Community Viewer (CV) 1.5

Production Operations Manual

January 2017

Version 1.9

Department of Veterans Affairs (VA)

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
01/10/2017	1.9	Updated per client feedback and resubmitted	AbleVets
12/30/2016	1.8	Updated per client feedback and resubmitted	AbleVets
12/29/2016	1.7	Updated per client feedback and resubmitted	AbleVets
12/28/2016	1.6	Updated per client feedback and resubmitted	AbleVets
12/22/2016	1.5	Updated per client feedback and resubmitted	AbleVets
12/09/2016	1.4	Updated for security banner information and resubmitted	AbleVets
11/29/2016	1.3	Updated per client feedback and resubmitted	AbleVets
11/08/2016	1.2	Updated per client feedback and resubmitted	AbleVets
11/02/2016	1.1	Updated per client feedback and submitted for CLIN 0003AK	AbleVets
10/11/2016	1.0	Prepared document for approval signatures	Apex

Artifact Rationale

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

Table of Contents

Table of Figures

Table of Tables

1. Introduction

This Production Operations Manual (POM) describes how to maintain the components of the Community Viewer (CV), as well as how to troubleshoot problems that may occur with this product, in production. The intended audience for the POM are the Information Technology (IT) teams responsible for hosting and maintaining the system after production release.

2. Routine Operations

The following sections define the routine operations, management, and monitoring of CV systems.

2.1. Administrative Procedures

2.1.1. System Start-up

VA Enterprise Operations (EO) manages the Global Traffic Managers (GTM). Startup steps for those devices are, therefore, out of the scope of this document.

1. Start the CV database servers in the Austin Information Technology Center (AITC).
    a. The database server processes are configured to run as system services, and will automatically start with the server itself. Their successful startup will be verified in a following step.
2. Start the VistADataService servers in AITC.
    a. The service processes are configured to run as system services, and will automatically start with the server itself. Their successful startup will be verified in a following step.
3. Start the jMeadows servers in AITC.
    a. The service processes are configured to run as system services, and will automatically start with the server itself. Their successful startup will be verified in a following step.
4. Start the CV web application servers for VA Administrative Staff (VAS) users in AITC (EO Cloud).
    a. The service processes are configured to run as system services, and will automatically start with the server itself. Their successful startup will be verified in a following step.
5. Start the CV web application servers for Community Care Provider (CCP) users in AITC (Non-cloud).
    a. The service processes are configured to run as system services, and will automatically start with the server itself. Their successful startup will be verified in a following step.
6. Open the CV web application (For VAS Users):
    a. Access the Uniform Resource Locator (URL) and use Personal Identity Verification (PIV) card, when prompted.
    b. Verify that the CV Login page for VAS users displays as expected, and indicates that system status is normal.

NOTE: A script is run to ensure that all systems are operational. In addition, opening the URL for CV ensures that all CV context roots will be reached.

c. For CCP users:

d. Access the URL

e. Verify that the CV Login page for CCP users displays as expected, and indicates that system status is normal.

NOTE: Troubleshooting details can be found in Section 3.4, Troubleshooting.

2.1.1.1. System Start-Up from Emergency Shutdown

As long as the system shutdown procedures are performed, no special startup procedure is necessary. Use the steps documented in, Section 2.1.1, System Start-up, as needed.

In case of a power outage or other abrupt termination of the server operating systems, start up the servers as documented, and allow the operating system to check disks for corruption. Consult with EO to ensure the database recovers successfully.

2.1.2. System Shutdown

NOTE: To avoid issues with in-progress transactions, these procedures should be performed during a published maintenance window so that there will be few users accessing the system.

1. Shut down the WebLogic services on the CV web application servers in AITC.
2. Shut down the CV web application servers in AITC (EO 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 on the VistADataService servers in AITC.
7. Shut down the VistADataService servers in AITC.
8. Shut down the CV database servers in AITC.

2.1.2.1. Emergency System Shutdown

Shut down all servers (CV web applications on EO Cloud and Non-cloud environments, jMeadows, VistADataService, and CV database) in the AITC, in any order.

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.

In VA production, EO Cloud manages the platform and installation of both the operating systems and the baseline installation of Microsoft (MS) Structured Query Language (SQL) Server.

2.1.3.1. Backup Procedures

Production systems are currently configured to back up the database daily. The database backups are assumed to be a part of the overall Virtual Machine (VM) backup.

The CV Support team, comprised Systems/Network/Security Engineers and Systems Administrators from team AbleVets, has created secondary backup procedure; it is an automated, scheduled job that backs up the database and stores it locally on the VM. This secondary backup is performed daily, and is monitored/audited on a weekly basis to ensure that the backups are running. Two weeks of backups are kept available at all times.

Under the full, or bulk-logged, recovery model, before a database in SQL Server Management Studio can be restored, the active transaction log, known as the tail of the log, must be backed up. In order to restore an encrypted database, access to the certificate or asymmetric key that was used to encrypt the database is required. Without the certificate or asymmetric key, the database restoration cannot be completed. As a result, the certificate used to encrypt the Database Encryption Key (DEK) must be retained as long as the backup is needed. The DEK is stored in a central location, to which all authorized System Administrators have access. Because all authorized System Administrators have access to this central location, no other contact is required to obtain the DEK.

2.1.3.2. Restore Procedures

Pre-requisites to recover databases:

1. Database backup (.bak) file for the CV database.

To restore a full database backup:

1. After you connect to the appropriate instance of the MS SQL Server Database Engine, in Object Explorer, click the server name to expand the server tree.
2. Right-click 'Databases', click 'Restore Database'
3. On the General page, use the Source section 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. In the Backup media type box, select 'File', click Add.
    c. Navigate to the location of the backup file (.bak) of the CV database, click OK.
    d. After you add the devices you want to the Backup media list box, click OK to return to the General page.
    e. In the Source Device: Database list box, select the name of the database to be restored (CV).

    NOTE: You may be prompted for the DEK.
4. In the Destination section, the Database box is automatically populated with the name of the database to be restored. To change the name of the database, enter the new name in the Database box.

5. In the Restore To box, leave the default as To 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.
6. In the Backup sets to restore grid, select the backups to restore. This grid displays the backups available for the specified location. By default, a recovery plan is suggested. To override the suggested recovery plan, change the selections in the grid. Backups that depend on 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.
7. Optionally, click Files in the Select a page pane to access the Files dialog box. From here, you can restore the database 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

1. Servers
   a. Backups of the VMs are done at the EO data center by the AITC/Philadelphia Information Technology Center (PITC) Systems Administrators.
   b. Backups are taken daily.
   c. Testing of those backups is done by EO.
   d. Validation of these restoration to be confirmed by:
      i. Validating all software/configurations are restored from the expected configuration.
      ii. Configuration files contain server specific settings.
      iii. Application server starts as expected, validated through logs and through smoke test of application.
2. Database
   a. Backups are taken daily.
   b. Backups are periodically restored to our backup database servers (vaausjlvsql202, vaphijlvsql202) to test restore procedures and integrity of the backup files.
   c. Administrators validate that data in the database contains up-to-date entries for whitelist, user profiles, and audit logging.
   d. Validation of operations will be confirmed through smoke test of applications.

2.1.3.4. Storage and Rotation

In CV production environments, the EO Cloud teams in AITC/PITC manage the platform, and, as such, also manage any storage and rotation scheduling. EO ensures the system and storage arrays for the system are operating properly by inspecting CV Quality of Service (QoS) logs and notifications.

The contractor is responsible for ensuring that the partition structure in use is sufficient, which, in turn, ensures the storage space is sufficient.

2.2. Security/Identity Management

The CV system restricts access to the CV Graphical User Interface (GUI) to authorized users within, and authorized providers outside of, the VA.

- The authorized user list for VAS users is generated from a table within the CV database. The table contains a list of names and associated va.gov e-mail addresses.
- The authorized user list for CCP users is generated from a table within the CV database. The table contains a list of names and associated e-mail addresses.

After reaching the CV Login page (VAS users):

- The CV Login page requires a VA PIV card and Personal Identification Number (PIN) to log in, along with the user’s local existing Veterans Information Systems and Technology Architecture (VistA)/Computerized Patient Record System (CPRS) Access and Verify codes. If there is no entry on the authorized user list that matches, an “*Access Denied. You are not an authorized user*” message is displayed.

The CV Login pages guide the user through the login process, including, where necessary, fields to enter user credentials. For VAS users, these fields will include Access/Verify Codes, Agency (Veterans Health Administration (VHA)), and Site. A VAS user must insert his/her PIV card into the computer before entering the URL of the CV web application into the address bar of the browser window.

Upon reaching the CV Login page (CCP users):

- Login: The CV Login page requires a user name (the e-mail address used when the account was created), and a password.
  - If there is no entry in the CV database that matches the credentials, the message: “*Access Denied. You are not an authorized user*” is displayed.
  - If there is an entry in the CV database that matches the credentials, the VA Privacy and Security Awareness Training page is displayed.
- Consent: Prior to accessing the functionality of the application, CCPs are prompted to agree to a security and legal disclaimer, confirming they are aware that they are accessing a government information system, provided for authorized users only.
- Training and Security Acknowledgement: Prior to accessing the CV functionality of the CV application for the first time, and each year thereafter (365 days from first successfully login), CCPs are prompted to complete and acknowledge VA Privacy and Security Awareness Training. The system will log and audit the CCP’s agreement.
  - Certification of Information Security Awareness Training: The first time the CCP user logs in to the CV application, and each year thereafter (365 days from first successfully login), they must download and acknowledge reading the Information Security Awareness document. The system will log and audit the CCP’s agreement.
  - Certification of Electronic Health Records Rules of Behavior: The first time the CCP user logs in to the CV application, and each year thereafter (365 days from first

successfully login), they must download and acknowledge reading the Electronic Health Records Rules and Behavior document. The system will log and audit the CCP's agreement.

  - Certification of Health Insurance Portability and Accountability Act (HIPAA) Privacy Training: The first time the CCP user logs in to the CV application, and each year thereafter (365 days from first successfully login), they must certify that they have completed HIPAA privacy training through their organization. The system will log and audit the CCP's agreement.

- Entry into Application: Based upon the user's login credentials, jMeadows retrieves the user's profile information from the CV database. User default host location, custom widget layout, and other user-specific settings/data are returned.

CV access control for CCP users is configured by VAS users. See Section 2.2.2 Access control, for more information.

2.2.1. Identity Management

After the VAS user logs in to the CV web application, there are navigation links and fields available that enable the creation of a CCP user and the CCP user's profile. The CV web application also includes GUI elements to allow VAS users to edit the CCP user profile, or remove the CCP user from the system.

Once the CCP user profile has been created, the VAS user can assign a patient consult to the CCP, which includes access to a specific portion and date range of the patient's EHR.

Patient Identity Management is provided by the VA Master Veteran Index (MVI).

2.2.2. Access control

CV validates user credentials retrieved from the Login page against tables in the CV database. If the credentials match what is stored in the CV database, the user is granted access to the CV web application.

When the credentials entered do not match what is stored in the CV database, the user (either VAS or CCP) will be presented a unique page with the message, *Access denied. You are not an authorized user.* When this message is displayed, the log in process stops, and no further options are presented.

CCP access to patient records is controlled by VAS users, by way of consult assignments. A CCP can access only the records of the patient with whom they have an assigned consultation, and the VAS user restricts CCP access to a specific date range of patient records.

Table 1 summarizes the CV system components and settings utilized in access control implementation.

Table 1: Access Control Design

Component	Description
Database table	The AUTH_USER table within the database contains field elements with user identifiers for VAS users. The C_Provider table within the database contains field elements with user identifiers

Component	Description
	for CCP users. See the *CV 1.5 System Design Document (SDD)*, provided with the CV release, contains the full list of tables and table elements within the CV database.
Database script	A database script is used for future updates to the tables within the CV database.
Configuration settings	A configuration setting within the appconfig-production.properties file enables access control: • Enable VA Access Control, On/Off - This setting enables access control for VAS users.

2.3. User Notifications

Notifications will be sent to the user community when there are scheduled or unscheduled changes in system state, to include but not limited to, planned outages, system upgrades, other maintenance work, and any unexpected system outages.

Notification of planned outages will be initiated 24-28 hours in advance of anticipated system downtime.

Notification of unscheduled outages will occur if an error does not clear within 15 minutes:

1. The CV Support team monitors and evaluates all system issues. The QoS service alerts the CV Support team when a service disruption occurs.
2. VHA Community Support (currently functioning as the Help Desk for CV) is notified by the CV Support team of any outage, and reports same to the users via an Automated Notification Report (ANR) e-mail, with a Help Desk ticket number, and date and time of the outage. Status updates are provided every two hours.

2.3.1. User Notification Points of Contact

The notification distribution list for alerting for VA stakeholders of CV scheduled downtime is maintained by AbleVets. Table 2 shows the current distribution list.

Table 2: CV Scheduled Downtime VA Stakeholders

Name	Organization	Email Address
Green, Elizabeth (Betsy)	VA-Government	Elizabeth.Green4@va.gov
Facundus, Latricia R. (Renae)	VA-Government	Latricia.Facundus@va.gov
Roberts, Jerilyn	VA-Government	Jerilyn.Roberts1@va.gov
Hines, Rick	VA-Government	Rick.Hines@va.gov
Bose, Mary Ellen	VA-Government	MaryEllen.Bose@va.gov
Odle, Phillip	VA-Government	phillip.odle@va.gov
Ortman, Joseph	VA-Government	Joseph.Ortman@va.gov
Rowe, Michelle	VA-Government	Michelle.Rowe1@va.gov
Mosley, Carolina	VA-Government	Carolina.Mosley@va.gov

Name	Organization	Email Address
Guebert, Chad	AbleVets	chad.guebert@ablevets.com
Lukens, Rich	AbleVets	rich.lukens@ablevets.com
Cardenas, Michael	HRG Technologies LLC (HRG)	mcardenas@hawaiirg.com
Goo, Brad	HRG	bgoo@hawaiirg.com
Suenaga, Gregory	HRG	gsuenaga@hawaiirg.com
Guebert, Cristeta J. (Crista)	HRG	cguebert@hawaiirg.com
Flemming, Mitch	SBG	mflemming@sbgts.com
Southerland, John B.	SMS	John.Southerland@va.gov

2.4. System Monitoring, Reporting and Tools

The CV system has the ability to trace and audit actions that a user executes within the CV application. CV audits are provided through the use of audit trails and audit logs that offer a backend view of system use, in addition to recording each user's access to patient data. Audit trails and logs record key activities, including date and time of event, patient identifiers, user identifiers, type of action, and access location, to show system threads of access and the viewing of patient records.

jMeadows writes user actions to an audit log and stores it in the CV data store. Specific events regarding user transactions are also audited (or captured in log files), including, but not limited to, user identification, date and time of the event, type of event, success or failure of the event, successful and failed log in 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, a record of the activity is logged and stored in the CV data store. The purpose of this retention is for traceability; specifically, to see what calls/actions are being made, where and by whom they originated, and when they terminated.

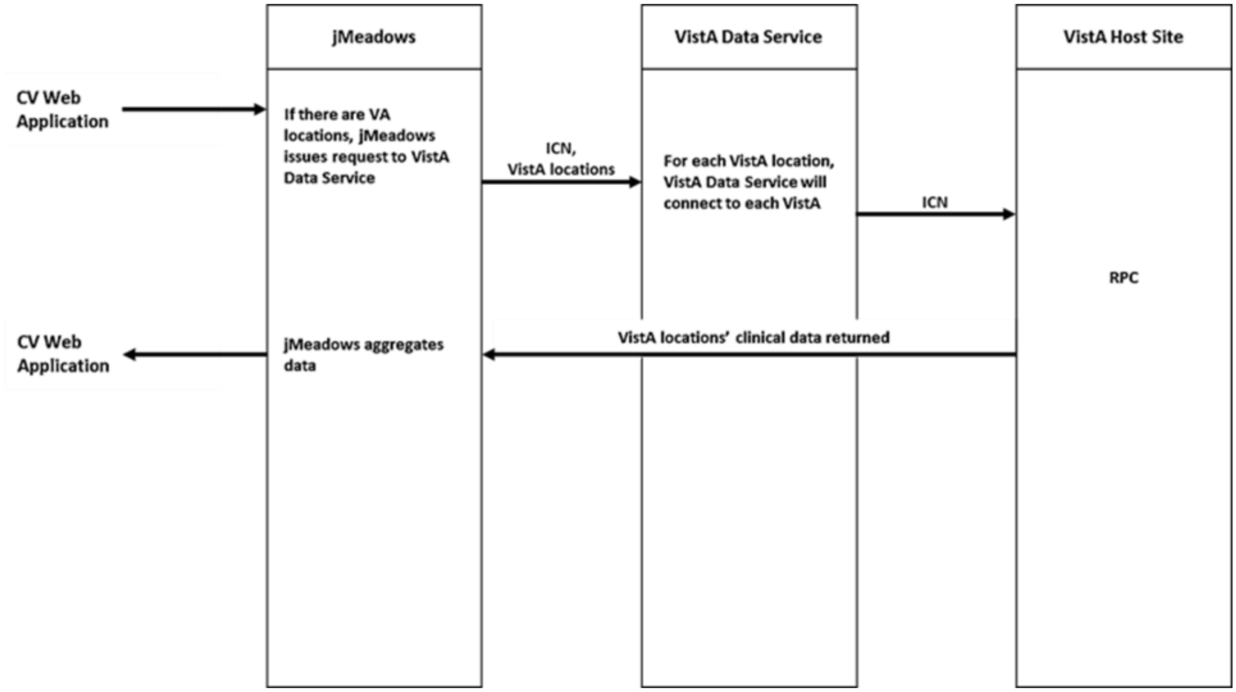
Each CV query for data (i.e., action) is audited, and has the user and patient IDs linked to it. Only one audit log is produced, and it is included in the overall VM backup. See Section 2.1.3, Backup and Restore.

2.4.1. Dataflow Diagram

The data retrieval sequence, depicted in Figure 1, occurs for VA data retrieval after a patient is selected:

1. For each VA location in the patient record, jMeadows issues a request to the VistA Data Service with the VA Integration Control Number (ICN) and VistA location. The ICN and VistA location information is received from MVI.
2. For each VistA location, the VistA Data Service will connect to each VistA, and return the clinical data to jMeadows.
3. jMeadows aggregates the data and returns the data to CV web application.

Figure 1: Data Retrieval from VA Systems


jMeadows
VistA Data Service
VistA Host Site
CV Web Application
If there are VA locations, jMeadows issues request to VistA Data Service
ICN, VistA locations
For each VistA location, VistA Data Service will connect to each VistA
ICN
RPC
VistA locations' clinical data returned
CV Web Application
jMeadows aggregates data

2.4.2. Availability Monitoring

Service availability is monitored through the QoS Service, a CV system component that is deployed with CV in the AITC. The QoS Service monitors the availability of the following:

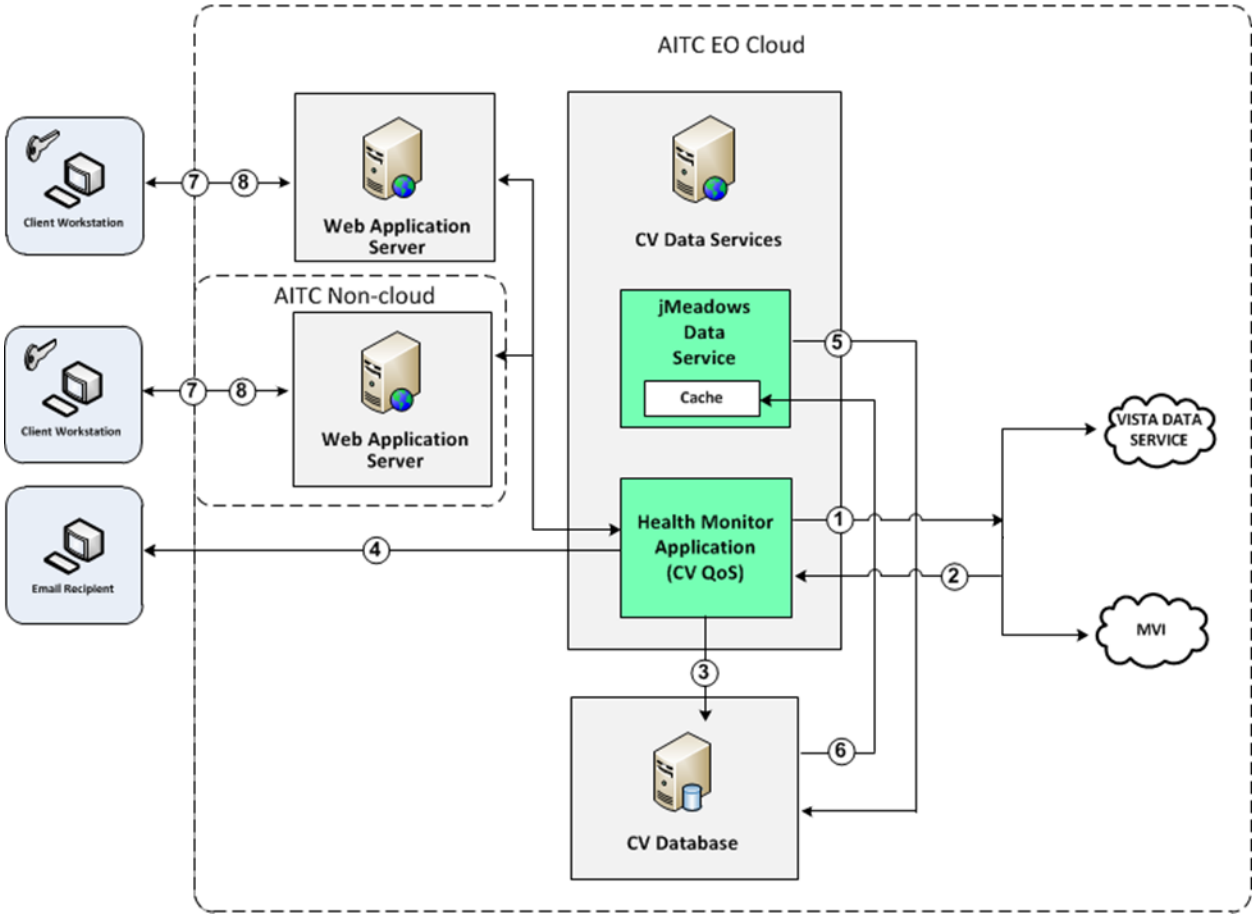
- Master Veteran Index (MVI)
- VistA Data Service
- jMeadows Data Service

In future releases, there will be tools in place to monitor the CV web application and its availability.

System status is displayed in the CV web application for the systems noted above, except for the jMeadows Data Service. System status events for the jMeadows Data Service are logged to the CV database and included in an automated e-mail notification to the CV Support team, but are not provided through the user interface.

A diagram of the system status check sequence can be seen in Figure 2. Additional information about the QoS Service is provided in the *Community Viewer 1.5 System Design Document (SDD)*.

Figure 2: System Status Check Sequence



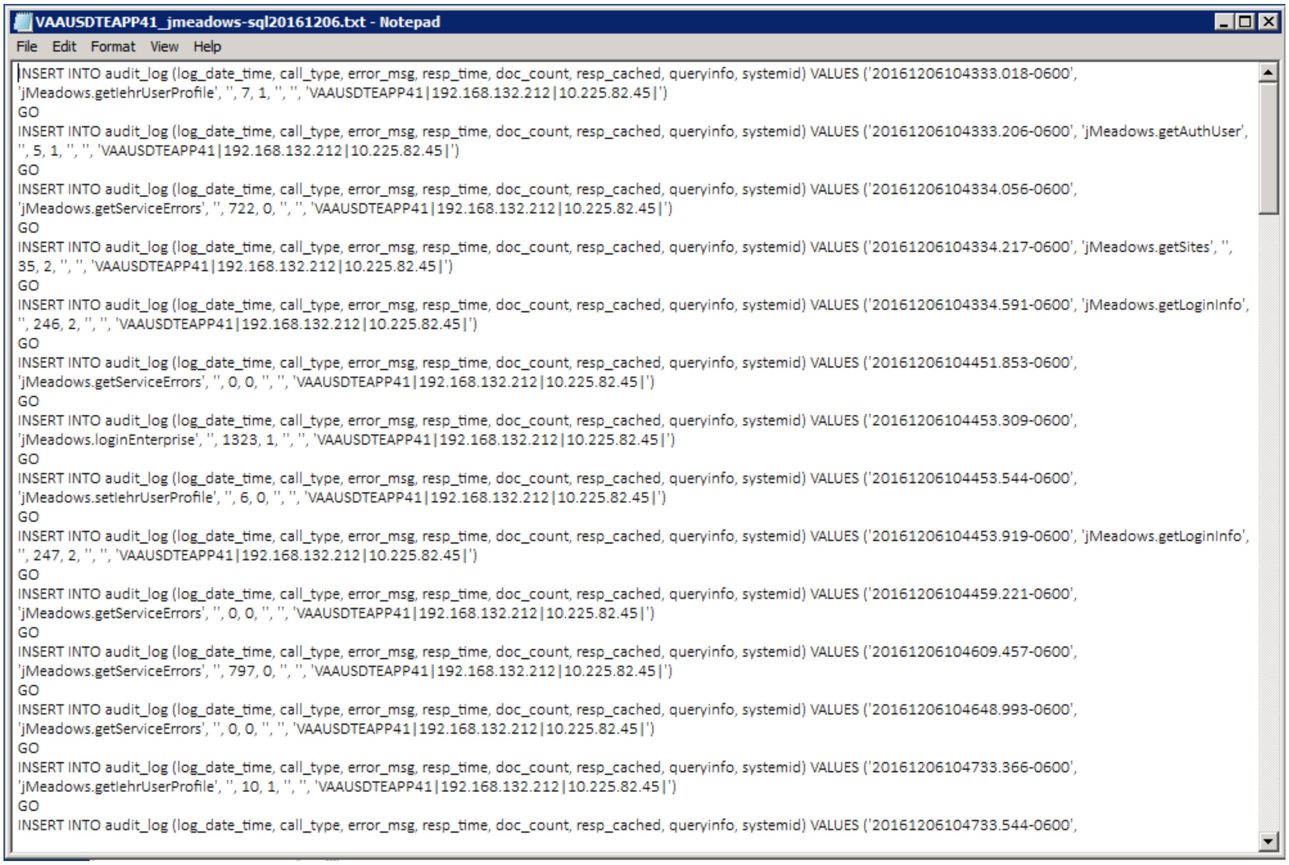
2.4.3. Performance/Capacity Monitoring

Query times for each web service call into jMeadows and VistA Data Service will be recorded to a file in the D:\Log directory on the server where the services are installed. A sample query time log file output for the jMeadows Data Service is provided in Figure 3.

Table 3: Response Time Log Location

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

Figure 3: jMeadows_logOutput


VAAUSDTEAPP41_jmeadows-sql20161206.txt - Notepad
File Edit Format View Help

```
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104333.018-0600',
'jMeadows.getIehrUserProfile', '', 7, 1, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104333.206-0600', 'jMeadows.getAuthUser',
'', 5, 1, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104334.056-0600',
'jMeadows.getServiceErrors', '', 722, 0, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104334.217-0600', 'jMeadows.getSites', '',
35, 2, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104334.591-0600', 'jMeadows.getLoginInfo',
'', 246, 2, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104451.853-0600',
'jMeadows.getServiceErrors', '', 0, 0, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104453.309-0600',
'jMeadows.loginEnterprise', '', 1323, 1, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104453.544-0600',
'jMeadows.setIehrUserProfile', '', 6, 0, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104453.919-0600', 'jMeadows.getLoginInfo',
'', 247, 2, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104459.221-0600',
'jMeadows.getServiceErrors', '', 0, 0, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104609.457-0600',
'jMeadows.getServiceErrors', '', 797, 0, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104648.993-0600',
'jMeadows.getServiceErrors', '', 0, 0, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104733.366-0600',
'jMeadows.getIehrUserProfile', '', 10, 1, '', '', 'VAAUSDTEAPP41|192.168.132.212|10.225.82.45|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20161206104733.544-0600',
```

2.4.4. Critical Metrics

Critical application metrics beyond the number of CCPs entered into the system, number of consults assigned, and number of provider logins have not yet been defined at this time. The CV Development team will add metric requirement reporting to the product backlog as metrics are defined.

2.5. Routine Updates, Extracts and Purges

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

Updates to the CV web application servers within the AITC (Non-cloud) will be performed by AITC personnel.

2.6. Scheduled Maintenance

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 Help Desk when the CV system is restored to service.

2.7. Capacity Planning

The CV Support team will monitor the performance of the CV web application and associated servers, user on-boarding, and user behaviors on a weekly basis. Server resource and CV application data are collected by the AITC Monitoring group using the Computer Associates (CA) Application Performance Management (APM) suite.

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

2.7.1. Initial Capacity Plan

Server processing capacity forecasts and workload modeling are conducted in an ad hoc manner, typically via quarterly updates. These forecasts are used to project server capacity based on real production data, CV requirements, and future CV application changes.

3. Exception Handling

Please see Section 2.4, System Monitoring, Reporting and Tools, for additional information.

3.1. Routine Errors

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

While the occasional occurrence of these errors may be routine, getting a large number of 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 an exceptional condition.

3.1.1. Security Errors

The following security design principles are applied to the CV system to ensure it is a system that follows security protocol standards for secured systems:

- Session security: Through the use of secured, unique session tokens generated using a 128-bit hash from a secure random number generator for each authenticated user, the system ensures prevention of communication session hijacking. Once the user logs out of the system, the session is immediately destroyed, and the session hash can no longer be used. If in some instance the session ID were to be obtained, the user cannot copy and paste it as part of a URL string in order to gain access to the system.
- Data Encryption: The use of Secure Sockets Layer (SSL) with Transport Layer Security (TLS) 1.0 ensures that all server communications are encrypted, which limits the ability to perform Man-in-the-Middle (MITM) attacks.
- Database Encryption at Rest: Microsoft SQL Server Transparent Data Encryption (TDE) Encryption level Advanced Encryption Standard (AES) 256-bit is used to encrypt

Personally Identifiable Information (PII) and Protected Health Information (PHI) data at rest.

- Schema Validation: WebLogic Services are used in CV to employ Schema Validation. This helps prevent Denial of Service (DoS) attacks by preventing the invocation of Extensible Markup Language (XML) bombs.

3.1.2. Time Outs

Each section below describes a possible time-out error.

3.1.2.1. Web Application Time Out

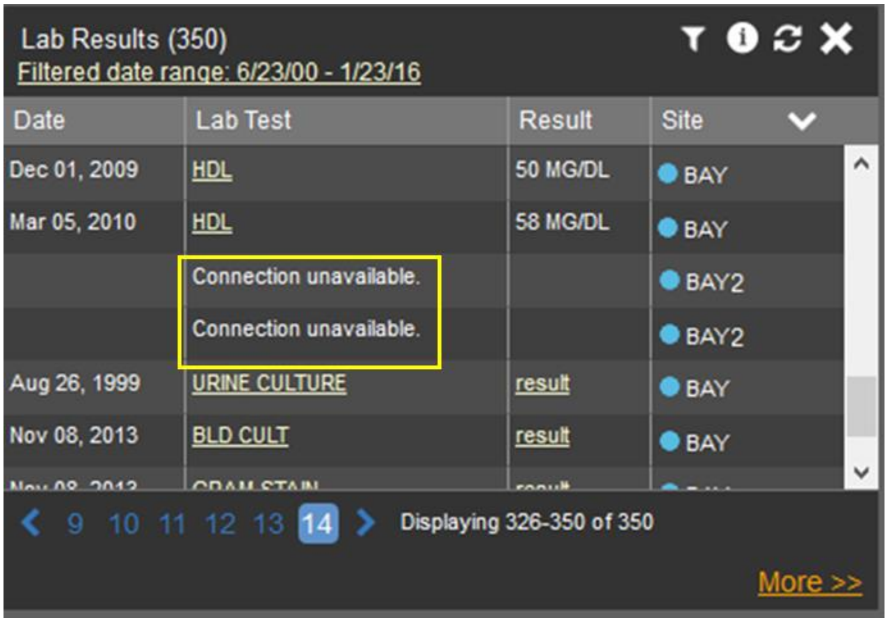
If users encounter a web browser time out error, or the browser displays *This page can't be displayed* when accessing the correct URL, it indicates that the CV web application services are not running, or there is a network outage.

Either the CV Support team, or AITC System Administrators, may attempt to remote desktop into each CV web application server to ensure the WebLogic services are running. If they are running, the EO group will be contacted to verify correct operation of the GTM.

3.1.2.2. Connection Unavailable Errors

The CV web application may also report timeouts to external systems within widgets by displaying *Connection Unavailable* in one or more rows of the widget, as seen in Figure 4.

Figure 4: Connection Unavailable Reporting



Lab Results (350)
Filtered date range: 6/23/00 - 1/23/16

Date	Lab Test	Result	Site
Dec 01, 2009	HDL	50 MG/DL	● BAY
Mar 05, 2010	HDL	58 MG/DL	● BAY
	Connection unavailable.		● BAY2
	Connection unavailable.		● BAY2
Aug 26, 1999	URINE CULTURE	result	● BAY
Nov 08, 2013	BLD CULT	result	● BAY
Nov 08, 2013	GRAM STAIN	result	

< 9 10 11 12 13 14 > Displaying 326-350 of 350

More >>

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

3.1.3. Concurrency

Resolution of concurrent record access is handled by the underlying system of record that is being queried, e.g., VistA.

3.2. Significant Errors

Significant errors can be 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

The QoS service deployed with the CV web application monitors the availability of application 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 database, and are 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 12 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the 12 hour timer is reset. The next e-mail is generated after 12 hours, if no further system status changes are detected. Detailed information on service interruption notifications, and sample e-mail messages are provided in the *Community Viewer 1.5 System Design Document (SDD)*. 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, e.g., /u01/apps/oracle/mwhome/user_projects/domains/<DOMAIN_NAME>/servers/<MGD_SERVER_NAME>/logs. Application information and errors are logged to those stores. At this time, error logs are kept indefinitely.

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 HTML 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

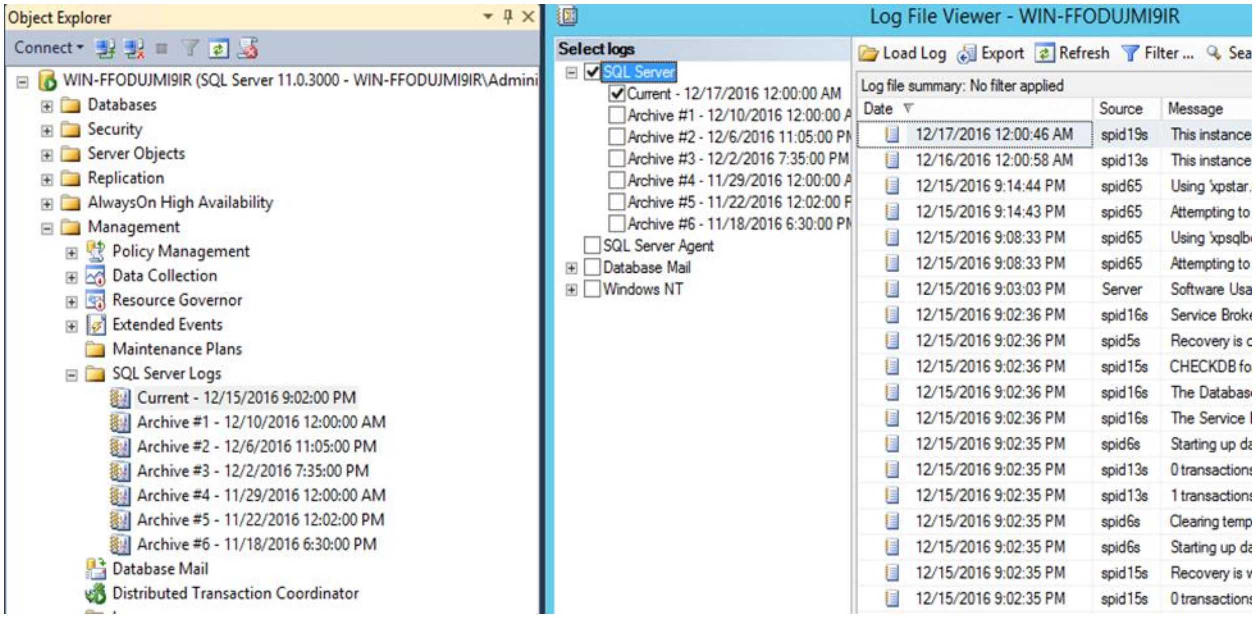
3.2.3. Infrastructure Errors

3.2.3.1. Database

For detailed information about errors and events for the SQL Server Database Engine, please see Database Engine Events and Errors.

The CV database errors are written to an error log within the AUDIT database table. The CV Support team can create reports and extract pertinent information from the database, as needed. A sample of the AUDIT log can be seen in Figure 5.

Figure 5: Sample of Information Collected in AUDIT Table



WIN-FFODUJMI9IR (SQL Server 11.0.3000 - WIN-FFODUJMI9IR\Admini
- Databases
- Security
- Server Objects
- Replication
- AlwaysOn High Availability
- Management
  - Policy Management
  - Data Collection
  - Resource Governor
  - Extended Events
  - Maintenance Plans
  - SQL Server Logs
    - Current - 12/15/2016 9:02:00 PM
    - Archive #1 - 12/10/2016 12:00:00 AM
    - Archive #2 - 12/6/2016 11:05:00 PM
    - Archive #3 - 12/2/2016 7:35:00 PM
    - Archive #4 - 11/29/2016 12:00:00 AM
    - Archive #5 - 11/22/2016 12:02:00 PM
    - Archive #6 - 11/18/2016 6:30:00 PM
  - Database Mail
  - Distributed Transaction Coordinator

☑ SQL Server
- ☑ Current - 12/17/2016 12:00:00 AM
- □ Archive #1 - 12/10/2016 12:00:00 A
- □ Archive #2 - 12/6/2016 11:05:00 PI
- □ Archive #3 - 12/2/2016 7:35:00 PM
- □ Archive #4 - 11/29/2016 12:00:00 A
- □ Archive #5 - 11/22/2016 12:02:00 F
- □ Archive #6 - 11/18/2016 6:30:00 PI

□ SQL Server Agent

□ Database Mail

□ Windows NT

Log file summary: No filter applied

Date	Source	Message
12/17/2016 12:00:46 AM	spid19s	This instance
12/16/2016 12:00:58 AM	spid13s	This instance
12/15/2016 9:14:44 PM	spid65	Using 'xpstar.
12/15/2016 9:14:43 PM	spid65	Attempting to
12/15/2016 9:08:33 PM	spid65	Using 'xpsqlb
12/15/2016 9:08:33 PM	spid65	Attempting to
12/15/2016 9:03:03 PM	Server	Software Usa
12/15/2016 9:02:36 PM	spid16s	Service Broke
12/15/2016 9:02:36 PM	spid5s	Recovery is c
12/15/2016 9:02:36 PM	spid15s	CHECKDB fo
12/15/2016 9:02:36 PM	spid16s	The Databas
12/15/2016 9:02:36 PM	spid16s	The Service I
12/15/2016 9:02:35 PM	spid6s	Starting up da
12/15/2016 9:02:35 PM	spid13s	0 transactions
12/15/2016 9:02:35 PM	spid13s	1 transactions
12/15/2016 9:02:35 PM	spid6s	Clearing temp
12/15/2016 9:02:35 PM	spid6s	Starting up da
12/15/2016 9:02:35 PM	spid15s	Recovery is v
12/15/2016 9:02:35 PM	spid15s	0 transactions

3.2.3.2. Web Server

The CV system uses Oracle WebLogic as its web server in the VA environment. CV does not implement any custom WebLogic error handling or reporting. For more information, please refer to WebLogic Server Error Messages Reference.

3.2.3.3. Application Server

The CV system uses Oracle WebLogic as its application server in the VA environment. CV does not implement any custom WebLogic error handling or reporting. For more information, please refer to the website WebLogic Server Error Messages Reference.

3.2.3.4. Network

The CV web application utilizes the network infrastructure provided by the 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)

The CV Login page requires a VAS user’s VA PIV card and PIN to log in, along with their VistA/CPRS Access and Verify codes. If there is no entry on the authorized user list that matches the VAS user, an “*Access Denied. You are not an authorized user*” message is displayed.

The CV Login page requires a CCP’s user name (e-mail address), and a password. If there is no entry in the CV database that matches the credentials, the message: “*Access Denied. You are not an authorized user*” is displayed.

Other examples of A&A error messages are:

- Smart Card Required: VAS user has not inserted their PIV card
- ActivClient: PIV password entered incorrectly
- Missing Code: User has not entered their credentials
- Invalid Access Code: User entered the incorrect credentials

3.2.3.6. Logical and Physical Descriptions

Refer to the *CV 1.5 System Design Document (SDD)* for detailed information.

3.3. Dependent System(s)

Table 4 lists the external VA systems on which CV depends. It also includes the errors related to each dependent system, and the remedies available to system administrators.

Table 4: CV External Dependent Systems

Other VA System	Related Error(s)	Available Remedies
Site VistA instances	If a particular VistA site is unavailable, CV will display the “Connection Unavailable” row in the widgets as shown in Section 3.1.2.2 Connection Unavailable Errors.	N/A
MVI	Patient search errors, or patient records unavailable.	N/A

3.4. Troubleshooting

Tier 1 troubleshooting for CV users is facilitated by VHA Community Support (VHA Community Support). Tier 2 and 3 support verifies service interruptions reported by users. All Tier 2 and 3 support and troubleshooting is handled directly with the application developers.

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, ending with a fully-operational system.

3.5.1. Restart after Non-Scheduled 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 Section 2.1.1.1 System Start-Up from Emergency Shutdown for guidance.

3.5.2. Restart after Database Restore

Please refer to Section 2.1.1 System Start-up for system start up procedures.

3.5.3. Backout Procedures

Backout procedures vary, depending on the specific release. Please refer to the *CV 1.5 Deployment, Installation, Backout and Rollback Guide*, provided with this release.

3.5.4. Rollback Procedures

Rollback procedures vary, depending on the specific release. Please refer to the *CV Deployment, Installation, Backout and Rollback Guide* provided with this release.

4. Operations and Maintenance Responsibilities

Table 5 represents the operational roles and responsibilities for CV.

Table 5: Responsibility Matrix (Operational Roles and Responsibilities)

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
VHA Community Support	**Tier 1 support for VAS and CCP users**	**N/A**	**vha.communitysupport@va.gov**
Michelle Rowe	Business Owner	512-592-8744	michelle.rowe1@va.gov
Carolina Mosley	Clinical SME	N/A	carolina.mosley@va.gov
VA - CV Project Office	**VA OI&T and VHA Stakeholders**	**N/A**	**N/A**
Cynthia Bias	Program Manager	N/A	cynthia.bias@va.gov
Elizabeth (Betsy) Green	CV Project Manager	504-885-3298	elizabeth.green4@va.gov
VA Authentication Federation Infrastructure (VAAFI) Data Power	**Technical Issues/Support Contacts**	**N/A**	**N/A**
Basavaraj "Raj" Devershetty	VAAFI Lead	813-842-3432	basavaraj.devershetty@va.gov
Courtney Rive	Deputy PM SSOi	757-772-0701	courtney.rive@va.gov
Mayank Acharya	VAAFI	818-804-9928	mayank.acharya@va.gov
AITC EO	**Technical Issues/ Support Contacts**	**N/A**	**N/A**
Tiffiny Roper	EO Project Manager	512-981-4939	tiffiny.roper@va.gov
Kelvin Hicks	EO Release Manager	512-981-4827	kelvin.hicks@va.gov

MVI (VA)	**Technical Issues/ Support Contacts**	**N/A**	**In VA Remedy assigned under: VA - Development - DEV-Person Service**
Jason Boire MVI/VAAFI	Lead Developer/ Architect	O:503-747-6883 C:240-381-6087	jason.boire@va.gov
Danny Reed	MVI point of contact	205-943-2415	danny.reed@va.gov
Cory Chin MVI	MVI point of contact	407-593-1963	cory.chin@va.gov
Vicky Steadman	MVI point of contact	205-943-2381	vicky.steadman@va.gov
Jeff Kemple	SSOi point of contact	913-707-9037	jeffrey.kemple@va.gov
VA Network – Network Security Operations Center (NSOC)	**Technical Issues/Support Contacts**	**855-673-4357 Option 6, then 4** **304-260-6685**	**In VA Remedy assigned under: VA NSOC Business Partner Extranet (BPE) Operations -OR- Network Support Center (NSC) BPE Operations** **VANSOCBPEOperations@va.gov**
Craig Wasson	Triple-I/VA-NSOC	304-262-5226	craig.wasson@va.gov

5. Approval Signatures

Signed: Cynthia L.
Bias 100602
Digitally signed by Cynthia L. Bias 100602
DN: dc=gov, dc=va, o=internal,
ou=people,
0.9.2342.19200300.100.1.1=cynthia.bias
@va.gov, cn=Cynthia L. Bias 100602
Date: 2017.01.12 08:44:16 -05'00'

Cynthia Bias, Program Manager Date

Signed: Fred J Mingo
1110027
Digitally signed by Fred J Mingo 1110027
DN: dc=gov, dc=va, o=internal,
ou=people,
0.9.2342.19200300.100.1.1=fred.mingo@
va.gov, cn=Fred J Mingo 1110027
Date: 2017.01.11 17:29:33 -05'00'

Fred Mingo, Product Owner Date

Signed: Michael J.
Streff 196925
Digitally signed by Michael J. Streff 196925
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=michael.streff@va.
gov, cn=Michael J. Streff 196925
Date: 2017.01.12 08:58:22 -07'00'

Michael Streff, Receiving Organization (Operations Support) Date

6. Appendix A – Acronyms and Abbreviations

Table 6 lists the acronyms and abbreviations used throughout this document, and their descriptions.

Table 6: Acronyms and Abbreviations

Acronym	Definition
A&A	Authentication and Authorization
AES	Advanced Encryption Standard
AITC	Austin Information Technology Center
APM	Application Performance Management
BPE	Business Partner Extranet
CA	Computer Associates
CCP	Community Care Provider
CPRS	Computerized Patient Record System
CV	Community Viewer
DEK	Database Encryption Key
DES	Data Exchange Service
DoS	Denial of Service
EHR	Electronic Health Record
EO	Enterprise Operations
GTM	Global Traffic Managers
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HRG	HRG Technologies LLC
ICN	Integration Control Number
ID	Identification
IT	Information Technology
MitM	Man in the Middle
MS	Microsoft
MVI	Master Veteran Index
NSC	Network Support Center
NSOC	Network Security Operations Center
OI&T	Office of Information and Technology
PHI	Protected Health Information

Acronym	Definition
PII	Personally Identifiable Information
PIN	Personal Identification Number
PITC	Philadelphia Information Technology Center
PIV	Personal Identity Verification
POM	Production Operations Manual
QoS	Quality of Service
SDD	System Design Document
SQL	Structured Query Language
SSL	Secure Sockets Layer
TDE	Transparent Data Encryption
TLS	Transport Layer Security
TPA	Third Party Administrator
URL	Uniform Resource Locator
VA	Department of Veterans Affairs
VAS	VA Administrative Staff
VAAFI	VA Authentication Federation Infrastructure
VHA	Veterans Health Administration
VistA	Veterans Information Systems and Technology Architecture
VM	Virtual Machine
XML	Extensible Markup Language