for more information on audit and server logs.

2.5.4. Purges

Neither data, nor audit log entries from the CV DB, nor other system components, are purged.

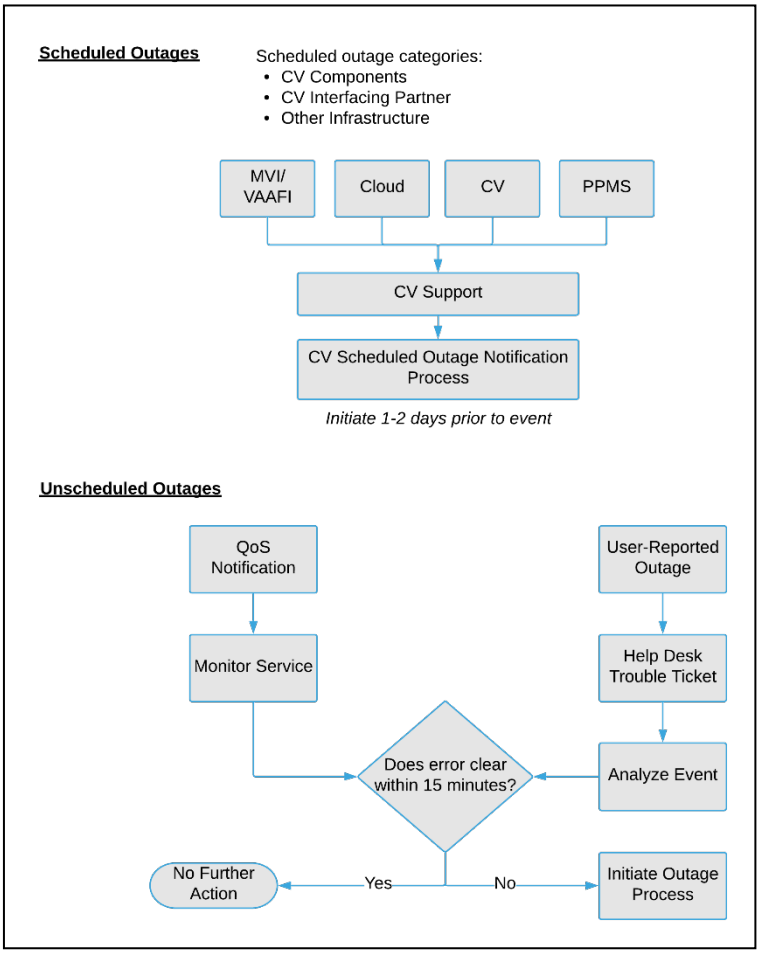
2.6. Scheduled Maintenance

Scheduled downtime typically occurs after 8:00 pm ET, and service is restored by 8:00 am ET. Any planned downtimes (within VA control) outside of these hours require justification and approval by VHA CV Team and the Office of Information and Technology (OIT) Project Manager (PM) / Contracting Officer's Representative (COR).

The Release Manager actively monitors all relevant systems maintenance schedules and follows the scheduled downtime notification process for CV application code-driven patch releases. A representative from the CV Support team notifies the VA stakeholders and the ESD when the CV system is restored to service.

Figure 13 depicts the CV process for monitoring, analyzing, and initiating the notification for an outage.

Figure 13: Scheduled Downtime and Unscheduled Outage Overview



2.7. Unscheduled Outage Triage Process

An unscheduled outage typically occurs when there is a major unexpected Production issue. As such, the processes in the following sections are triggered (i.e., when the entire CV application is down and/or a significant number of end users are impacted).

NOTE: The Quality of Service (QoS) tool is the primary means of monitoring the CV application. The processes described below are specific to the QoS tool and its related incident responses. The VHA CV team is responsible for notifying end users.

2.7.1. Outage Triage Timeline

The CV Outage Triage process is executed by CV Support in coordination with the VA CV interface systems teams (e.g., MVI), as necessary.

The following steps represent routine system monitoring:

1. Monitor e-mail to see if the CV application corrects itself

a. Wait 15 minutes to see if a QoS e-mail arrives indicating that there are no errors (e.g., *AITC - CVQoS Report: NO ERRORS DETECTED)*
b. Check junk e-mail folder for QoS alerts

4. If a QoS e-mail is received indicating "*NO ERRORS DETECTED,"* the system is connected and executing properly

2.7.2. Escalation

The escalation process typically follows this progression:

1. The problem is reported
   a. QoS reports a problem that remains unresolved for over 15 minutes (See Availability Monitoring)

      -OR-

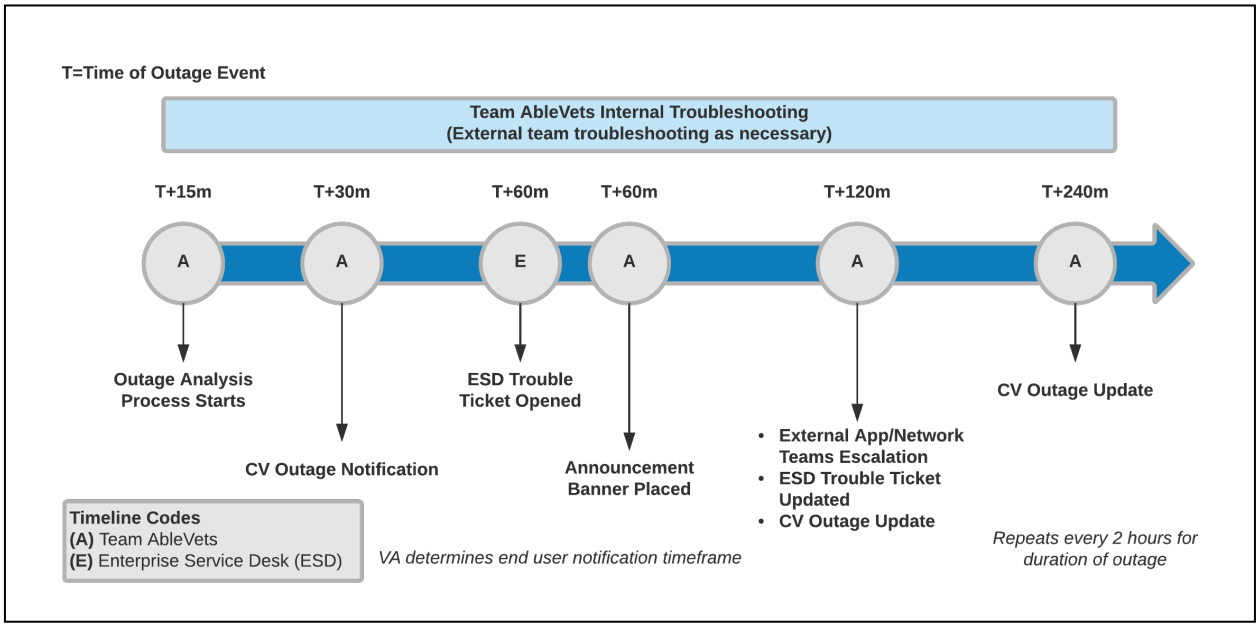
   b. A VA Staff user calls the ESD, or a Community Care Provider contacts the Community Provider Technical Service Desk and opens a trouble ticket

      NOTE: There are instances when a VA user may bypass the ESD and go directly to the VA PM/COR or other program contact. Should this occur, direct the user to the ESD to complete an official trouble ticket.

2. CV Support analyzes the problem and determines whether to initiate the triage process
3. Once the triage process is initiated, CV Support follows the analysis and notification timeline and escalation (as necessary) processes, and includes external systems teams (Figure 14)

   NOTE: Discoveries made regarding the root cause of an issue and the service restoration time frame are communicated via e-mail to the stakeholders as soon as they come to light.

Figure 14: Outage Event Activities and Timeline



2.7.3. Issue Resolution and After Action

The following steps are taken after the issue is resolved:

1. After the issue is resolved, determine if the root cause was *internal* to the CV application
   a. If the problem was with an *external system/service*, obtain the root cause from the applicable team (Table 14)
2. Send an e-mail to the CV stakeholders (Table 3) stating that CV is back online and available for use
   a. Include the root cause of the issue and details of the fix required to resolve the issue, if available

2.8. Capacity Planning

The CV Support team monitors the performance of CV, the associated servers, user onboarding, and user behavior on a weekly basis. Server resources and CV application data are collected by the AITC Monitoring group, using the CA APM suite.

CA APM monitors and stores data and sends alerts to notify the members of the CV Operations team e-mail distribution group when any metric exceeds its upper or lower boundary. The e-mail distribution group is maintained by the CV Support team.

2.8.1. Initial Capacity Plan

Server processing capacity forecasts and workload modeling is conducted in an ad hoc manner. These forecasts are used to project server capacity based on Production data, CV requirements, and CV application changes planned for future releases.

3. Exception Handling

Like most systems, CV may generate a small set of errors that are considered routine, in the sense that they have minimal impact on users and do not compromise the operational state of the system. Most errors are transient in nature and are resolved by the user trying to execute an operation again. The following subsections describe these errors, their causes, and what, if any, response an operator should take.

3.1. Routine Errors

While the occasional occurrence of errors may be routine, encountering many individual errors over a short period of time is an indication of a more serious problem. In that case, the error must be treated as a significant error. Refer to Significant Errors for more information.

3.1.1. Security Errors

A VA Staff user may encounter the login error message, "*Not a valid ACCESS/VERIFY CODE pair*," if they mistype their VistA Access or Verify code.

CCPs may encounter a login error message if they attempt to access CV when their status is not set to *active* in PPMS: "*There is an issue preventing your access to Community Viewer. Please contact your VA Contractor or VA Medical Center for assistance*." CCPs may also encounter the error message, "*Username and/or Password is incorrect*," if they enter an invalid username/password combination.

3.1.2. Login Errors

A VA Staff user's login credentials will be locked after five incorrect login attempts by the VistA service to which CV connects. If this occurs, the user contacts the ESD and opens a service request ticket. The user's local VistA Administrator can unlock their account.

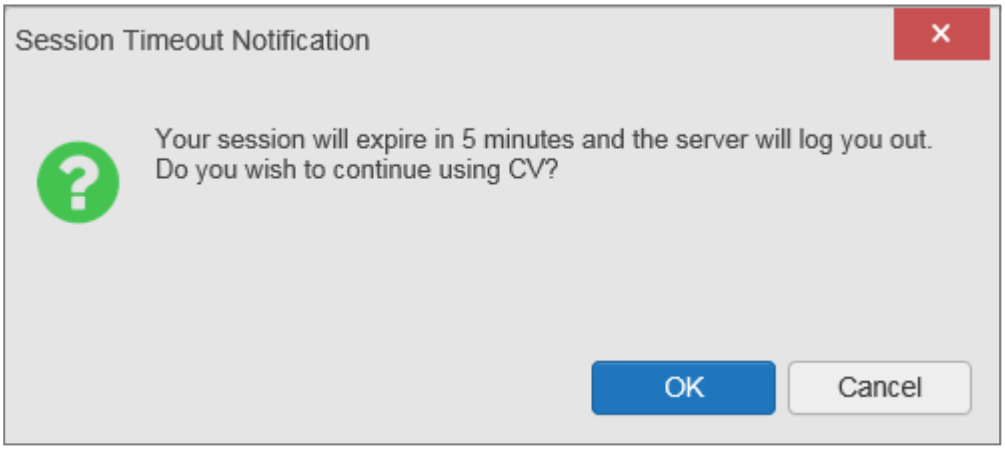
3.1.3. Timeouts

Each section below describes a possible timeout error.

3.1.3.1. Application Timeout

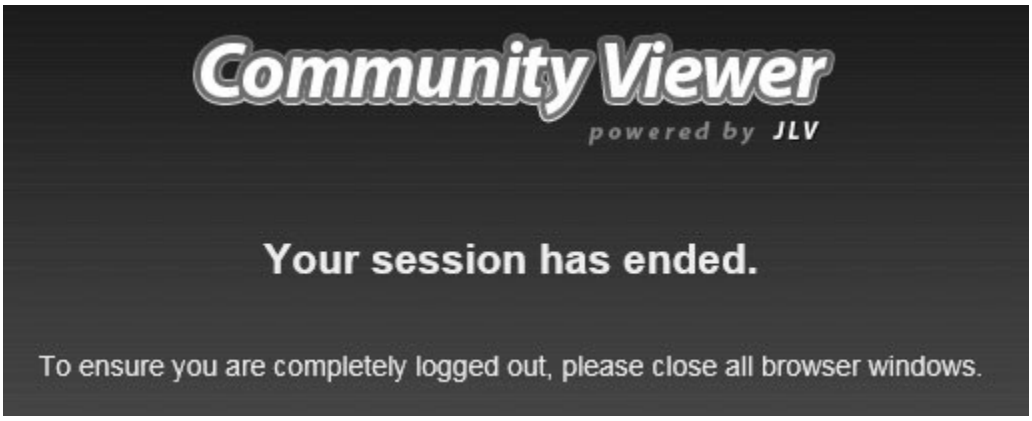
CV has a timeout feature that is set to 30 minutes of inactivity. If users leave the CV application idle for 25 minutes, they receive an audible and visual Session Timeout Notification (Figure 9). If the user would like to extend the session, they can click the OK button to continue using CV.

Figure 15: Session Timeout Notification



If the user does not interact with the Session Timeout Notification message within the 30-minute time limit, the CV session times out (Figure 16). The user must then close the browser, reopen the browser, and log back in to CV.

Figure 16: Session Timeout



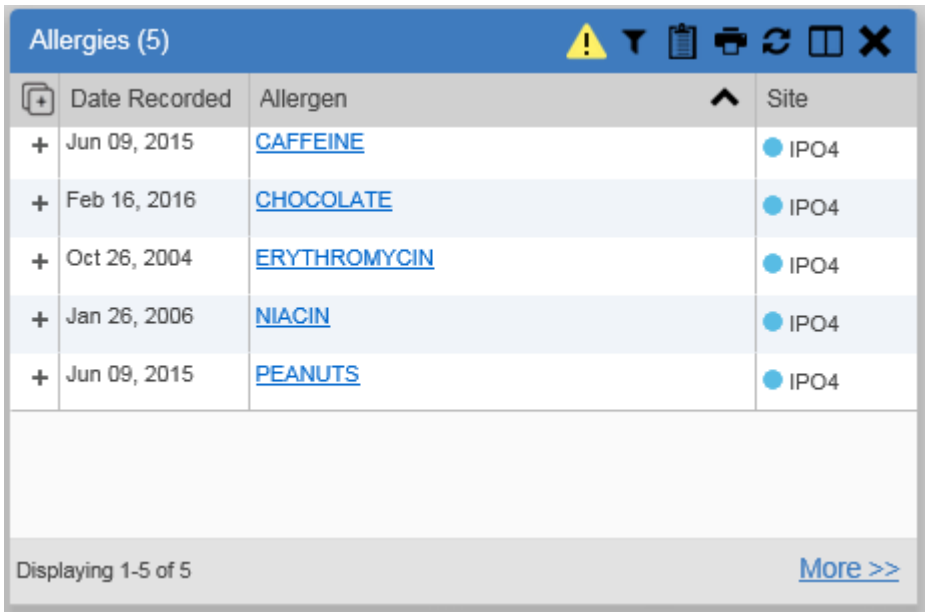
3.1.3.2. Connection Errors

If users encounter a web browser timeout error or the browser displays, *"This page can't be displayed,"* when accessing the correct URL, it indicates that CV application services are either not running or there is a network outage.

Either the CV Support team or the active site's System Administrators may attempt to remote desktop in to each CV application server to ensure the WebLogic services are running. If they are running, System Administrators contact IO to verify that the Local Traffic Manager (LTM) is operating correctly.

CV may also report timeouts to external systems within widgets by displaying a message that one or more data sources could not be connected (Figure 17).

Figure 17: Connection Error



NOTE: Connection errors that persist for more than 5 minutes must be investigated by Tier 3 support.

3.1.4. Concurrency

Concurrency is monitored and handled by IO. They optimize the load balancing of the application using an F5 appliance to handle concurrent user sessions.

3.2. Significant Errors

Significant errors are defined as errors or conditions that affect the system stability, availability, performance, or otherwise make the system unavailable to its user base. The following subsections contain information to aid administrators, operators, and other support personnel in the resolution of significant errors, conditions, or other issues.

3.2.1. Application Error Logs

jMeadows retains user actions in an audit log and stores it in the CV data store. Specific events regarding user transactions are also audited (captured in log files), including but not limited to user ID, date and time of the event, type of event, success or failure of the event, successful and failed login attempts, and the identity of the information system component in which the event occurred.

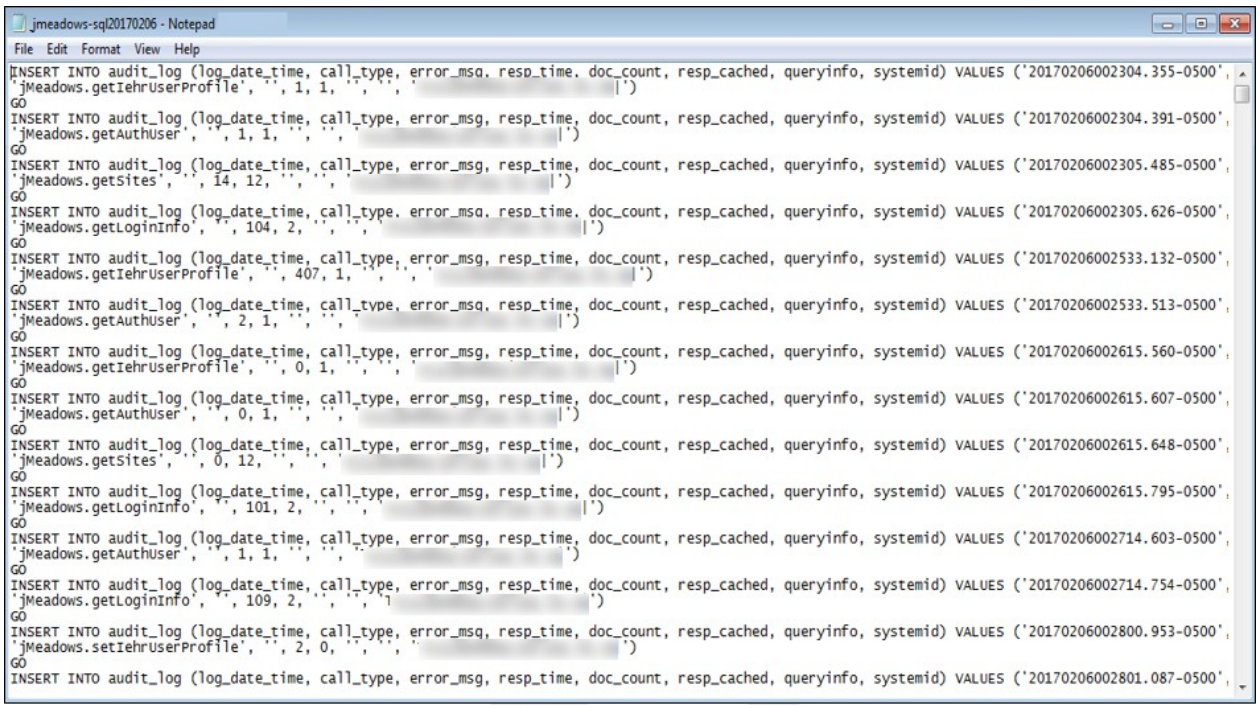
Each time an attempt is made to interface with jMeadows, whether it is a service communication or a user searching for a patient, the activity is logged and stored in the CV data store. The purpose of retention is for traceability; specifically, to show what calls/actions were made, where, by whom, and when they terminated. Each query for data is audited and has both the user and patient ID linked to it. Only one audit log is produced, and it is included in the overall VM backup.

Query times for each web service call in to jMeadows and VDS are recorded to a file in the /u01/CV_HOME/logs/ directory on the server, where the services are installed. A log file output for jMeadows Data Service provided in Figure 18. Table 11 lists the response time log locations.

Table 11: Response Time Log Location

Data Service	Log File Name
jMeadows Data Service	jmeadows-sql.txt
VDS	vds-sql.txt

Figure 18: jMeadows Log Output



The QoS service deployed with the CV web application monitors the availability of services that connect to CV data sources and other outside systems. Connection errors within the CV environment are written to the QOS_LOGS table within the CV DB and displayed in the CV web application.

Service interruptions detected by the QoS service are reported to the CV Support team via e-mail. An automated e-mail notification is sent every 6 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset. The next e-mail is generated after 6 hours if no further system status changes are detected. The QoS service does not send service interruption notices to external systems or services. Each backend server has its own functional and service-specific application store, for example: /u01/apps/oracle/mwhome/user_projects/domains/<DOMAIN_NAME>/servers/<MGD_SERVER_NAME>/logs. Application information and errors are logged to those stores. Error logs are kept indefinitely.

The CV Support team utilizes system notifications generated from the QoS service to diagnose service interruptions and troubleshoot potential issues.

Standard SQL server, WebLogic, Java, Hypertext Markup Language (HTML), and PPMS error codes, generated by the system and recorded in application logs, are used to identify, triage, and resolve complex issues that may arise during system operation.

3.2.2. Application Error Codes and Descriptions

The CV Support team utilizes system notifications generated from the QoS service to diagnose service interruptions and troubleshoot potential issues.

Standard SQL Server, WebLogic, Java, and Hypertext Markup Language (HTML) error codes - generated by the system and recorded in the application logs - are used to identify, triage, and resolve complex issues that may arise during system operation.

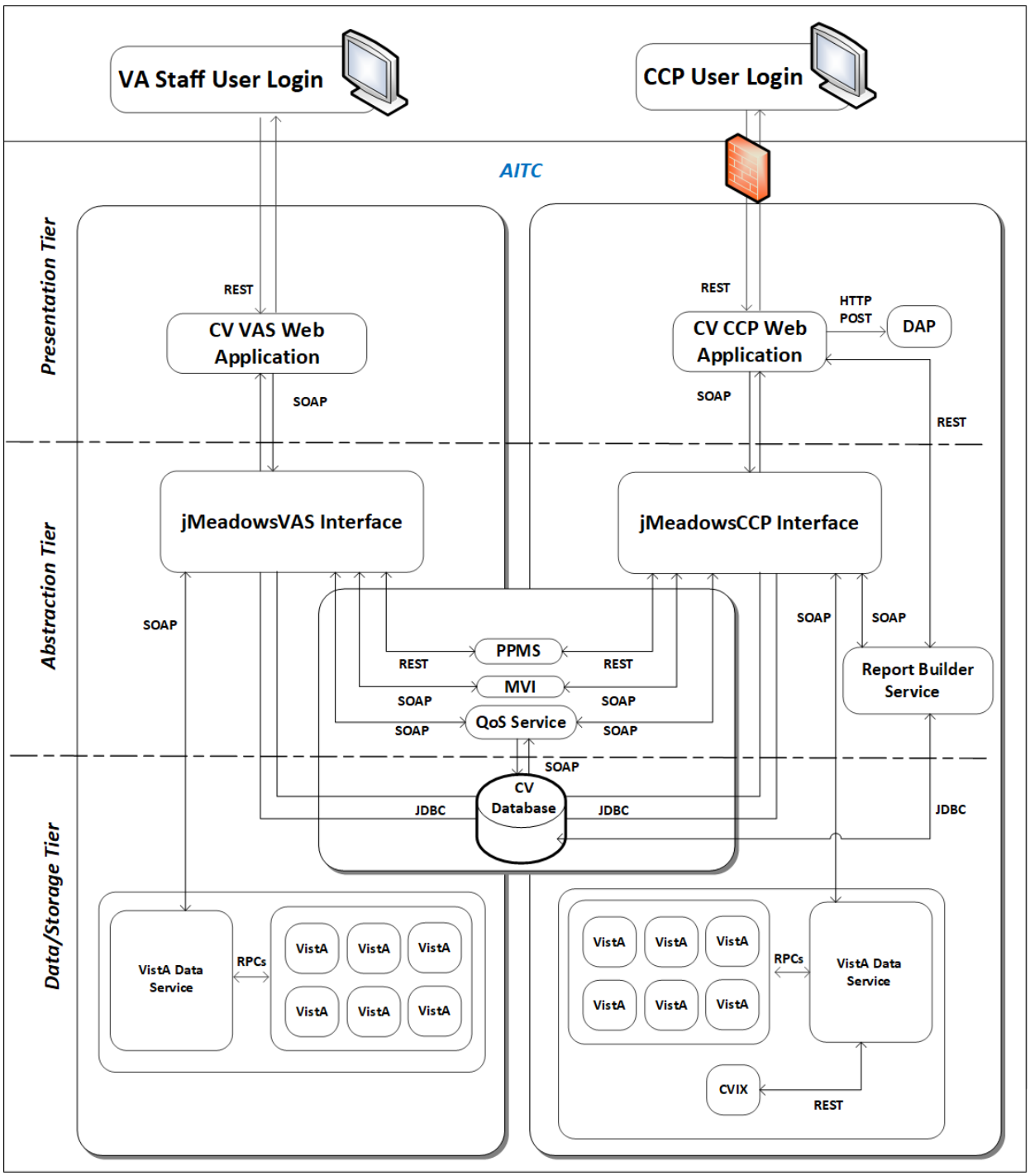
3.2.3. Infrastructure Errors

3.2.3.1. DB

The CV DB is a relational DB used to store user profile information and audit data. It also stores terminology mappings (both local terminology and national standards). The DB does NOT store, neither long term nor temporarily, patient or provider electronic health records (EHRs) from source systems.

The CV DB sits on a dedicated server within a deployed CV environment, alongside the server hosting the CV application and VDS (Figure 19). Only the CV application and components of the CV system connect to, and utilize, the CV DB.

Figure 19: CV Architecture and Components



For detailed information about errors and events for the SQL Server DB Engine, please see the website MS Developer Network Database Engine Events and Errors. [5]

[5] https://msdn.microsoft.com/en-us/library/ms365212(v=sql.110).aspx

The CV DB has a table to audit user actions within the application within the AUDIT DB table. This table collects system usage data and provides the CV Support team the ability to create reports and extract pertinent information from the DB, as needed. A sample of the Audit log can be seen in Figure 20.

Figure 20: Audit Log

	auditID	entryDate	startDate	endDate	systemID	userID	userNPI	userName	patID	category	info	queryType	cardID	ipAddress	email	tester	eventID	siteAgency	siteMoniker	complexTransaction
1	362797	2017-07-18 22:46:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	RadiologyVbxViewer		JLV	654321	NULL	dood@mcluvin.com	NULL	6899798.8451-1	VA	AINA	NULL
2	362798	2017-07-18 22:46:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	RadiologyVbxViewer		JLV	654321	NULL	dood@mcluvin.com	NULL	6849870.8462-1	VA	AINA	NULL
3	362785	2017-07-18 22:45:00	NULL	NULL	200	10000000270				login		JLV	654321	0:0:0:0:0:0:0:1	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
4	362786	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	SelectPatientMVI	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	0000000003	NULL	NULL	NULL
5	362787	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	selectPatientForVASensitive	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
6	362788	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
7	362789	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
8	362790	2017-07-18 22:45:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
9	362791	2017-07-18 22:45:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
10	362792	2017-07-18 22:45:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
11	362793	2017-07-18 22:45:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
12	362794	2017-07-18 22:45:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
13	362795	2017-07-18 22:45:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
14	362796	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	RadiologyVbxViewer		JLV	654321	NULL	dood@mcluvin.com	NULL	6849796.8287-1	VA	AINA	NULL
15	362783	2017-07-18 22:44:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	getAuthUser		JLV	6254...	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
16	362784	2017-07-18 22:44:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	getAuthUser		JLV	6254...	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
17	362773	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	SelectPatientMVI	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	0000000003	NULL	NULL	NULL
18	362774	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	selectPatientForVASensitive	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
19	362775	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
20	362776	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
21	362777	2017-07-18 22:09:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
22	362778	2017-07-18 22:09:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
23	362779	2017-07-18 22:09:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
24	362780	2017-07-18 22:09:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
25	362781	2017-07-18 22:09:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
26	362782	2017-07-18 22:09:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
27	362771	2017-07-18 22:08:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	authNoDbVerification		JLV	6254...	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
28	362772	2017-07-18 22:08:00	NULL	NULL	200	10000000270				login		JLV	654321	0:0:0:0:0:0:0:1	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
29	362769	2017-07-18 22:02:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	RadiologyVbxViewer		JLV	654321	NULL	dood@mcluvin.com	NULL	6849796.8287-1	VA	AINA	NULL
30	362770	2017-07-18 22:02:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
31	362768	2017-07-18 21:52:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
32	362757	2017-07-18 21:51:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	authNoDbVerification		JLV	6254...	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
33	362758	2017-07-18 21:51:00	NULL	NULL	200	10000000270				login		JLV	654321	0:0:0:0:0:0:0:1	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
34	362759	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	SelectPatientMVI	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	0000000003	NULL	NULL	NULL
35	362760	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	selectPatientForVASensitive	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
36	362761	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
37	362762	2017-07-18 21:51:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
38	362763	2017-07-18 21:51:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
39	362764	2017-07-18 21:51:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER,PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL
40	362765	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER,PANORAMA	0000000003	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL	NULL	NULL

3.2.3.2. Web Server

CV uses Oracle WebLogic as its web server in the VA environment. CV does not implement any custom WebLogic error handling or reporting. Please refer to the Oracle WebLogic Server Error Messages Reference [6] for more information.

3.2.3.3. Application Server

CV uses Oracle WebLogic as its application server in the VA environment. CV does not implement any custom WebLogic error handling or reporting. Please refer to the Oracle WebLogic Server Error Messages Reference[6] for more information.

3.2.3.4. Network

CV utilizes the network infrastructure provided at AITC. Any network errors that arise are corrected by the team associated with the location of the error.

3.2.3.5. Authentication and Authorization (A&A)

User access control and authentication takes place before CV interfaces with jMeadows. The user is authenticated to their user profile, granting them access to the presentation layer. jMeadows retrieves user profile information from the CV DB, based on their credentials.

VA Staff users must provide their VistA Access and Verify codes to log in. If credentials are not found the message, "*Not a valid Access Code/Verify Code pair.*" displays.

If CCP credentials are not found or are inactive in the CV DB, the message, "*There is an issue preventing your access to Community Viewer. Please contact your VA Contractor or your VA Medical Center for assistance.*" displays. In either case, the login process stops for the user, and no further options appear.

Other A&A error messages are:

- Smart Card Required: The user has not inserted their PIV card into the card reader
- ActivClient: The user's PIV PIN was entered incorrectly
- Missing Code: The user has not entered their Access/Verify code(s)
- Invalid Access Code: The user has entered an incorrect Access/Verify code

Table 12 provides an overview of the authentication sequence for each user.

Table 12: User Authentication Sequence Overview

User	Authentication Sequence Overview
VA Staff	• VA Staff users must provide their PIV and PIN to log in, as well as their VistA Access and Verify codes

[6] https://docs.oracle.com/cd/E24329_01/doc.1211/e26117.pdf

User	Authentication Sequence Overview
CCP	• CCPs are required to use their NPI or the e-mail address associated with their account in the username field, and a password to log in • CV validates their e-mail address against the C_Provider table **-OR-** • CV validates their NPI against the PPMS_Provider table • jMeadows retrieves information from PPMS, determines if the CCP exists in PPMS, and verifies the CCP has a status of "active" in PPMS
RM User (Provider)	• RM users are required to use their e-mail address (username) and a password to log in • CV validates their credentials against the C_Provider table
SDU	• SDUs must be added to the VAS_UserRole table as authorized users • Once authorized, SDUs must provide their PIV and PIN to log in
RM VA Staff	• RMPMs must be added to the VAS_UserRole table as authorized users • RMPM users must provide their PIV and PIN to log in, as well as their VistA Access and Verify codes • UserRole field of VAS_UserRole set to "RMP" provides RM VA Staff access to the RMP Management Widget

A detailed overview of the login process from the user's perspective is provided in the *CV 3.2 VA Staff User Guide* and the *CV 3.2 CCP User Guide*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See System Startup for the link to the repository.

3.2.3.6. Logical and Physical Descriptions

System design specifications and diagrams can be found in the DE&A Compliance Requirements collection for CV in the IBM Rational Tool Suite. See Table 2 for the link to the collection.

3.3. Dependent System(s)

Table 13 lists the external VA systems upon which CV depends, and the errors related to each dependent system.

Table 13: CV External Dependent Systems

Other VA System	Related Error(s)
Site VistA instances	If a VistA site is unavailable, CV displays the *Connection Unavailable* row in the widgets as shown in Connection Errors.
MVI	If MVI is unavailable, CV may display patient search errors or the *"Patient records unavailable"* error message.
PPMS	If PPMS is unavailable, CV displays the "*Failed to retrieve a PPMS response.*" error message.
CVIX	If CVIX is unavailable, CV displays the "*VistA Imaging service is unavailable: Images may not display.*" error message.

3.4. Troubleshooting

Tier 1 troubleshooting for VA users is handled through the ESD. The Community Provider Technical Service Desk provides end user support and troubleshooting for CCPs. They can be reached via e-mail (Community_Provider_Technical_Service_Desk@va.gov).

Tier 2 issues are handled by Health Product Support (HPS).

Tier 3 support and troubleshooting is handled directly by the CV Support team.

3.5. System Recovery

The following subsections define the processes and procedures necessary to restore the system to a fully operational state after a service interruption. Each of the subsections starts at a specific system state and ends with a fully operational system.

3.5.1. Restart After Unscheduled System Interruption

The simplest way to bring the system back to normal operation after the crash of a component is to restart the affected server(s). See System Startup from Emergency Shutdown for guidance.

3.5.2. Restart After DB Restore

Refer to System Startup for system startup procedures.

3.5.3. Backout Procedures

Backout procedures vary depending on the specific release. Please see the *CV DIBR* specific to the version to be backed out for more information. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See System Startup for the link to the repository.

3.5.4. Rollback Procedures

Rollback procedures are dependent on each specific release. Please see the *CV DIBR* specific to the version to be rolled back for more information. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See System Startup for the link to the repository.

4. Operations and Maintenance Responsibilities

Table 14 represents the operational roles and responsibilities for CV.

Table 14: Operations and Maintenance Responsibility Matrix

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
VA ESD Region	N/A	REDACTED	ESD@va.gov
VA ESD Tuscaloosa	N/A	REDACTED	ESD@va.gov
Veterans Health Administration (VHA) Community Support	Tier 1 support for CCPs	N/A	vha.communitysupport@va.gov

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
VA CV Project Office	**Office of Information Technology (OIT) and VHA Stakeholders**	**N/A**	**N/A**
REDACTED	Program Manager (PM)	REDACTED	REDACTED
REDACTED	CV PM	REDACTED	REDACTED
REDACTED	Business Owner	REDACTED	REDACTED
REDACTED	CV Test Lead	REDACTED	REDACTED
REDACTED	**CV Support**	**N/A**	**N/A**
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
VAAFI Data Power	**Technical Issues/Support Contacts**	**N/A**	**N/A**
REDACTEDhet ty	VAAFI Lead	REDACTED	REDACTED

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
REDACTED	Deputy PM Single Sign on Internal (SSOi)	REDACTED	REDACTED
REDACTED	VAAFI	REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
IO	**Technical Issues/ Support Contacts**	**N/A**	**N/A**
REDACTED	Analyst	REDACTED	REDACTED
REDACTED	Analyst	REDACTED	REDACTED
REDACTED	WebLogic / Java Admin	REDACTED	REDACTED
REDACTED	Windows Admin	REDACTED	REDACTED
REDACTED	Linux Admin	REDACTED	REDACTED
MVI (VA)	**Technical Issues/ Support Contacts**	**N/A**	**In VA ServiceNow assigned under: VA—Development—DEV-Person Service** **VHAISWIAMHELPDESK@va.gov** **MVITECHLEAD@va.gov**
REDACTED	MVI/VAAFI Lead Developer/Architect	REDACTED	REDACTED
REDACTED	MVI Point of Contact (POC)	REDACTED	REDACTED
REDACTED	MVI POC	REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED	MVI POC	REDACTED	REDACTED
REDACTED	SSOi POC	REDACTED	REDACTED
PPMS	**Technical Issues/Support Contact**	**N/A**	**N/A**
REDACTED	PPMS POC	REDACTED	REDACTED
VA Network Security Operations Center (NSOC)	**Technical Issues/Support Contacts**	**855-673-4357 Option 6, then 4 304-260-6685**	**In VA ServiceNow assigned under: VA NSOC Business Partner Extranet (BPE) Operations -OR- Network Support Center (NSC) BPE Operations** **VANSOCBPEOperations@va.gov**
REDACTED	Triple-I/VA-NSOC	REDACTED	REDACTED

5. Approval Signatures

REDACTED

REDACTED

A. Acronyms and Abbreviations

Table 15 lists the acronyms and abbreviations used throughout this document and their descriptions.

Table 15: Acronyms and Abbreviations

Acronym	Definition
A&A	Authentication and Authorization
AITC	Austin Information Technology Center
API	Application Programming Interface
APM	Application Performance Management
BPE	Business Partner Extranet
BSE	Broker Security Enhancement
CA	Computer Associates
CCP	Community Care Provider
CPU	Central Processing Unit
CV	Community Viewer
CVIX	Central VistA Imaging Exchange
DB	Database
DE&A	Design, Engineering, and Architecture
DIBR	Deployment, Installation, Backout, and Rollback
DWS	Data Web Service
EHR	Electronic Health Record
ESD	Enterprise Service Desk
GB	Gigabyte
GUI	Graphical User Interface
HPS	Health Product Support
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language
HTTP	HyperText Transfer Protocol
IBM	International Business Machines Corporation
ICD	Interface Control Document
ICN	Integration Control Number
ID	Identification
IEN	Internal Entry Number
IO	Infrastructure Operations
JLV	Joint Legacy Viewer
JDBC	Java Database Connectivity
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
LTM	Local Traffic Manager

Acronym	Definition
MS	Microsoft
MVI	Master Veteran Index
NPI	National Provider Identifier
NSC	Network Support Center
NSOC	Network Security Operations Center
OIT	Office of Information and Technology
PDF	Portable Document Format
PIN	Personal Identification Number
PIV	Personal Identity Verification
PM	Program/Project Manager
POC	Point of Contact
POM	Production Operations Manual
PPMS	Provider Profile Management System
QoS	Quality of Service
RAM	Random Access Memory
REST	Representational State Transfer
RM	Risk Management
RMPM	Risk Management Provider Manager
SOAP	Simple Object Access Protocol
SDU	Service Desk User
SQL	Structured Query Language
SMS	Systems Made Simple
SSMS	SQL Server Management Studio
SSOi	Single Sign on Internal
URL	Uniform Resource Locator
VA	Department of Veterans Affairs
VAAFI	VA Authentication Federation Infrastructure
VAS	VA Staff
VDS	VistA Data Service
VHA	Veterans Health Administration
VI	VistA Imaging
VistA	Veterans Information Systems and Technology Architecture
VM	Virtual Machine