Joint Legacy Viewer (JLV) 2.5.2

Production Operations Manual (POM)

April 2017

Version 1.3

Department of Veterans Affairs

Revision History

Date	Version	Description	Author
04/04/2017	1.3	Final comments addressed, document approved.	AbleVets
03/30/2017	1.2	Resubmitted with client comments addressed	AbleVets
03/16/2017	1.1	Resubmitted with client comments addressed	AbleVets
02/20/2017	1.0	Draft submitted for review	AbleVets
01/15/2017	0.1	Initial draft of artifact	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

Table of Figures

Table of Tables

1. Introduction

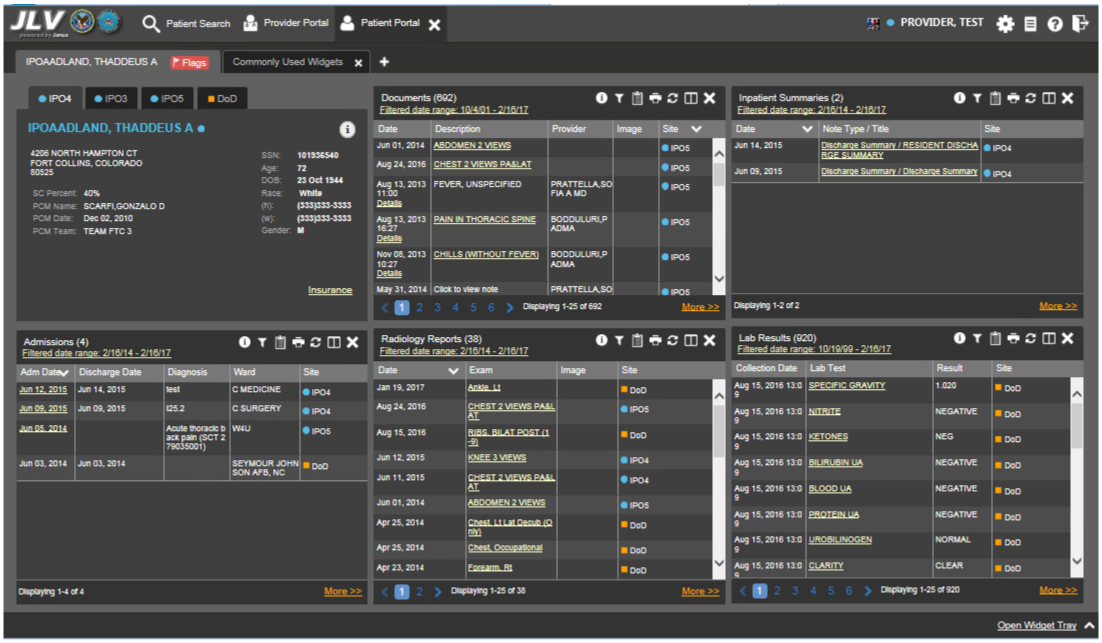
JLV is a centrally hosted, java-based web application that is managed as a single code baseline, and deployed in separate Department of Defense (DoD) and Department of Veteran Affairs (VA) environments. JLV is a browser-based, graphical user interface (GUI) that provides an integrated, read-only view of Electronic Health Record (EHR) data from the DoD, VA, and Virtual Lifetime Electronic Record (VLER) eHealth Exchange (eHX) partners, within a single application.

The JLV GUI retrieves and displays clinical data from a number of native data sources and systems. The data is then presented to the user in a simple to use, web-based interface, through widgets. Each widget corresponds to a clinical data domain. JLV eliminates the need for VA and DoD clinicians to access separate, disparate viewers. Born from a joint DoD-VA venture called JANUS, JLV was directed by the Secretary of Defense and Secretary of Veterans Affairs in early 2013 to further support interoperability between the two departments.

JLV users can create and personalize tabs, drag and drop widgets onto tabs, sort data within a widget's columns, set date filters, and expand a widget for a detailed view of patient information. Within each widget, a circular, blue icon indicates the data retrieved is from a VA source; a square orange icon indicates that the data retrieved is from a DoD source; and a hexagonal, purple icon indicates data that the data retrieved is from VA VLER partners.

Figure 1 depicts the primary JLV Patient Portal, which is comprised of several widgets (viewers) that retrieve clinical data from sources in real time, displaying them in a unified, chronological view.

Figure 1: Sample of the JLV Patient Portal Page



IPOAADLAND, THADDEUS A ●

4206 NORTH HAMPTON CT
FORT COLLINS, COLORADO
80525

SC Percent: 40%
PCM Name: SCARFI,GONZALO D
PCM Date: Dec 02, 2010
PCM Team: TEAM FTC 3

SSN: 101936540
Age: 72
DOB: 23 Oct 1944
Race: White
(h): (333)333-3333
(w): (333)333-3333
Gender: M

Documents (692)
Filtered date range: 10/4/01 - 2/16/17

Date	Description	Provider	Image	Site
Jun 01, 2014	ABDOMEN 2 VIEWS			● IPO5
Aug 24, 2016	CHEST 2 VIEWS PA&LAT			● IPO5
Aug 13, 2013 11:00 Details	FEVER, UNSPECIFIED	PRATTELLA,SOFIA A MD		● IPO5
Aug 13, 2013 16:27 Details	PAIN IN THORACIC SPINE	BODDULURI,PADMA		● IPO5
Nov 08, 2013 10:27 Details	CHILLS (WITHOUT FEVER)	BODDULURI,PADMA		● IPO5
May 31, 2014	Click to view note	PRATTELLA,SO		● IPO5

1 2 3 4 5 6 Displaying 1-25 of 692

Inpatient Summaries (2)
Filtered date range: 2/16/14 - 2/16/17

Date	Note Type / Title	Site
Jun 14, 2015	Discharge Summary / RESIDENT DISCHARGE SUMMARY	● IPO4
Jun 09, 2015	Discharge Summary / Discharge Summary	● IPO4

Displaying 1-2 of 2

Admissions (4)
Filtered date range: 2/16/14 - 2/16/17

Adm Date	Discharge Date	Diagnosis	Ward	Site
Jun 12, 2015	Jun 14, 2015	test	C MEDICINE	● IPO4
Jun 09, 2015	Jun 09, 2015	I25.2	C SURGERY	● IPO4
Jun 05, 2014		Acute thoracic back pain (SCT 279035001)	W4U	● IPO5
Jun 03, 2014	Jun 03, 2014		SEYMOUR JOHNSON AFB, NC	■ DoD

Displaying 1-4 of 4

Radiology Reports (38)
Filtered date range: 2/16/14 - 2/16/17

Date	Exam	Image	Site
Jan 19, 2017	Ankle, Lt		■ DoD
Aug 24, 2016	CHEST 2 VIEWS PA&LAT		● IPO5
Aug 15, 2016	RIBS, BILAT POST (1-9)		■ DoD
Jun 12, 2015	KNEE 3 VIEWS		● IPO4
Jun 11, 2015	CHEST 2 VIEWS PA&LAT		● IPO4
Jun 01, 2014	ABDOMEN 2 VIEWS		● IPO5
Apr 25, 2014	Chest, Lt Lat Decub (Only)		■ DoD
Apr 25, 2014	Chest, Occupational		■ DoD
Apr 23, 2014	Forearm, Rt		■ DoD

1 2 Displaying 1-25 of 38

Lab Results (920)
Filtered date range: 10/19/99 - 2/16/17

Collection Date	Lab Test	Result	Site
Aug 15, 2016 13:09	SPECIFIC GRAVITY	1.020	■ DoD
Aug 15, 2016 13:09	NITRITE	NEGATIVE	■ DoD
Aug 15, 2016 13:09	KETONES	NEG	■ DoD
Aug 15, 2016 13:09	BILIRUBIN UA	NEGATIVE	■ DoD
Aug 15, 2016 13:09	BLOOD UA	NEGATIVE	■ DoD
Aug 15, 2016 13:09	PROTEIN UA	NEGATIVE	■ DoD
Aug 15, 2016 13:09	UROBILINOGEN	NORMAL	■ DoD
Aug 15, 2016 13:09	CLARITY	CLEAR	■ DoD

1 2 3 4 5 6 Displaying 1-25 of 920

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

2.1.1. System Startup

1. Start the JLV database (DB) servers in AITC.
   - The database server processes are configured to run as system services and automatically start with the server itself. Their successful startup is verified in a below step.
2. Start the JLV VistADataService servers in AITC.
   - The service processes are configured to run as system services and automatically start with the server itself. Their successful startup is verified in a below step.
3. Start the JLV jMeadows servers in AITC.
   - The service processes are configured to run as system services and automatically start with the server itself. Their successful startup is verified in a below step.
4. Start the JLV web application servers in AITC.
   - The service processes are configured to run as system services and automatically start with the server itself. Their successful startup is verified in a below step.
5. Repeat steps 1-4 above for the servers in PITC.
6. Enterprise Operations (EO) manages the Global Traffic Managers (GTM). Startup steps for those devices are therefore out of the scope of this document.
7. User launches the JLV Universal Resource Locator (URL) in a web browser.
8. VA Users are required to authenticate through the VA SSOi system.
9. If the user is in the whitelist; the JLV Login page is presented.
10. Verify that the JLV login page displays and indicates that system status is normal.

2.1.1.1. System Startup from Emergency Shutdown

In case of a power outage, or other abrupt termination of the server operating systems, start up the servers as detailed in Section 2.1.1, System Startup, and allow the operating system to check the disks for corruption. Consult with EO to ensure that the database successfully recovers.

2.1.2. System Shutdown

NOTE: To avoid issues with in-progress transactions, this procedure should be performed during a published maintenance window, when there are few users accessing the system. Table 1 lists the AITC and PITC Servers.

1. Shut down the WebLogic services on the JLV web application servers in AITC.
2. Shut down the JLV web application servers in AITC.

3. Shut down the WebLogic services on the jMeadows servers in AITC.
4. Shut down the jMeadows servers in AITC.
5. Shut down the WebLogic on the VistADataService servers in AITC.
6. Shut down the VistADataService servers in AITC.
7. Shut down the database servers in AITC.
8. Repeat steps 1-7 above for the servers in PITC.

Table 1: AITC and PITC Servers

JLV System Component	AITC Servers	PITC Servers
Web Application	VAAUSJLVWEB201	VAPHIJLVWEB201
	VAAUSJLVWEB202	VAPHIJLVWEB202
	VAAUSJLVWEB203	VAPHIJLVWEB203
	VAAUSJLVWEB204	VAPHIJLVWEB204
VistA Data Service	VAAUSJLVWEB205	VAPHIJLVWEB205
	VAAUSJLVWEB206	VAPHIJLVWEB206
	VAAUSJLVWEB207	VAPHIJLVWEB207
	VAAUSJLVWEB208	VAPHIJLVWEB208
jMeadows Data Service JLV Print Service JLV Quality of Service (QoS)	VAAUSJLVWEB209	VAPHIJLVWEB209
	VAAUSJLVWEB210	VAPHIJLVWEB210
	VAAUSJLVWEB211	VAPHIJLVWEB211
	VAAUSJLVWEB212	VAPHIJLVWEB212
Database	VAAUSJLVSQL202	VAPHIJLVSQL202
	VAAUSSQLJLV405	VAPHISQLJLV405

2.1.2.1. Emergency System Shutdown

Shut down all servers (JLV web application, jMeadows, VistADataService, and database) in AITC and PITC, in any order.

2.1.3. Backup and Restore

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

This is a guide to recover the JLV and JLV_ Transparent Data Encryption (TDE) databases from an existing backup (.bak) file. Production systems are currently configured to back up both databases, JLV and JLV_TDE, on a daily basis.

Under the full or bulk-logged recovery model, before a database can be restored in SQL Server Management Studio, the active transaction log (known as the tail of the log) must be backed up. To restore a database that is encrypted, access to the certificate or asymmetric key used to encrypt the database is needed. Without the certificate or asymmetric key, the database cannot be restored. As a result, the certificate used to encrypt the database encryption key must be retained as long as the backup is needed. JLV System Administrators maintain local and offline backups of the database keys.

2.1.3.1. Backup Procedures

Backups for both databases, JLV and JLV_TDE, are configured to run, automatically, on a daily basis.

2.1.3.2. Restore Procedures

Pre-requisites to recover databases:

- Database backup (.bak) file for the JLV and JLV_ TDE databases.
- Backup of encryption keys for JLV_TDE 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 on '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 JLV 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 restore (JLV).
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 on 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, you can 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.
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/PITC Systems Administrators.
   b. Backups are taken daily.
   c. Testing of those backups are done by EO.
   d. Validation of these restoration to be confirmed by:
      - Validating all software/configurations are restored from the expected configuration.
      - Configuration files contain server specific settings.
      - Application server starts as expected, validated through logs and through smoke test of application.
2. Database
   a. Backups are taken daily.
   b. Backups are restored to backup database servers (vaausjlvsql202, vaphijlvsql202) to test restore procedures and integrity of the backup files. The testing of the database restoration process is performed once every quarter and/or during each deployment of the JLV application.
   c. Administrators to validate that data in the database contains up-to-date entries for whitelist, user profiles, and audit logging.
   d. Validation of operations is confirmed through smoke test of applications.

2.1.3.4. Storage and Rotation

The JLV Support team, comprised Systems/Network/Security Engineers and Systems Administrators from team AbleVets, ensures the system and storage arrays for the system are operating properly, with daily inspections of JLV QoS logs, system notifications, and frequent systems checks.

2.2. Security/Identity Management

The JLV system restricts access to the JLV GUI to authorized users within the VA and DoD enterprise. There is an authorized user table within the JLV database that lists VA users and their associated @va.gov e-mail addresses known as the whitelist.

VA users are required to authenticate through the VA Single Sign On Interface (SSOi) system. JLV receives the user’s email address from SSOi to validate the user against the whitelist of authorized users stored in the JLV database. If the user is in the whitelist, the JLV log in page is presented.

After reaching the JLV log in page, JLV requires that VA users provide the following credentials:

- **For Veterans Health Administration (VHA)/Clinical Users:** The user’s local existing Veterans Information Systems and Technology Architecture (VistA)/Computerized Patient Record System (CPRS) Access and Verify codes

- **For Veterans Benefits Administration (VBA)/Benefits Users:** The user’s existing VistA/Compensation and Pension Records Interchange (CAPRI) Access and Verify codes.

When the user’s email is not found in the JLV whitelist, the user is presented a unique page with the message, *Access denied. You are not an authorized user.* For this user, the log in process stops and no further options are presented.

Access control and authentication takes place before JLV interfaces with jMeadows. The user is authenticated to his/her host EHR system, granting the user access to the presentation layer. Based on user credentials, jMeadows retrieves the user’s profile information from the JLV database. The user’s default host location, custom widget layout, and other user data are returned. See Section 2.2.2, Access Control, for more information.

A detailed overview of the access an log in process, from the user’s perspective, can be found in the *Joint Legacy Viewer (JLV) 2.5.2 User Guide*. Once approved, all referenced documentation is available on the Technical Services Project Repository (TSPR)[1].

2.2.1. Identity Management

To add a user:

- VA support staff provides user name to be added
- Log on to VA machine - VA network
- Navigate to Remote Desktop Connection
- Log on to AITC DB
- Open Microsoft SQL Server Management Studio
- Once connected to the DB, navigate to the Libraries folder
  - Locate the JLV_SQLQueries folder
  - Click and open the Script for Daily Tracker
  - Query the AUTH_USER table for user count prior to import
  - Properly format the approved user list before queuing it on the DB
  - Execute the script to import users
  - Query the AUTH_USER table for users count after import, verify the correct number of users have been added to the DB
- Once the user(s) have been added to the DB, navigate to SharePoint
- Activate and update the user(s)
  - Once the user(s) have been activated and updated in SharePoint
  - Check the Tracker back in
- JLV team notifies VA support staff

[1] **NOTE:** Access to TSPR is restricted, and must be requested.

To remove a user:

- VA support staff provides the name(s) to remove
- Log on to VA machine - VA network
- Navigate to Remote Desktop Connection
- Log on to AITC DB
    - Open Microsoft SQL Server Management Studio
    - Once connected to the DB, navigate to the Libraries folder
- Locate the JLV_SQLQueries folder
    - Search for the JLV user(s) to be deleted
    - Delete the user(s)
    - Update the VHA Whitelist Tracker file for record
- JLV team notifies VA support staff

To update a user:

- VA support staff provides name(s) to update
- Log on to VA machine - VA network
- Navigate to Remote Desktop Connection
- Log on to AITC DB
    - Open Microsoft SQL Server Management Studio
    - Once you are connected to the DB, navigate to the Libraries folder
- Locate the JLV_SQLQueries folder
    - Search for the JLV user(s) to be updated
    - Update the user(s)
    - Update the internal file for record
- JLV team notifies VA support staff

2.2.2. Access control

JLV access control for VA users consists of two checks:

- JLV validates the VA user's e-mail address, retrieved from SSOi, against the JLV database. When the user's e-mail address is found in the whitelist, the JLV log in page is presented to the user.
    - If the user's e-mail is not found in the JLV database, the user is presented with a unique page that displays the message, *Access denied. You are not an authorized user*. For this user, the log in process stops and no further options are presented.
- JLV validates the user's Access/Verify Codes entered on the JLV log in page against the local host site before the user is allowed access to the JLV web application.
    - If the user's Access/Verify Codes are invalid, they are returned to the log in page, and an *Invalid Access/Verify Codes* error message is presented above the fields.

Table 2 summarizes the JLV system components, and the settings utilized in the access control implementation.

Table 2: Access Control Design

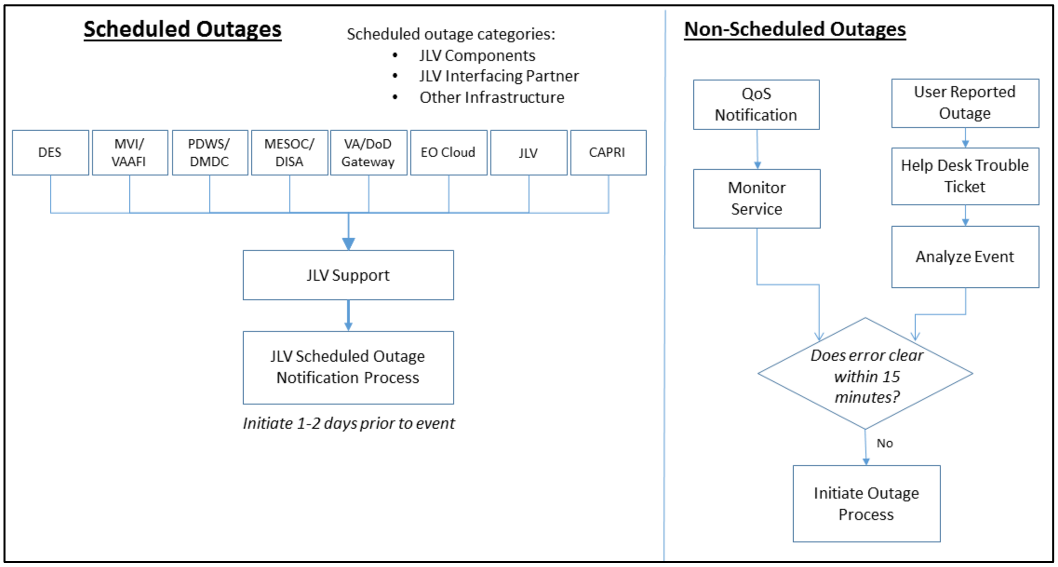
Component	Description
Database table	The AUTH_USER table within the JLV database contains field elements with user identifiers.
Database script	A database script is used for the initial upload and future updates to the AUTH_USER table.
Configuration settings	A configuration setting within the appconfig-production.properties file enable access control: • Enable VA Access Control, On/Off - This setting enables access control for VA users.

2.3. User Notifications

User notifications follow the JLV downtime notification and outage triage process.

Figure 2 depicts the JLV process for monitoring, analyzing, and initiating the notification or outage.

Figure 2: Scheduled Downtime and Non-Scheduled Outage Overview



2.3.1. User Notification Points of Contact

Table 3 shows the current notification distribution list for alerting for VA stakeholders of JLV scheduled downtime. The list is maintained by the JLV Support team.

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

Name	Organization	Email Address
Bose, Mary Ellen	VA- Government	maryellen.bose@va.gov
Cardenas, Michael	HRG	mcardenas@hawaiirg.com
Cournoyer, Amanda	VA-Government	amanda.cournoyer@va.gov
Facundus, Latricia R.	VA-Government	latricia.facundus@va.gov
Flemming, Mitch	SBG	mflemming@sbgts.com
Goo, Brad	HRG	bgoo@hawaiirg.com
Green, Betsy	VA-Government	elizabeth.green4@va.gov
Guebert, Chad	AbleVets (JLV PM)	chad.guebert@ablevets.com
Guebert, Crista	HRG	cguebert@hawaiirg.com
Hines, Rick	VA-Government	rick.hines@va.gov
Lukens, Rich	AbleVets	rich.lukens@ablevets.com
McNamee, Shane	VA-Government	shane.mcnamee@va.gov
O’Brien, Mark	AbleVets	mark.obrien@ablevets.com
Odle, Phillip	VA-Government	phillip.odle@va.gov
Omizo, Reese K.	VA-Government	reese.omizo@va.gov
Ortman, Joseph	VA-Government	joseph.ortman@va.gov
Roberts, Jerilyn	VA-Government	jerilyn.roberts1@va.gov
Rutherford, Jerald	VA-Government	jerald.rutherford@va.gov
Sanchez, Gene W.	SMS	gene.sanchez@va.gov
Southerland, John B.	SMS	john.southerland@va.gov
Suenaga, Greg	HRG	gsuenaga@hawaiirg.com
Wiebe, Rachel S	VA-Government	rachel.wiebe@va.gov

2.4. System Monitoring, Reporting and Tools

The JLV system traces and audits actions that a user executes within the application. JLV audits are provided through audit trails and audit logs that offer a back-end view of system use, in addition to storing user views of patient data. Audit trails and logs record key activities (date and time of event, patient identifiers, user identifiers, type of action, and access location) to show system threads of access, and views of patient records. Refer to Section 3.2.1, Application Error Logs, for more information on audit and server logs.

The JLV QoS service monitors the availability of data sources. Refer to Section 2.4.2, Availability Monitoring.

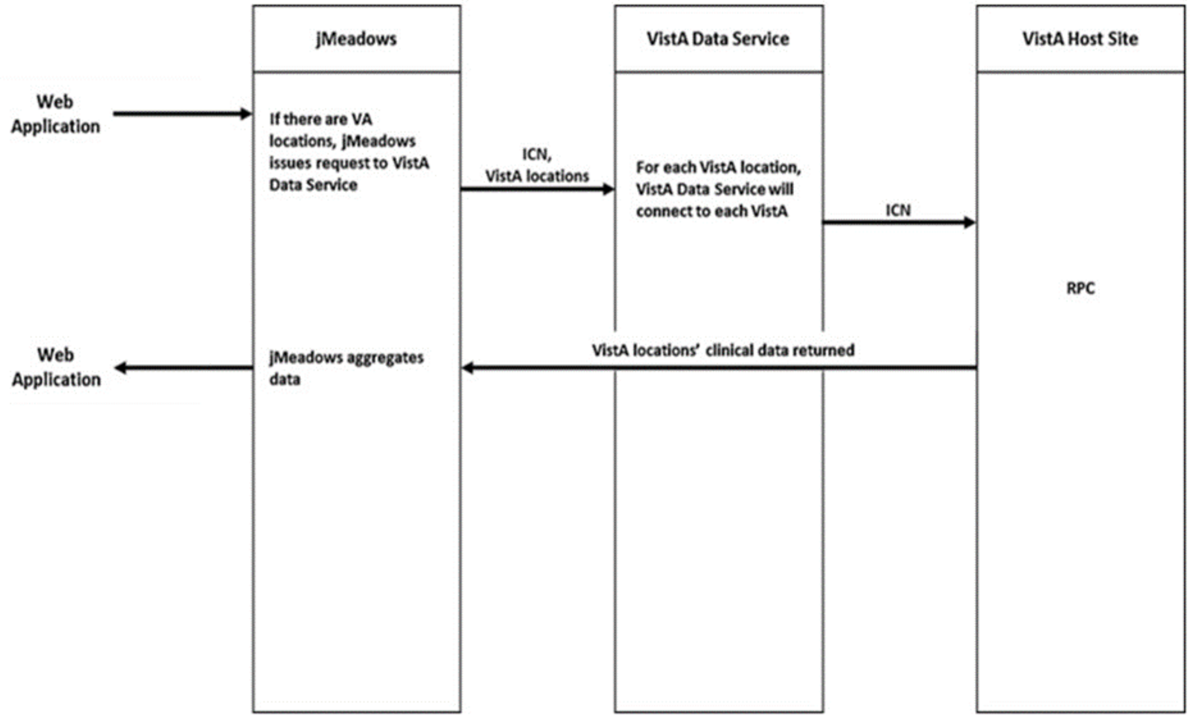
2.4.1. Dataflow Diagram

The data retrieval sequence, depicted in Figure 3, 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 VDS 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 connects to each VistA, and return the clinical data to jMeadows.
3. jMeadows aggregates the data and returns the data to JLV web application.

Figure 3: Data Retrieval from VA Systems

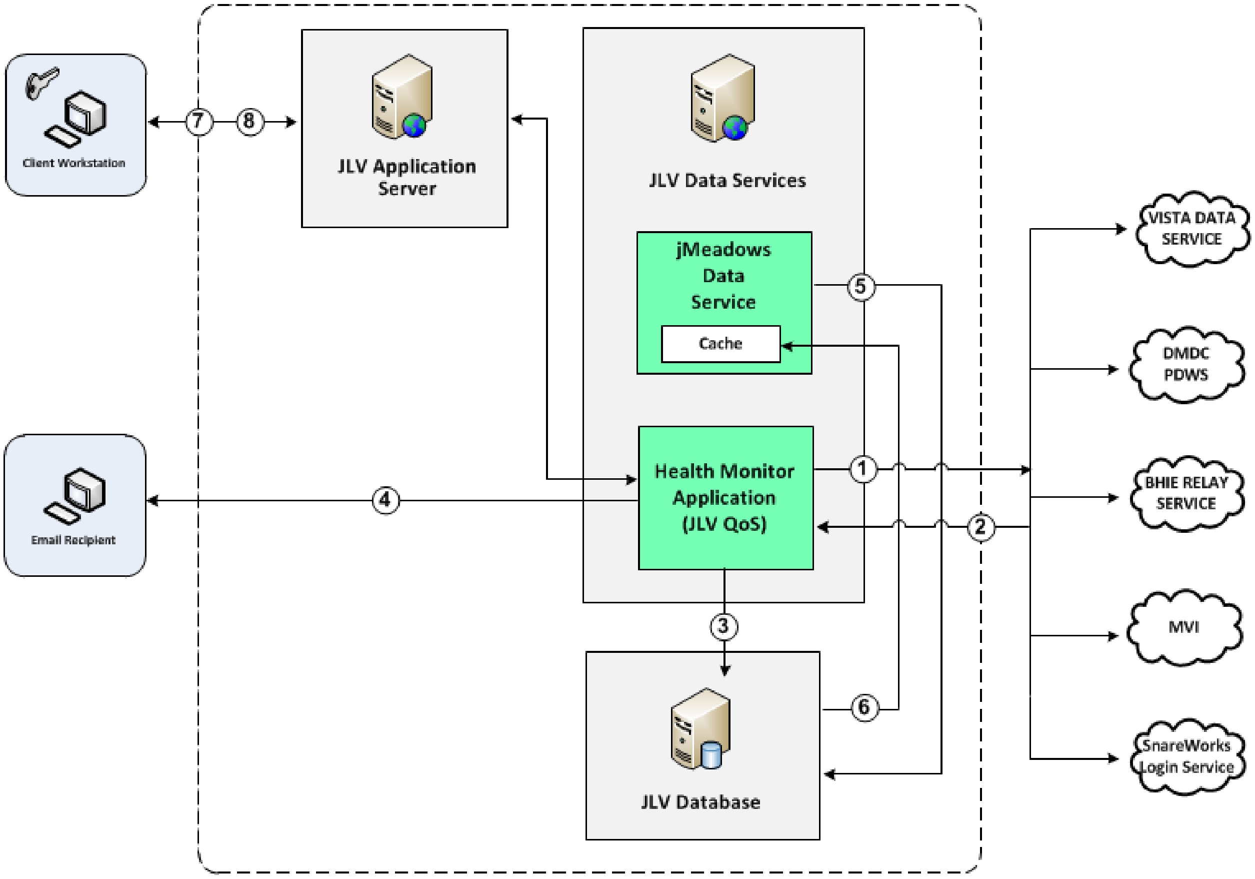

jMeadows
VistA Data Service
VistA Host Site
Web Application
If there are VA locations, jMeadows issues request to VistA Data Service
ICN, VistA locations
For each VistA location, VistA Data Service will connect to each VistA
ICN
RPC
Web Application
jMeadows aggregates data
VistA locations' clinical data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

2.4.2. Availability Monitoring

The QoS monitors the health of the JLV application. QoS checks for the availability or disruption of dependent services within the systems in the DoD and/or in the VA environments. The services monitored by the JLV QoS Service are:

- Master Veteran Index (MVI)
- Defense Manpower Data Center (DMDC) Patient Discovery Web Service (PDWS)
- Relay Service (DoD data retrieval)
- SnareWorks Login Service (DoD user authentication)
- VistA Data Service
- jMeadows Data Service

Figure 4: System Status Check Sequence



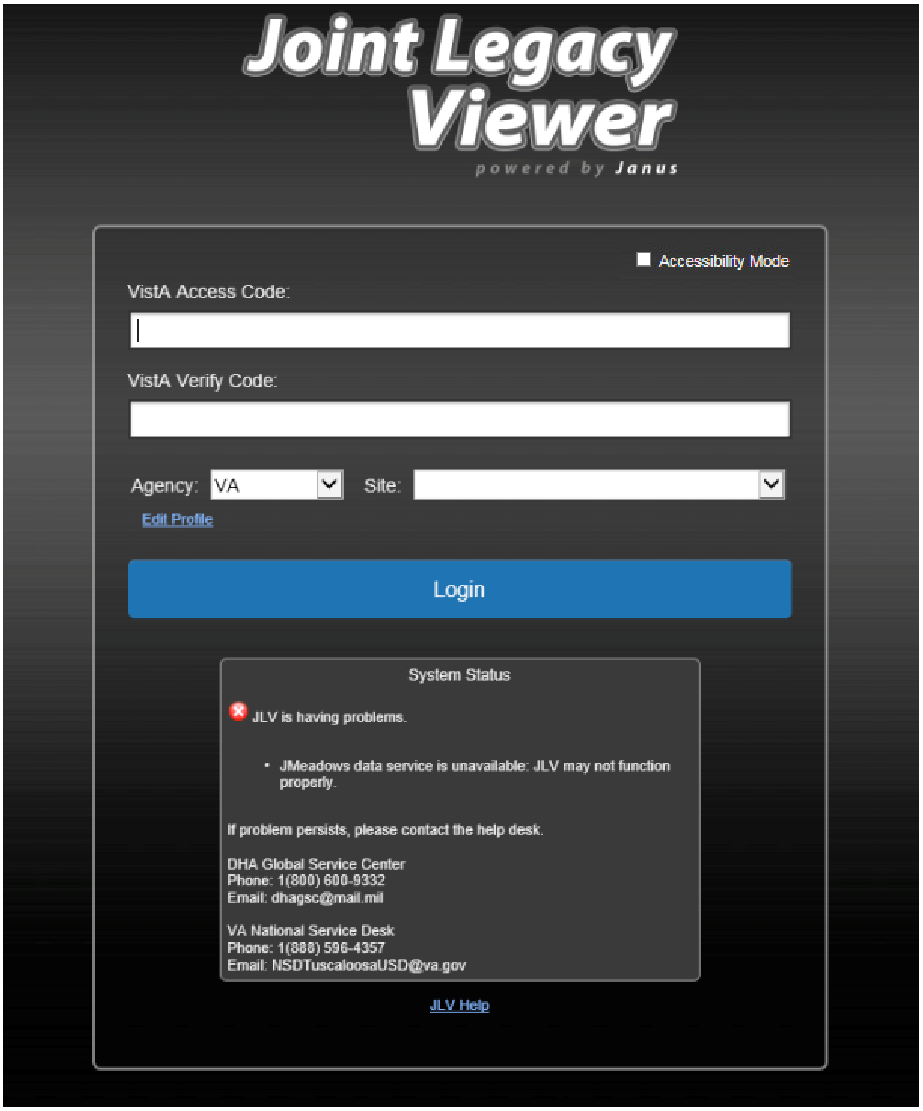
System status checks are performed as follows:

1. The Health Monitor pings the monitored services every five minutes.
2. The Health Monitor receives a system status from each monitored service.
3. System status events are written to the QOS_LOGS table, within the JLV database.
4. The Health Monitor sends an automated e-mail notification every 12 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the twelve-hour timer is reset. The next e-mail is generated after twelve hours, if no further system status changes are detected.
5. The jMeadows Data Service pings the JLV database every two minutes for status checks.
6. The jMeadows Data Service stores the data returned from the JLV database in an internal cache, the jMeadows Data Service cache.
7. When a user accesses the JLV log in page, the JLV application requests and receives system status data from the jMeadows Data Service cache.
8. During active user sessions, the JLV application requests system status data from the jMeadows Data Service cache every five minutes. Current system status is retrieved from the cache, and sent to the JLV GUI.

A diagram of the system status check sequence can be seen in Figure 4.

Figure 5 provides an example of a system status message on the JLV log in page.

Figure 5: Sample System Status Message on the JLV Login Page



☐ Accessibility Mode

VistA Access Code:

VistA Verify Code:

Agency: VA Site:

System Status

JLV is having problems.

- JMeadows data service is unavailable: JLV may not function properly.

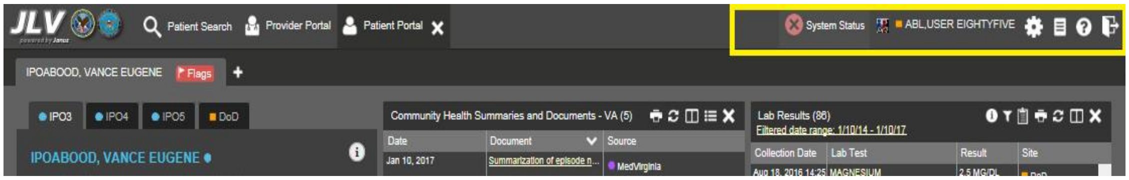
If problem persists, please contact the help desk.

DHA Global Service Center
Phone: 1(800) 600-9332
Email: dhagsc@mail.mil

VA National Service Desk
Phone: 1(888) 596-4357
Email: NSDTuscaloosaUSD@va.gov

Figure 6 provides an example system error status displayed on the JLV Patient Portal page, presented only if the system status is yellow or red. If the system does not detect a service connection error, no notice is displayed.

Figure 6: Sample System Status Message on the Patient Portal Page



2.4.2.1. Domain Level Availability Monitoring

JLV includes interface status icons on the toolbar of multiple Patient Portal widgets that display the status of the data source for each widget's clinical domain.

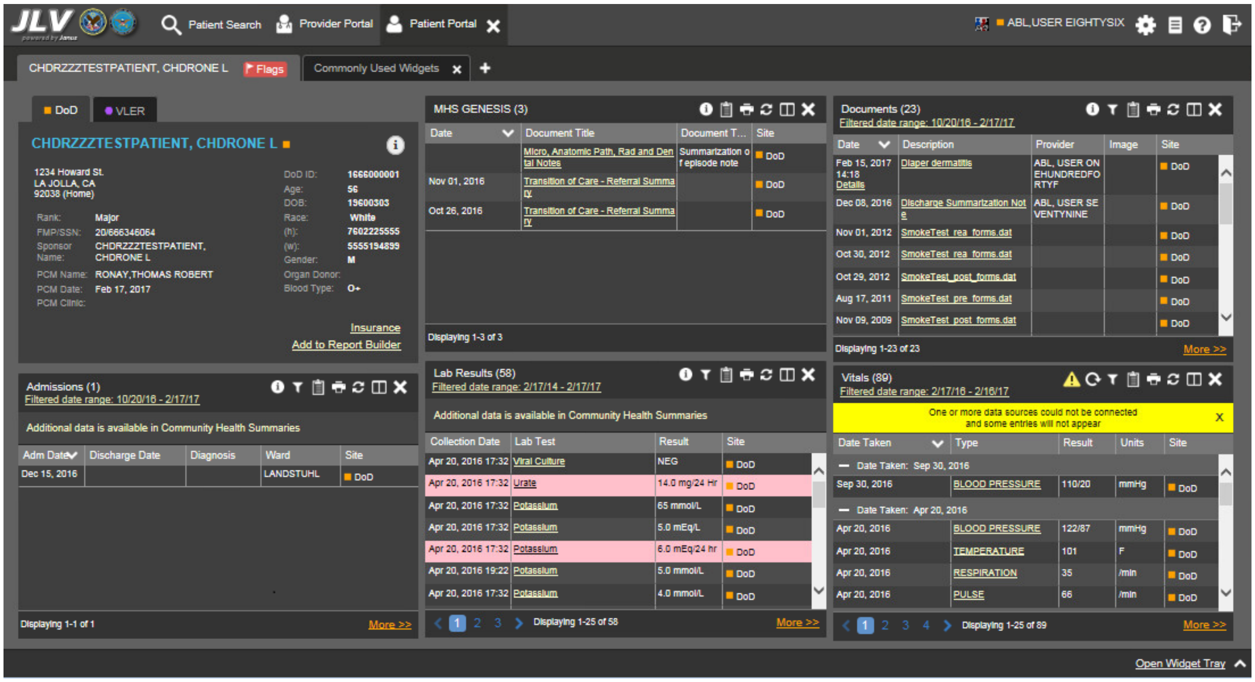
There are two conditions:

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

A yellow banner (Figure 7) is displayed over a widget when one or more sources are unavailable, indicating that a connection to the data source could not be made, and some records may not appear.

Both icons are used to provide status for DoD, VA, and community partner data sources. Clicking either status icon opens the interface status details in a separate window, as seen in Figure 8. Interface status details opened from within a widget shows the connection status at the domain level.

Figure 7: Sample Interface Status Notification (Yellow Banner)



CHDRZZZTESTPATIENT, CHDRONE L

1234 Howard St.
LA JOLLA, CA
92038 (Home)

Rank:	Major	DoD ID:	1666000001
FMP/SSN:	20/666346064	Age:	56
Sponsor Name:	CHDRZZZTESTPATIENT, CHDRONE L	DOB:	19600303
PCM Name:	RONAY,THOMAS ROBERT	Race:	White
PCM Date:	Feb 17, 2017	(h):	7602225555
PCM Clinic:		(w):	5555194899
		Gender:	M
		Organ Donor:	
		Blood Type:	O+

Insurance
Add to Report Builder

Admissions (1)
Filtered date range: 10/20/16 - 2/17/17

Additional data is available in Community Health Summaries

Adm Date	Discharge Date	Diagnosis	Ward	Site
Dec 15, 2016			LANDSTUHL	DoD

Displaying 1-1 of 1 More >>

MHS GENESIS (3)

Date	Document Title	Document T...	Site
	Micro, Anatomic Path, Rad and Dental Notes	Summarization of episode note	DoD
Nov 01, 2016	Transition of Care - Referral Summary		DoD
Oct 26, 2016	Transition of Care - Referral Summary		DoD

Displaying 1-3 of 3

Lab Results (58)
Filtered date range: 2/17/14 - 2/17/17

Additional data is available in Community Health Summaries

Collection Date	Lab Test	Result	Site
Apr 20, 2016 17:32	Viral Culture	NEG	DoD
Apr 20, 2016 17:32	Urate	14.0 mg/24 Hr	DoD
Apr 20, 2016 17:32	Potassium	65 mmol/L	DoD
Apr 20, 2016 17:32	Potassium	5.0 mEq/L	DoD
Apr 20, 2016 17:32	Potassium	6.0 mEq/24 hr	DoD
Apr 20, 2016 19:22	Potassium	5.0 mmol/L	DoD
Apr 20, 2016 17:32	Potassium	4.0 mmol/L	DoD

1 2 3 Displaying 1-25 of 58 More >>

Documents (23)
Filtered date range: 10/20/16 - 2/17/17

Date	Description	Provider	Image	Site
Feb 15, 2017 14:18 Details	Diaper dermatitis	ABL, USER ONEHUNDREDFORTYF		DoD
Dec 08, 2016	Discharge Summarization Note	ABL, USER SEVENTYNINE		DoD
Nov 01, 2012	SmokeTest_rea_forms.dat			DoD
Oct 30, 2012	SmokeTest_rea_forms.dat			DoD
Oct 29, 2012	SmokeTest_post_forms.dat			DoD
Aug 17, 2011	SmokeTest_pre_forms.dat			DoD
Nov 09, 2009	SmokeTest_post_forms.dat			DoD

Displaying 1-23 of 23 More >>

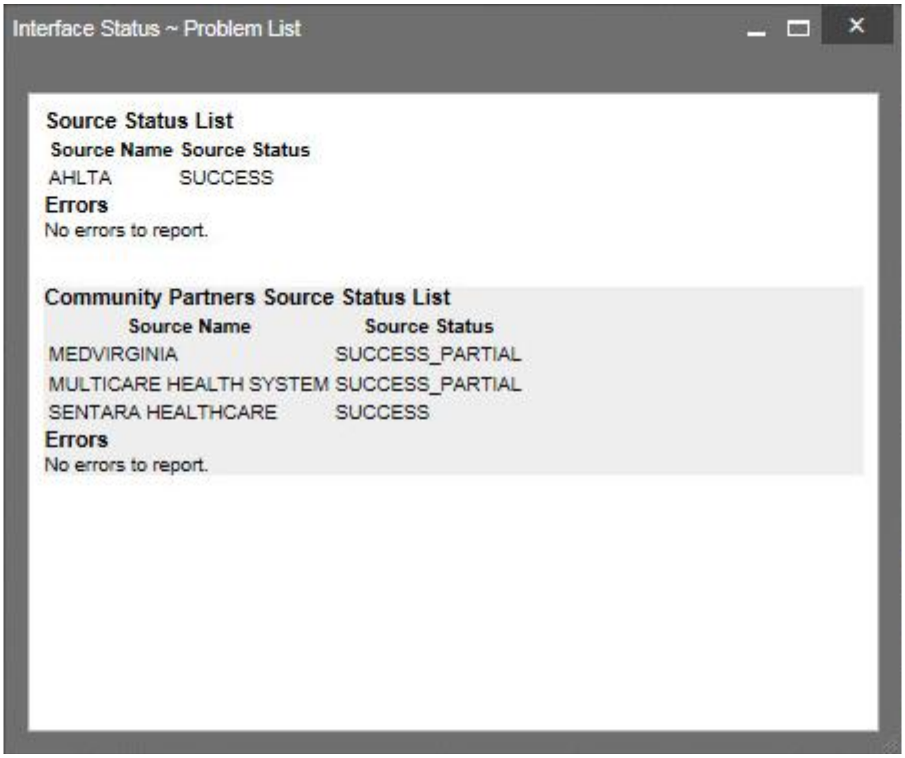
Vitals (89)
Filtered date range: 2/17/16 - 2/16/17

One or more data sources could not be connected
and some entries will not appear X

Date Taken	Type	Result	Units	Site
— Date Taken: Sep 30, 2016				
Sep 30, 2016	BLOOD PRESSURE	110/20	mmHg	DoD
— Date Taken: Apr 20, 2016				
Apr 20, 2016	BLOOD PRESSURE	122/87	mmHg	DoD
Apr 20, 2016	TEMPERATURE	101	F	DoD
Apr 20, 2016	RESPIRATION	35	/min	DoD
Apr 20, 2016	PULSE	66	/min	DoD

1 2 3 4 Displaying 1-25 of 89 More >>

Figure 8: Sample Interface Status Details



Interface Status ~ Problem List

Source Status List

Source Name	Source Status
AHLTA	SUCCESS

Errors

No errors to report.

Community Partners Source Status List

Source Name	Source Status
MEDVIRGINIA	SUCCESS_PARTIAL
MULTICARE HEALTH SYSTEM	SUCCESS_PARTIAL
SENTARA HEALTHCARE	SUCCESS

Errors

No errors to report.

2.4.3. Performance/Capacity Monitoring

Query times for each web service call into the Relay Service, jMeadows, and VistA Data Service are recorded to a file in the D:\Log directory on the server, where the services are installed. Refer to Section 3.2.1, Application Error Logs, for more information on audit and server logs.

2.4.4. Critical Metrics

- **VA providers, VHA users, or VBA users accessing a DoD-only patient (i.e., no VA identifiers for a patient):** JLV records each access of Protected Health Information (PHI) through JLV. This includes the identification of the individual whose PHI was accessed, the identification of the user who accessed the information, and identification of the specific PHI accessed.
- **User access to sensitive DoD data:** DoD and VA users are audited each time a sensitive DoD record (domains: sensitive notes, outpatient encounters, and labs) is viewed, regardless of how many times the user has previously viewed it, including viewing multiple times in the same user session. When a user accesses and closes the sensitive record, then re-opens the same record and views it a second time, the user is asked to agree to be audited again.

The following information is captured for each attempt to access DoD sensitive data, whether successful or unsuccessful:

- Organization (i.e., VHA, VBA, DoD)
- User name

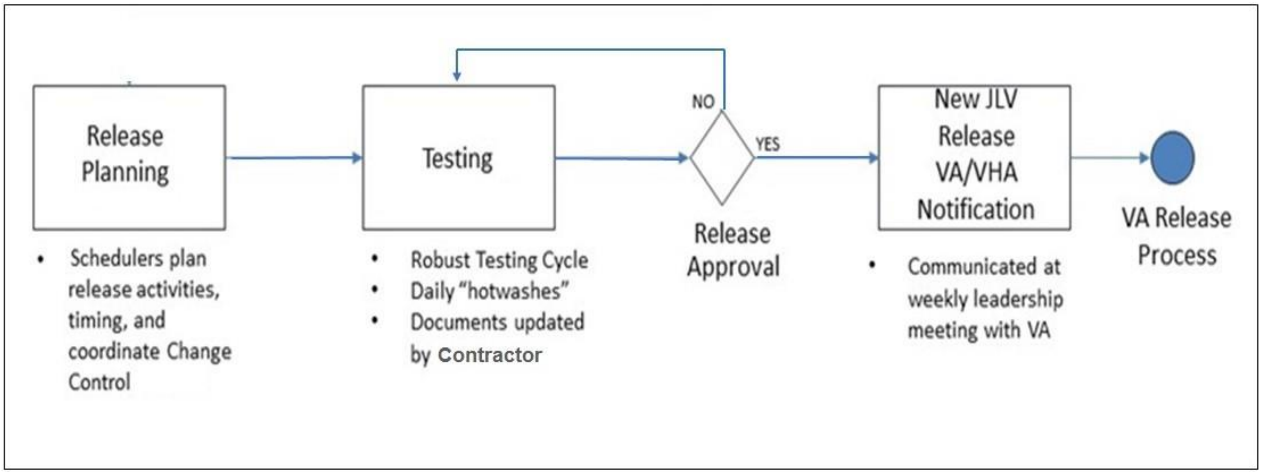
- User Social Security Number (SSN)
- User PIV (if known for VA users)
- User Location
- Patient Last Name, First Name, Middle Initial (MI), SSN, MVI, Date of Birth (DOB)
- Sensitive data accessed, e.g., unique note identifier
- Date/Time of access
- Reason for access, e.g., Emergent Care, Clinical Care, or Authorized Administrative Use

2.5. Routine Updates, Extracts and Purges

2.5.1. Routine Updates

Patches and other routine updates follow the JLV patching process as shown in Figure 9.

Figure 9: Patching Process for VA and DoD Components


Release Planning
• Schedulers plan release activities, timing, and coordinate Change Control
Testing
• Robust Testing Cycle
• Daily "hotwashes"
• Documents updated by Contractor
NO
YES
Release Approval
New JLV Release VA/VHA Notification
• Communicated at weekly leadership meeting with VA
VA Release Process

2.5.2. Extracts

Extracts of JLV audit logs and server logs are available on an as-needed basis, and by request only. 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 send it to the requestor, via an encrypted method. Refer to Section 3.2.1, Application Error Logs, for more information on audit logs and server logs.

2.5.3. Purges

Neither data, nor audit log entries from the JLV database, or other system components, is purged.

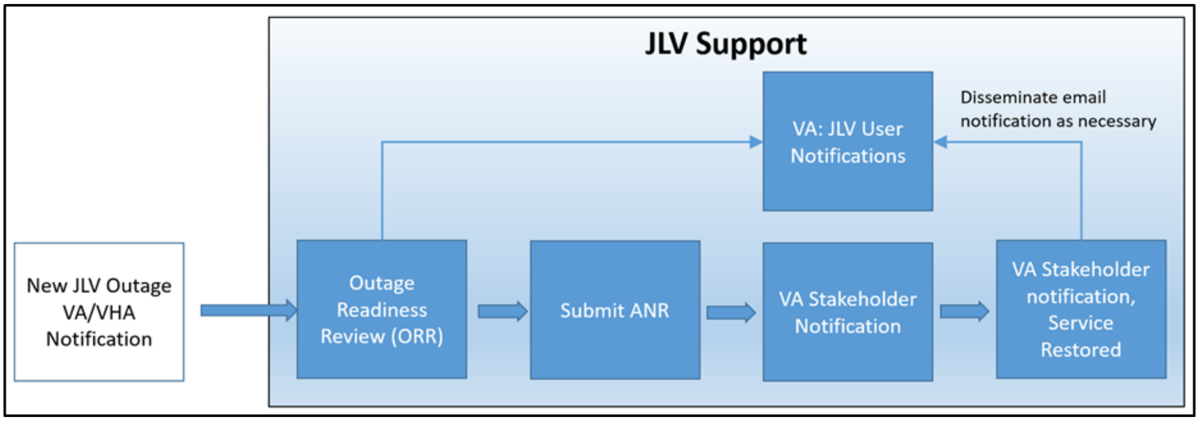
2.6. Scheduled Maintenance

The JLV Support team actively monitors all relevant systems maintenance schedules, and follows the scheduled downtime notification process for JLV code-driven patch releases:

- The VA notifies JLV users of pending system downtime, when JLV is unavailable, and when the system is restored.
- The JLV Support team notifies the VA stakeholders (Table 3) when the JLV system is restored to service.

NOTE: The process flow (Figure 10) is designed primarily for JLV code-driven patch releases, and as a guide for scheduled downtime notifications. However, not all steps may apply for JLV downtimes triggered by scheduled maintenance or outages on external components that are outside the control of the JLV application.

Figure 10: Scheduled Downtime Notification Process


JLV Support
VA: JLV User Notifications
Disseminate email notification as necessary
New JLV Outage VA/VHA Notification
Outage Readiness Review (ORR)
Submit ANR
VA Stakeholder Notification
VA Stakeholder notification, Service Restored

2.7. Capacity Planning

JLV monitors application performance, user onboarding, and user behaviors on a weekly basis. Server resources and JLV application data are collected by the AITC monitoring group, using Computer Associates (CA) Application Performance Management (APM) suite. CA APM monitors, stores data, and sends off alerts to notify members of an e-mail distribution group when any metric exceeds its upper or lower boundary.

2.7.1. 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 real production data, JLV requirements, and future JLV application changes.

3. Exception Handling

Like most systems, JLV may generate a small set of errors that may be 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 are resolved by the user trying an operation again. The following subsections describe these errors, their causes, and what, if any, response an operator should take.

3.1. Routine Errors

Like most systems, JLV 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

One possible security error an end user may encounter is an invalid log in error. Causes of such an error range from the user attempting to access JLV before they are authorized to do so (*Access denied. You are not an authorized user.*), to mistyping the Verify or Access code (*Invalid Access/Verify Codes*).

3.1.2. Timeouts

Each section below describes a possible timeout error

3.1.2.1. Web Application Timeout

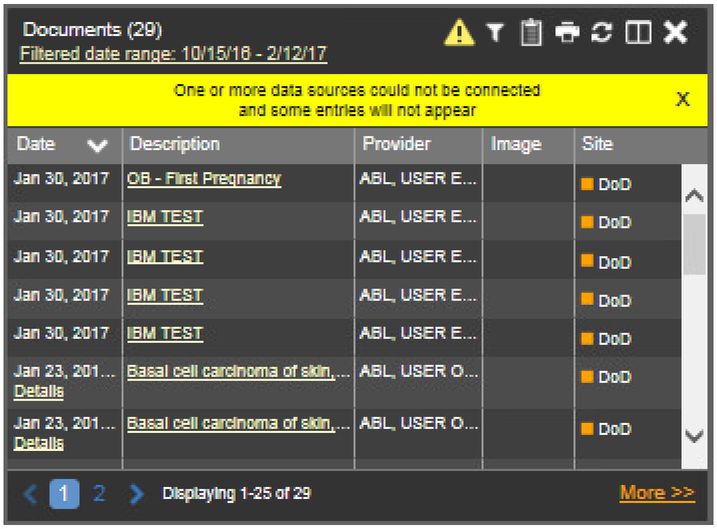
If users encounter a web browser timeout error, or the browser displays *This page can’t be displayed* when accessing the correct URL, it indicates that the JLV web application services are not running, or there is a network outage.

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

3.1.2.2. Connection Errors

JLV may also report time outs to external systems within widgets by displaying a message that one or more data sources could not be connected (Figure 11).

Figure 11: Connection Error Banner



Documents (29)
Filtered date range: 10/15/16 - 2/12/17

One or more data sources could not be connected
and some entries will not appear

X

Date	Description	Provider	Image	Site
Jan 30, 2017	OB - First Pregnancy	ABL, USER E...		■ DoD
Jan 30, 2017	IBM TEST	ABL, USER E...		■ DoD
Jan 30, 2017	IBM TEST	ABL, USER E...		■ DoD
Jan 30, 2017	IBM TEST	ABL, USER E...		■ DoD
Jan 30, 2017	IBM TEST	ABL, USER E...		■ DoD
Jan 23, 201... Details	Basal cell carcinoma of skin,...	ABL, USER O...		■ DoD
Jan 23, 201... Details	Basal cell carcinoma of skin,...	ABL, USER O...		■ DoD

Displaying 1-25 of 29

More >>

NOTE: Connection 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 being queried (VistA, DES), not JLV.

EO continues to make improvements at AITC (F5 Load balancer); the JLV Engineering team optimizes the database (stored procedures for user profiles) to avoid concurrency contention.

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 resolving significant errors, conditions, or other issues.

3.2.1. Application Error Logs

jMeadows retains user actions within the JLV application. Specific events regarding user transactions are also audited (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 log ons, 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 communicating, or a user searching for a patient, the activity is logged and stored in the JLV database. 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 JLV query for data (i.e., action) is audited, and has the user ID linked to it. Only one audit log is produced that contains both VA and DoD user IDs, as well as user names.

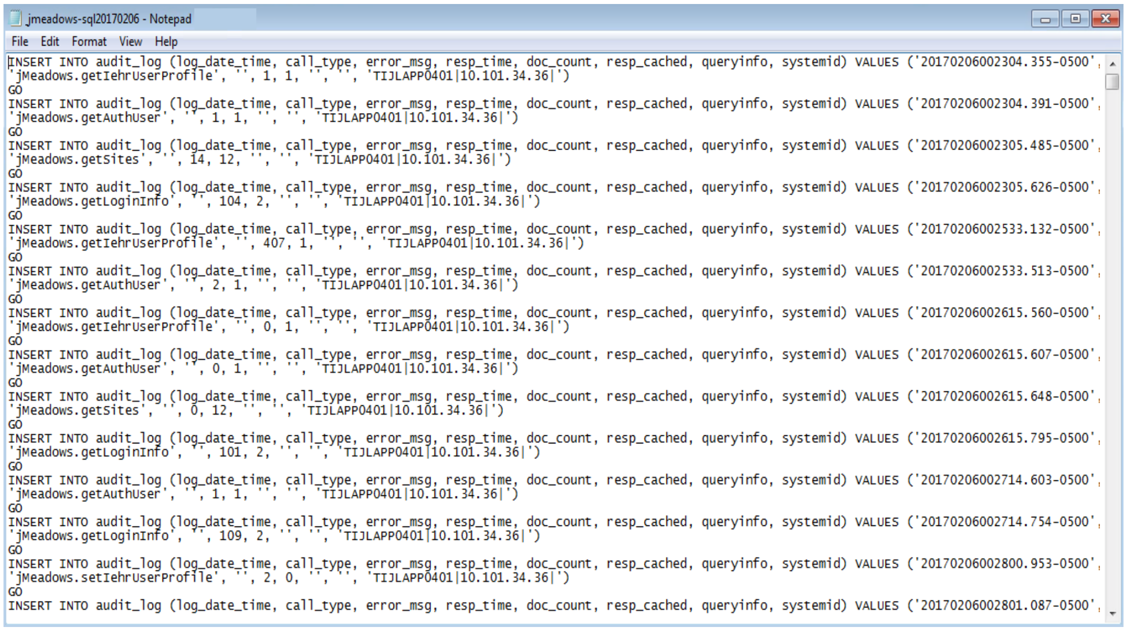
Query times for each web service call into the Relay Service, jMeadows, and VistA Data Service is recorded to a file in the D:\Log directory, on the server where the services are installed. A sample log file output for the jMeadows Data Service is provided in Figure 12.

Table 4 lists the response time log locations.

Table 4: Response Time Log Location

Data Service	Log File Name
jMeadows Data Service	jmeadows-sql.txt
Relay Service	bhie*-sql.txt
VistA Data Service	vds-sql.txt
* *Bidirectional Health Information Exchange*	

Figure 12: Sample jMeadows Log Output



```
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002304.355-0500',
'jMeadows.getIehrUserProfile', '', 1, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002304.391-0500',
'jMeadows.getAuthUser', '', 1, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002305.485-0500',
'jMeadows.getSites', '', 14, 12, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002305.626-0500',
'jMeadows.getLoginInfo', '', 104, 2, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002533.132-0500',
'jMeadows.getIehrUserProfile', '', 407, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002533.513-0500',
'jMeadows.getAuthUser', '', 2, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.560-0500',
'jMeadows.getIehrUserProfile', '', 0, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.607-0500',
'jMeadows.getAuthUser', '', 0, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.648-0500',
'jMeadows.getSites', '', 0, 12, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.795-0500',
'jMeadows.getLoginInfo', '', 101, 2, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002714.603-0500',
'jMeadows.getAuthUser', '', 1, 1, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002714.754-0500',
'jMeadows.getLoginInfo', '', 109, 2, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002800.953-0500',
'jMeadows.setIehrUserProfile', '', 2, 0, '', '', 'TIJLAPP0401|10.101.34.36|')
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002801.087-0500',
```

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

Service interruptions detected by the QoS service are reported to the JLV 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. The QoS service does not send service interruption notices to external systems or services. Detailed information on service interruption notifications, and sample e-mail messages are provided in the *CLIN 0003AA JLV 2.5.2 SDD*. Once approved, all referenced documentation for JLV 2.5.2 is available on the TSPR.

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 JLV 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

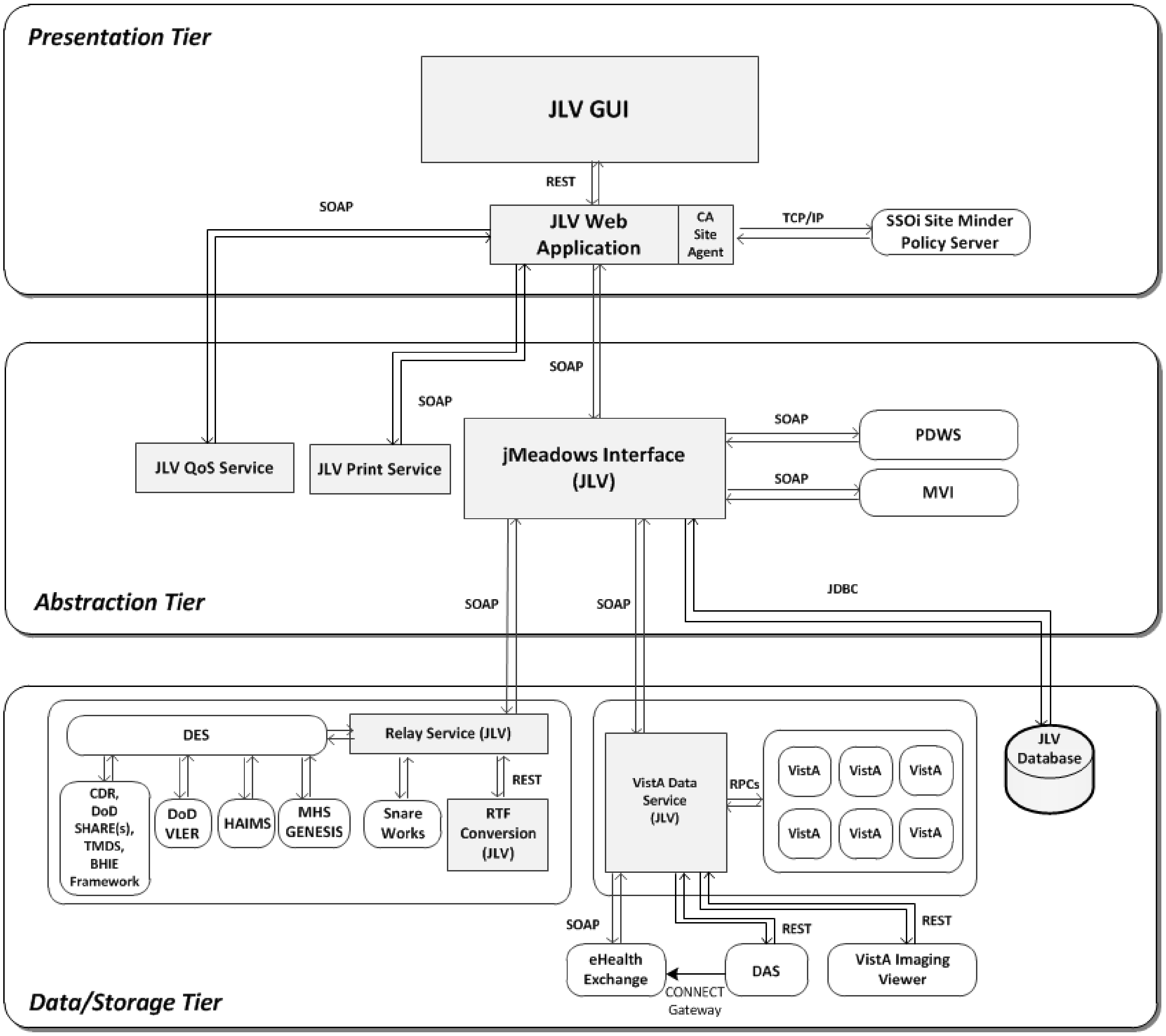
3.2.3.1. Database

The JLV database is a relational database used to store user profile information and audit data for users of the JLV web application.

The JLV database also stores VA and DoD terminology mappings (both local terminology and national standards). The JLV database does NOT store, either long term or temporarily, patient or provider EHR from VA, DoD, or VLER systems.

The JLV database sits on a dedicated server within a deployed JLV environment, alongside the server hosting the JLV web application, and the VistA Data Service (Figure 13). Only the JLV web application and components of the JLV system, including the jMeadows Data Service, connect to, and utilize, the JLV database.

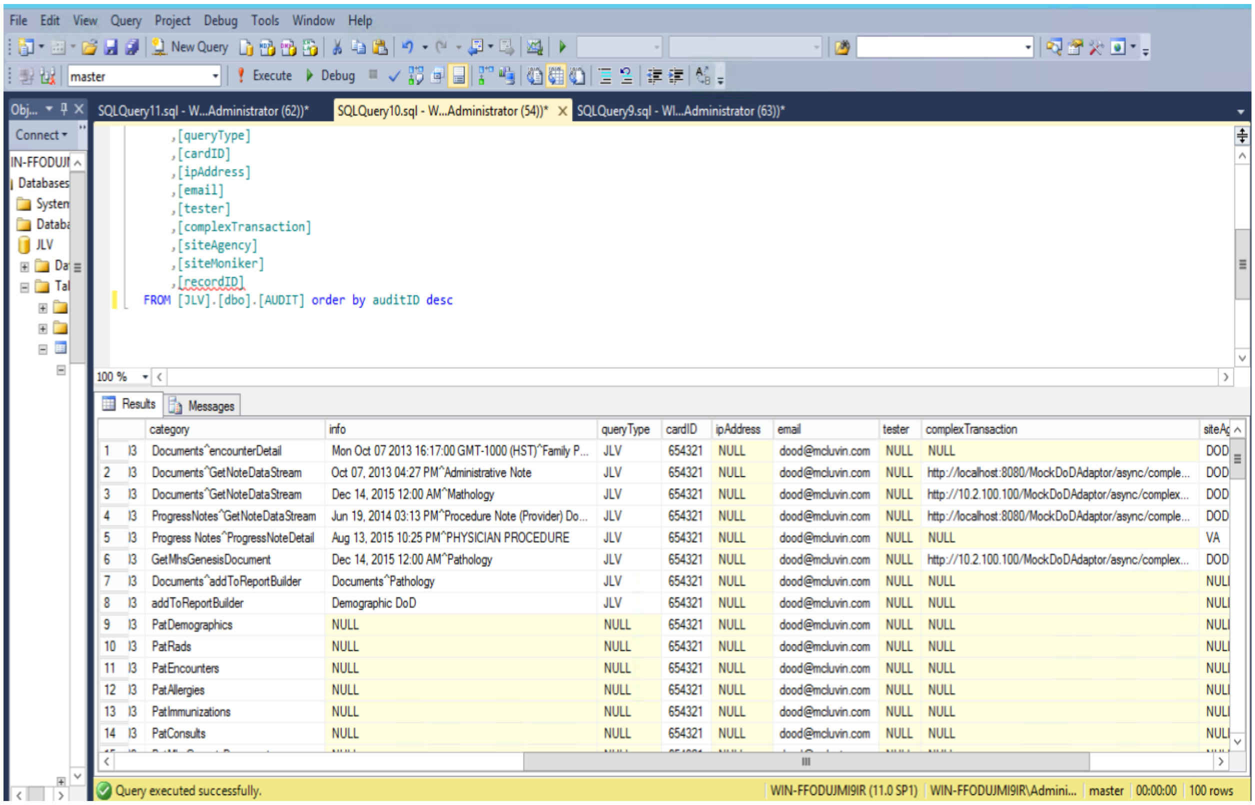
Figure 13: JLV Architecture and Components



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

JLV database errors are written to an error log within the AUDIT database table. The JLV 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 14.

Figure 14: Sample of Audit Log



```
,[queryType]
,[cardID]
,[ipAddress]
,[email]
,[tester]
,[complexTransaction]
,[siteAgency]
,[siteMoniker]
,[recordID]
FROM [JLV].[dbo].[AUDIT] order by auditID desc
```

		category	info	queryType	cardID	ipAddress	email	tester	complexTransaction	siteAg
1	13	Documents^encounterDetail	Mon Oct 07 2013 16:17:00 GMT-1000 (HST)^Family P...	JLV	654321	NULL	dood@mcluvin.com	NULL	NULL	DOD
2	13	Documents^GetNoteDataStream	Oct 07, 2013 04:27 PM^Administrative Note	JLV	654321	NULL	dood@mcluvin.com	NULL	http://localhost:8080/MockDoDAdaptor/async/comple...	DOD
3	13	Documents^GetNoteDataStream	Dec 14, 2015 12:00 AM^Mathology	JLV	654321	NULL	dood@mcluvin.com	NULL	http://10.2.100.100/MockDoDAdaptor/async/complex...	DOD
4	13	ProgressNotes^GetNoteDataStream	Jun 19, 2014 03:13 PM^Procedure Note (Provider) Do...	JLV	654321	NULL	dood@mcluvin.com	NULL	http://localhost:8080/MockDoDAdaptor/async/comple...	DOD
5	13	Progress Notes^ProgressNoteDetail	Aug 13, 2015 10:25 PM^PHYSICIAN PROCEDURE	JLV	654321	NULL	dood@mcluvin.com	NULL	NULL	VA
6	13	GetMhsGenesisDocument	Dec 14, 2015 12:00 AM^Pathology	JLV	654321	NULL	dood@mcluvin.com	NULL	http://10.2.100.100/MockDoDAdaptor/async/complex...	DOD
7	13	Documents^addToReportBuilder	Documents^Pathology	JLV	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
8	13	addToReportBuilder	Demographic DoD	JLV	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
9	13	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
10	13	PatRads	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
11	13	PatEncounters	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
12	13	PatAllergies	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
13	13	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL
14	13	PatConsults	NULL	NULL	654321	NULL	dood@mcluvin.com	NULL	NULL	NULL

Query executed successfully. | WIN-FFODUJMI9IR (11.0 SP1) | WIN-FFODUJMI9IR\Admini... | master | 00:00:00 | 100 rows

3.2.3.2. Web Server

The JLV system uses Oracle WebLogic as its web server in the VA environment. JLV does not implement any custom WebLogic error handling or reporting. For more information, please refer to WebLogic Server Error Messages Reference[2].

3.2.3.3. Application Server

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

3.2.3.4. Network

The JLV web application utilizes the network infrastructure provided by the AITC and PITC. Any network errors that arise are corrected by the team associated with the location of the error.

3.2.3.5. Authentication and Authorization

Refer to Section 2.2, Security/Identity Management for detailed information.

A detailed overview of the access an login process from the user's perspective, is included in the *CLIN 0003AM JLV 2.5.2 User Guide*. Once approved, all referenced documentation for JLV 2.5.2 is available on the TSPR.

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

3.2.3.6. Logical and Physical Descriptions

Refer to the *CLIN 0003AA JLV 2.5.2 SDD* for detailed information. Once approved, all referenced documentation for JLV 2.5.2 is available on the TSPR.

3.3. Dependent System(s)

Table 5 lists the other VA systems upon which JLV depends. It also includes the errors related to each dependent system, and remedies available to System Administrators.

Table 5: JLV Dependent Systems

Other VA System	Related Error(s)	Available Remedies
MVI	The JLV QoS Service monitors MVI availability. When MVI is unavailable, the message *MVI Service may be offline or unavailable* is shown in System Status. Refer to Section 2.4.2.1, Domain Level Availability Monitoring.	Tier 3 System Engineers follow a triage process to determine the root cause of the error, and contact the Point of Contact (POC) for external system, as needed.
Site VistA instances	VistA connection errors are reported through Interface Status notification for each clinical domain. Refer to Section 2.4.2.1, Domain Level Availability Monitoring.	Tier 3 System Engineers follow a triage process to determine the root cause of the error, and contact the POC for external system, as needed.
VLER	If the VA VLER service is not available, the Community Health Summaries and Documents – VA widget displays the message *Something went wrong: Internal Server Error (500)*	Tier 3 System Engineers follow a triage process to determine the root cause of the error, and contact the POC for external system, as needed.

3.4. Troubleshooting

Tier 1 troubleshooting contact information can be can be found in CA Service Desk Manager by searching for *JLV* in the *Knowledge* tab. Tier 1 support is handled by the National Service Desk (NSD) 855-673-4357. Refer to Table 6 for additional contact information.

Tier 2 issues are handled by the CLIN3 team, (Product Health Support).

Tier 3 support and troubleshooting is handled directly with the application developers.

The JLV Engineering and Operations teams perform a rigorous set of procedures to validate that the status of JLV is operational. Those procedures are detailed below.

Validate and test the application using test patients CHDR 1 and CHDR 2:

1. Log in as VA user to JLV application.
   a. Expected Result: Successful login
2. Log in as VBA user to JLV_CLAIMS application
   a. Expected Result: Successful login
3. Validate VA Master Veteran Index (MVI).
   a. Expected Result: Successful patient search, and patient correlation.

4. Validate Patient Search Patient Discovery Web Service (PDWS).
    a. Expected Result: Successfully able to view DoD patient demographics.
5. Validate the VistA Data Service.
    a. Expected Result: VA data is being returned.
6. Validate that the jMeadows interface with the Relay Service is functional.
    a. Expected Result: DoD data is being returned.
7. Validate that VA Terminology mapping is occurring.
    a. Expected Result: VA terminology is properly being mapped in JLV widgets.
8. Validate that DoD Terminology mapping is occurring.
    a. Expected Result: DoD terminology is properly being mapped in JLV widgets.
9. Validate the Health Monitor (QoS).
    a. Expected Result: QoS Service is sending email alerts; System status is displaying.
10. Validate the JLV Print Service.
    a. Expected Result: User is able to add items to report builder and generate a printable PDF file.
11. Validate the RTF Conversion Service.
    a. Expected Result: DoD notes are being displayed in PDF format (when source data is RTF)

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 end up with a fully operational system.

3.5.1. Restart after an Unscheduled System Interruption

The simplest way to bring the system into normal operations after the crash of a component is to restart the affected server(s). See Section 2.1.1, System Startup, for guidance.

3.5.2. Restart after Database Restore

Refer to Section 2.1.1, System Startup, for the system start up procedures.

3.5.3. Backout Procedures

These procedures are dependent on each specific release. Please refer to the *CLIN 0003AL JLV 2.5.2 Deployment, Installation, Backout, and Rollback (DIBR) Guide* specific to the version to be rolled back. Once approved, all project documentation is available on the TSPR.

3.5.4. Rollback Procedures

These procedures are dependent on each specific release. Please refer to the *CLIN 0003AL JLV 2.5.2 DIBR* specific to the version to be rolled back. Once approved, all project documentation is available on the TSPR.

4. Operations and Maintenance Responsibilities

Operational roles and responsibilities for JLV are summarized in Table 6.

Table 6: Operations and Maintenance Responsibility Matrix

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
VA NSD Region 1 and Tuscaloosa	Tier 1 support for VA Users	855-673-4357	nsdtuscaloosausd@va.gov
DoD MHS Service Desk	Tier 1 support for DoD Users	800-600-9332	servicecenter@dha.mil
VA JLV Project Office	**VA OI&T and VHA Stakeholders**		
Cynthia Bias	Program Manager	N/A	cynthia.bias@va.gov
Latricia (Renae) Facundus	Project Manager	202-695-9180	latricia.facundus@va.gov
Elizabeth (Betsy) Green	Project Manager	504-885-3298	elizabeth.green4@va.gov
Amanda Cournoyer		202-480-7370	amanda.cournoyer@va.gov
Jerald Rutherford		708-955-9545	jerald.rutherford@va.gov
Rachel Wiebe		206-462-0131	rachel.wiebe@va.gov
DoD JLV Project Office	**Defense Medical Information Exchange (DMIX) Stakeholders**		
Tiffani Horne		571-858-1631	tiffani.k.horne.ctr@mail.mil
Michael Zrimm		703-588-5716	michael.p.zrimm.civ@mail.mil
DMDC	**PDWS Technical Issues and Support Contacts**	**703-578-5050**	
Lynn Deglin		831-583-2500	lynn.a.deglin.ctr@mail.mil
Ms. Dickie England		706-294-8851	dickie.w.england.civ@mail.mil
Daniel Vidosic		858-621-3632	daniel.p.vidosic.civ@mail.mil
David Wolf		831-583-4128	david.l.wolf24.ctr@mail.mil

Data Exchange Service (DES)	**DoD Adapter Technical Issues and Support Contacts**		
Karlin McNeill		703-253-6001	kmcneill@ellumen.com
Sean Miller		202-430-3456	sean.miller@mantech.com
Adam Rabinowitz		703-230-8830	adam.rabinowitz@mantech.com
DoD Defense Information Systems Administration (DISA)	**Technical Issues and Support Contacts**		
Christopher Tucker		334-416-5170	christopher.a.tucker6.ctr@mail.mil
Jerry Newell		334-416-4267	jerry.l.newell4.civ@mail.mil
VA Authentication Federation Infrastructure (VAAFI)	**Data Power Technical Issues and Support Contacts**		
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
EO	**Technical Issues/ Support Contacts**	**N/A**	**N/A**
Gene Sanchez		512-981-4798	gene.sanchez@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
William (Bill) Hunt		304-680-4301	william.hunt4@va.gov
VA Network – Network Security Operations Center (NSOC)	**Technical Issues/Support Contacts**		**In VA Remedy:**
NSOC		855-673-4357 Option 6, then 4	VA NSOC Business Partner Extranet (BPE) Operations -OR- Network Support Center (NSC) BPE Operations
NSOC		304-260-6685	VANSOCBPEOperations@va.gov

VA Network – Network Security Operations Center (NSOC)	**Technical Issues/Support Contacts**		**In VA Remedy:**
Craig Wasson	Triple-I/VA-NSOC	304-262-5226	craig.wasson@va.gov
DoD Network Space & Naval Warfare Systems (SPAWAR) Virtual Private Network (VPN)	**Technical Issues and Support Contacts**		**In VA Remedy:**
SPAWAR VPN			SPAWARVPN
Shay McFatridge		843-708-9321 (W) 210-845-4256 (C)	shay.mcfatridge.ctr@nsoc.health.mil
Hugh Schmidt			hugh.schmidt.ctr@nsoc.health.mil
DoD NSOC	**Technical Issues and Support Contacts**		
DoD NSOC		800-600-9332 Option 9, then 3, then 2	
Gupreet Brar			gurpreet.brar.ctr@nsoc.health.mil

5. Approval Signatures

Signed: Michael J.
Braithwaite 570687

Digitally signed by Michael J. Braithwaite 570687
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=michael.braithwaite
@va.gov, cn=Michael J. Braithwaite 570687
Date: 2017.04.05 11:11:48 -06'00'

Michael Braithwaite, 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@v
a.gov, cn=Fred J Mingo 1110027
Date: 2017.04.06 11:20:13 -04'00'

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: 2017.04.06 10:26:24 -06'00'

Michael Streff, Receiving Organization (Operations Support) Date

A. Appendix A: Acronyms and Abbreviations

Table 7 lists the acronyms and abbreviations used throughout this document, and their descriptions.

Table 7: Acronyms and Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
AITC	Austin Integration Technology Center
APM	Application Performance Management
BPE	Business Partner Extranet
BTG	Break the Glass
CA	Computer Associates
CAPRI	Compensation and Pension Records Interchange
CPRS	Computerized Patient Record System
DB	Database
DES	Data Exchange Service
DISA	Defense Information Systems Administration
DMDC	Defense Manpower Data Center
DMIX	Defense Medical Information Exchange
DOB	Date of Birth
DoD	Department of Defense
DoS	Denial of Service
EHR	Electronic Health Record
EO	Enterprise Operations
GUI	Graphical User Interface
GTM	Global Traffic Manager
IAM	VA Identity Access Management
JLV	Joint Legacy Viewer
MI	Middle Initial
MITM	Man in the Middle
MS	Microsoft
MVI	Master Veteran Index
NSC	Network Support Center
NSD	National Service Desk
NSOC	Network Security Operations Center
PDWS	Patient Discovery Web Service
PHI	Protected Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification

Acronym	Description
PITC	Philadelphia Information Technology Center
POC	Point of Contact
POM	Production Operations Manual
QoS	Quality of Service
SPAWAR	Space and Naval Warfare Systems
SSD	System Design Document
SSL	Secure Sockets Layer
SSN	Social Security Number
SQL	Microsoft Structured Query Language
TDE	Transparent Data Encryption
TLS	Transport Layer Security
TSPR	Technical Services Project Repository
URL	Universal Resource Locator
VA	Veterans Administration
VAAFI	VA Authentication Federation Infrastructure
VBA	Veterans Benefits Administration
VLER	Virtual Lifetime Electronic Record
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VPN	Virtual Private Network
XML	Extensible Markup Language