VistA Services Assembler Phase 2 (VSA-P2)

Joint Legacy Viewer (JLV)

Production Operations Manual

December 2016

Version 1.2

Department of Veterans Affairs

Revision History

Date	Version	Description	Author
12/05/2016	1.2	Resubmitted with client comments addressed	AbleVets
12/02/2016	1.1	Resubmitted with client comments addressed	AbleVets
11/22/2016	1.0	Draft submitted for review CLIN 0003AK	AbleVets
11/14/16	0.1	Initial draft of the document	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

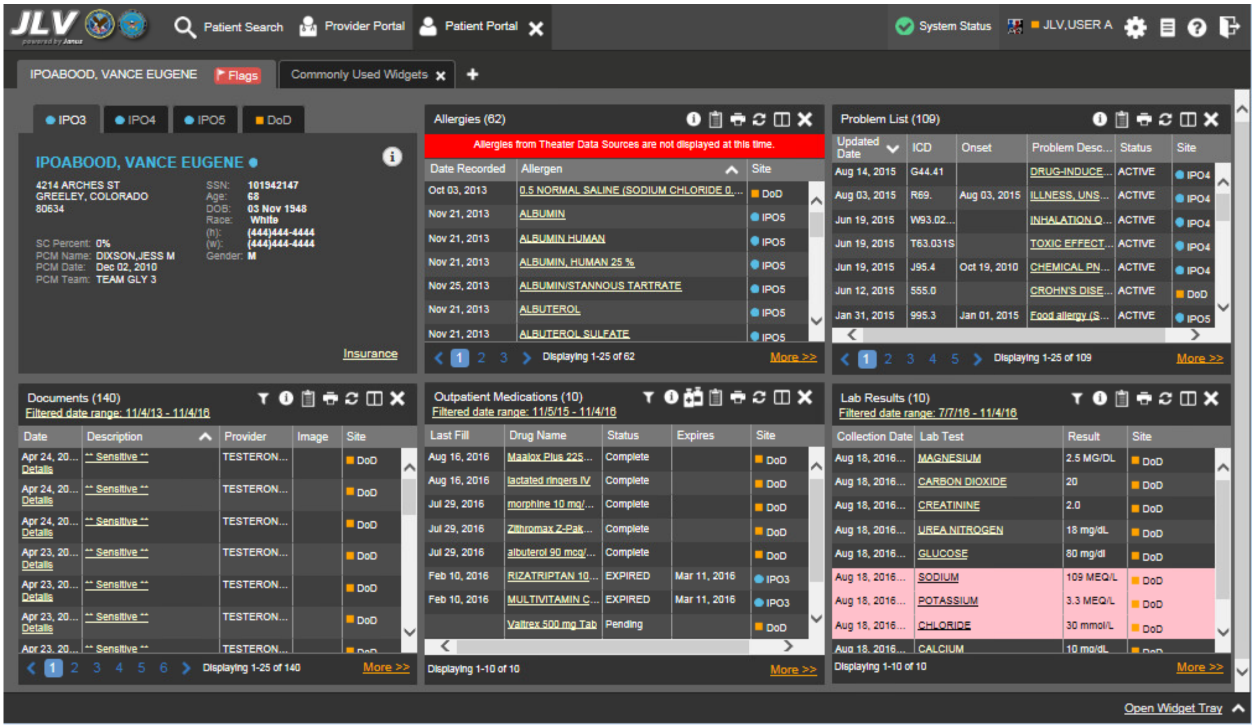
The Joint Legacy Viewer (JLV) is a graphical user interface (GUI) that displays data from the Department of Veterans Affairs (VA) electronic health record (EHR) systems, the Department of Defense (DoD) EHR systems, and VA and DoD Virtual Lifetime Electronic Record (VLER) community partners in a single user interface. The JLV web application provides a common data display of view-only, real-time patient information. The application servers are located at both the Austin Information Technology Center (AITC) and the Philadelphia Information Technology Center (PITC) data centers.

Users can view patient records through JLV, which provides authorized DoD and VA users with a combined view of patient record data. The common data view groups similar data from each health information system and displays them chronologically on a single screen, eliminating the need to access two separate applications to obtain complete patient information. All VA, DoD, and VLER patient data is collated and combined in single screens.

Figure 1 depicts the primary JLV Patient Portal, which is comprised of a number of widgets (viewers) that retrieve clinical data from DoD (orange square), VA (blue circle), and VA and DoD VLER partner (purple hexagon) data sources in real time, displaying them in a unified, chronological view.

A user can create and personalize tabs, drag and drop widgets onto tabs, sort data in widget columns, set date filters, and view each widget in Expanded and Detailed views.

Figure 1: Sample JLV Patient Portal Screen



IPOABOOD, VANCE EUGENE ●

4214 ARCHES ST
GREELEY, COLORADO
80634

SSN: 101942147
Age: 68
DOB: 03 Nov 1948
Race: White
(h): (444)444-4444
(w): (444)444-4444
Gender: M

SC Percent: 0%
PCM Name: DIXSON,JESS M
PCM Date: Dec 02, 2010
PCM Team: TEAM GLY 3

Allergies (62)

Allergies from Theater Data Sources are not displayed at this time.

Date Recorded	Allergen	Site
Oct 03, 2013	0.5 NORMAL SALINE (SODIUM CHLORIDE 0....	■ DoD
Nov 21, 2013	ALBUMIN	● IPO5
Nov 21, 2013	ALBUMIN HUMAN	● IPO5
Nov 21, 2013	ALBUMIN, HUMAN 25 %	● IPO5
Nov 25, 2013	ALBUMIN/STANNOUS TARTRATE	● IPO5
Nov 21, 2013	ALBUTEROL	● IPO5
Nov 21, 2013	ALBUTEROL SULFATE	● IPO5

1 2 3 Displaying 1-25 of 62 More >>

Problem List (109)

Updated Date	ICD	Onset	Problem Desc...	Status	Site
Aug 14, 2015	G44.41		DRUG-INDUCE...	ACTIVE	● IPO4
Aug 03, 2015	R69.	Aug 03, 2015	ILLNESS, UNS...	ACTIVE	● IPO4
Jun 19, 2015	W93.02...		INHALATION O...	ACTIVE	● IPO4
Jun 19, 2015	T63.031S		TOXIC EFFECT...	ACTIVE	● IPO4
Jun 19, 2015	J95.4	Oct 19, 2010	CHEMICAL PN...	ACTIVE	● IPO4
Jun 12, 2015	555.0		CROHN'S DISE...	ACTIVE	■ DoD
Jan 31, 2015	995.3	Jan 01, 2015	Food allergy (S...	ACTIVE	● IPO5

1 2 3 4 5 Displaying 1-25 of 109 More >>

Documents (140)
Filtered date range: 11/4/13 - 11/4/16

Date	Description	Provider	Image	Site
Apr 24, 20... Details	** Sensitive **	TESTERON...		■ DoD
Apr 24, 20... Details	** Sensitive **	TESTERON...		■ DoD
Apr 24, 20... Details	** Sensitive **	TESTERON...		■ DoD
Apr 23, 20... Details	** Sensitive **	TESTERON...		■ DoD
Apr 23, 20... Details	** Sensitive **	TESTERON...		■ DoD
Apr 23, 20... Details	** Sensitive **	TESTERON...		■ DoD
Apr 23, 20...	** Sensitive **	TESTERON...		■ DoD

1 2 3 4 5 6 Displaying 1-25 of 140 More >>

Outpatient Medications (10)
Filtered date range: 11/5/15 - 11/4/16

Last Fill	Drug Name	Status	Expires	Site
Aug 16, 2016	Maalox Plus 225...	Complete		■ DoD
Aug 16, 2016	lactated ringers IV	Complete		■ DoD
Jul 29, 2016	morphine 10 mg/...	Complete		■ DoD
Jul 29, 2016	Zithromax Z-Pak...	Complete		■ DoD
Jul 29, 2016	albuterol 90 mcg/...	Complete		■ DoD
Feb 10, 2016	RIZATRIPTAN 10...	EXPIRED	Mar 11, 2016	● IPO3
Feb 10, 2016	MULTIVITAMIN C...	EXPIRED	Mar 11, 2016	● IPO3
	Valtrex 500 mg Tab	Pending		■ DoD

Displaying 1-10 of 10 More >>

Lab Results (10)
Filtered date range: 7/7/16 - 11/4/16

Collection Date	Lab Test	Result	Site
Aug 18, 2016...	MAGNESIUM	2.5 MG/DL	■ DoD
Aug 18, 2016...	CARBON DIOXIDE	20	■ DoD
Aug 18, 2016...	CREATININE	2.0	■ DoD
Aug 18, 2016...	UREA NITROGEN	18 mg/dL	■ DoD
Aug 18, 2016...	GLUCOSE	80 mg/dl	■ DoD
Aug 18, 2016...	SODIUM	109 MEQ/L	■ DoD
Aug 18, 2016...	POTASSIUM	3.3 MEQ/L	■ DoD
Aug 18, 2016...	CHLORIDE	30 mmol/L	■ DoD
Aug 18, 2016...	CALCIUM	10 mg/dL	■ DoD

Displaying 1-10 of 10 More >>

2. Routine Operations

Routine Operations will be performed by the system administrators to ensure the upkeep, configuration, and reliable operation of computer systems. System administrators will 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 Start-up

1. Start the JLV database servers in AITC.
   - 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 below step.
2. Start the JLV VistADataService servers in AITC.
   - 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 below step.
3. Start the JLV jMeadows servers in AITC.
   - 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 below step.
4. Start the JLV web application servers in AITC.
   - 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 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. Open the JLV web application in a web browser.
8. Authenticate using your Personal Identity Verification (PIV) card when prompted.
9. Verify that the JLV login page displays and indicates that system status is normal.

2.1.1.1. System Start-Up from Emergency Shut-Down

As long as one of the below shut down procedures were performed, no special startup procedure is necessary. One may use the steps in Section 2.1.1 System Start-up.

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

2.1.2. System Shut-down

NOTE: To avoid issues with in-progress transactions, this procedure should be performed during a publish maintenance window in which there will be few users accessing the system. (See Table 1)

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 QoS Service	VAAUSJLVWEB209	VAPHIJLVWEB209
	VAAUSJLVWEB210	VAPHIJLVWEB210
	VAAUSJLVWEB211	VAPHIJLVWEB211
	VAAUSJLVWEB212	VAPHIJLVWEB212
Database	VAAUSJLVSQL201	VAPHIJLVSQL201
	VAAUSJLVSQL202	VAPHIJLVSQL202

2.1.2.1. Emergency System Shut-down

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

2.1.3. Back-up 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. Currently, production systems are configured to backup both databases, JLV and JLV_TDE, on a daily basis.

Under the full or bulk-logged recovery model, before you can restore a database in SQL Server Management Studio, you must back up the active transaction log (known as the tail of the log). To restore a database that is encrypted, you must have access to the certificate or asymmetric key that was used to encrypt the database. Without the certificate or asymmetric key, the database cannot be restored. As a result, the certificate that is 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. Back-Up Procedures

As stated above, backups are configured to backup both databases, JLV and JLV_TDE on a daily basis automatically.

2.1.3.2. Restore Procedures

Pre-requisites to recover databases:

1. Database backup (.bak) file for the JLV and JLV_ TDE databases.
2. 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. Back-Up 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:
        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 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 will be confirmed through smoke test of applications.

2.1.3.4. Storage and Rotation

The JLV Support Team (lead by Rich Lukens and Michael Cardenas) ensures the system and storage arrays for the system is 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. Within the JLV database there is an authorized user table for VA users that contains a list of names and their associated va.gov email addresses; this is the authorized user list.

After reaching the JLV Login page:

- For VA users, JLV requires a VA Personal Identity Verification (PIV) card and 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 (for Veterans Health Administration (VHA)/clinical users) or the user's existing VistA/Compensation and Pension Records Interchange (CAPRI) Access and Verify codes (for Veterans Benefits Administration (VBA)/benefits users). If there is no entry on the authorized user list that matches, an "Access Denied. You are not an authorized user." message is displayed.

User access control and authentication takes place before JLV interfaces with jMeadows. The user is authenticated to his/her host Electronic Health Records (EHR) system, granting that user access to the presentation layer. Based on user credentials, jMeadows retrieves the user's profile information from the JLV database. User default host location, user custom widget layout, and other user data are returned.

User access control for VA users can be configured by system administrators, but it is not enabled by default. See Section 2.2.2 Access Control more information.

A user must insert his/her PIV card into the computer before entering the URL of the JLV application into a browser window. The onscreen JLV login pages guide the user through the login process, including, where necessary, fields to enter user credentials such as PIV PIN, agency, and site. A detailed overview of this process from the user's perspective is included in the JLV User Manual provided with the JLV release.

2.2.1. Identity Management

To add a user:

- VA Support Staff provides name to add
- Logon to VA machine - VA network
- Navigate to Remote Desktop Connection
- Logon 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
  - Click and open Script for Daily Tracker
  - Query AUTH_USER table for users count prior to import
  - Properly format the approved user list before queuing it on the DB
  - Execute script to import users
  - Query AUTH_USER table for users count after import, verify the correct number of users have been added to the DB
- Once users have been added to the DB Navigate to Share Point
- Activate and update users
  - Once users have been Activated and updated in Share Point
  - Check Tracker back in
- JLV Team notifies VA Support Staff

To remove a user:

- VA Support Staff provides name to remove
- Logon to VA machine - VA network
- Navigate to Remote Desktop Connection
- Logon 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 JLV User to be deleted
  - Delete user
  - Update internal file for record.
- JLV Team notifies VA Support Staff

To update a user:

- VA Support Staff provides name to update
- Logon to VA machine - VA network
- Navigate to Remote Desktop Connection
- Logon 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 JLV User to be updated
  - update user
  - Update internal file for record.
- JLV Team notifies VA Support Staff

2.2.2. Access Control

Access control provides the ability to limit access to JLV to VA users registered by system administrators. When configured and enabled, JLV will validate user credentials retrieved from a user's PIV card against a table in the JLV database. If those credentials match what has been entered in the database table, the user is allowed access into the JLV web application.

When the credentials entered do not match what has been entered in the database table, the user will be 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.

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

Table 2: Access Control Design

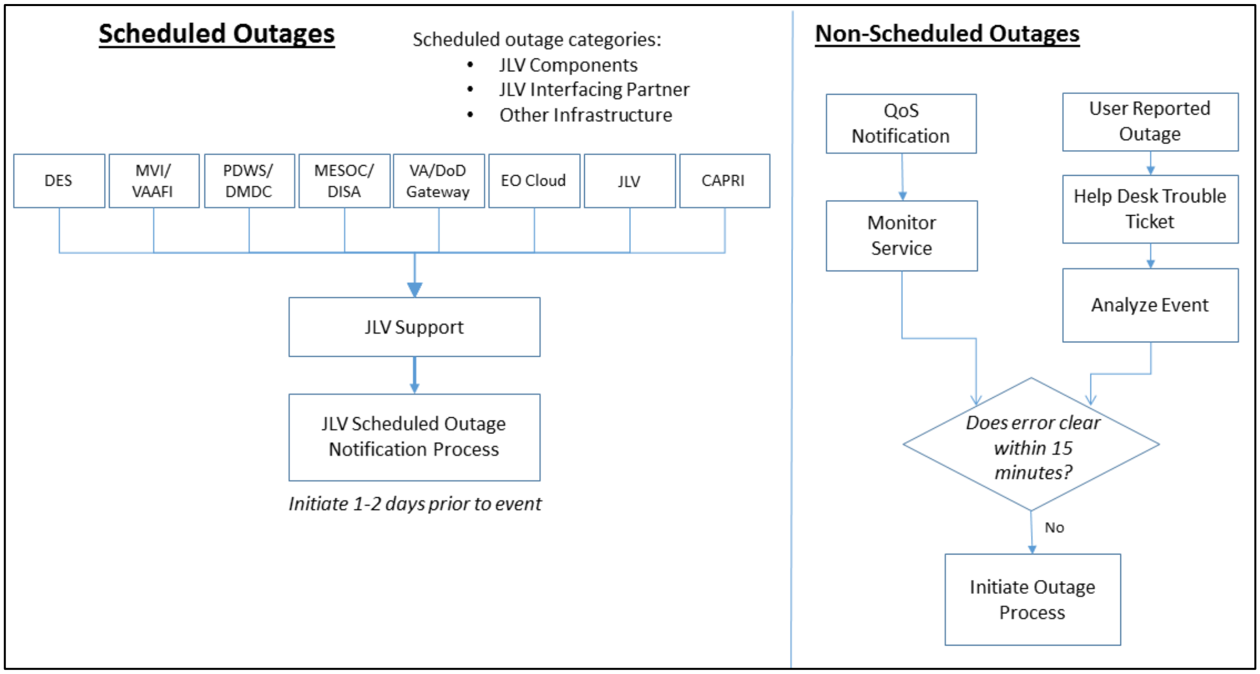
Component	Description
Database table	The AUTH_USER table within the JLV database contains field elements with user identifiers.
Database script	A database script is used for the initial upload and future updates to the AUTH_USER table.
Configuration settings	A configuration setting within the appconfig-production.properties 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 is maintained by JLV Support.

Table 3: JLV Scheduled Downtime VA Stakeholders

Name	Organization	Email Address
Cournoyer, Amanda	VA-Government	Amanda.Cournoyer@va.gov
Roberts, Jerilyn	VA-Government	Jerilyn.Roberts1@va.gov
Green, Betsy	VA-Government	Elizabeth.Green4@va.gov
Hines, Rick	VA-Government	Rick.Hines@va.gov
Bose, Mary Ellen	VA- Government	MaryEllen.Bose@va.gov
Facundus, Latricia R.	VA-Government	Latricia.Facundus@va.gov
McNamee, Shane	VA-Government	Shane.Mcnamee@va.gov
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
Rutherford, Jerald	VA-Government	Jerald.Rutherford@va.gov
Wiebe, Rachel S	VA-Government	Rachel.Wiebe@va.gov
Guebert, Chad	AbleVets (JLV PM)	Chad.Guebert@ablevets.com
Lukens, Rich	AbleVets	Rich.Lukens@ablevets.com
O'Brien, Mark	AbleVets	Mark.Obrien@ablevets.com
Guebert, Crista	HRG	cguebert@hawaiirg.com
Cardenas, Michael	HRG	mcardenas@hawaiirg.com
Goo, Brad	HRG	bgoo@hawaiirg.com
Suenaga, Greg	HRG	gsuenaga@hawaiirg.com
Flemming, Mitch	SBG	mflemming@sbgts.com
Sanchez, Gene W. (SMS)	SMS	Gene.Sanchez@va.gov
Southerland, John B. (SMS)	SMS	John.Southerland@va.gov

2.4. System Monitoring, Reporting and Tools

The JLV system has the ability to trace and audit actions that a user executes within the JLV 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 (including date and time of event, patient identifiers, user identifiers, type of action, and access location) to show system threads of access and viewing patient records.

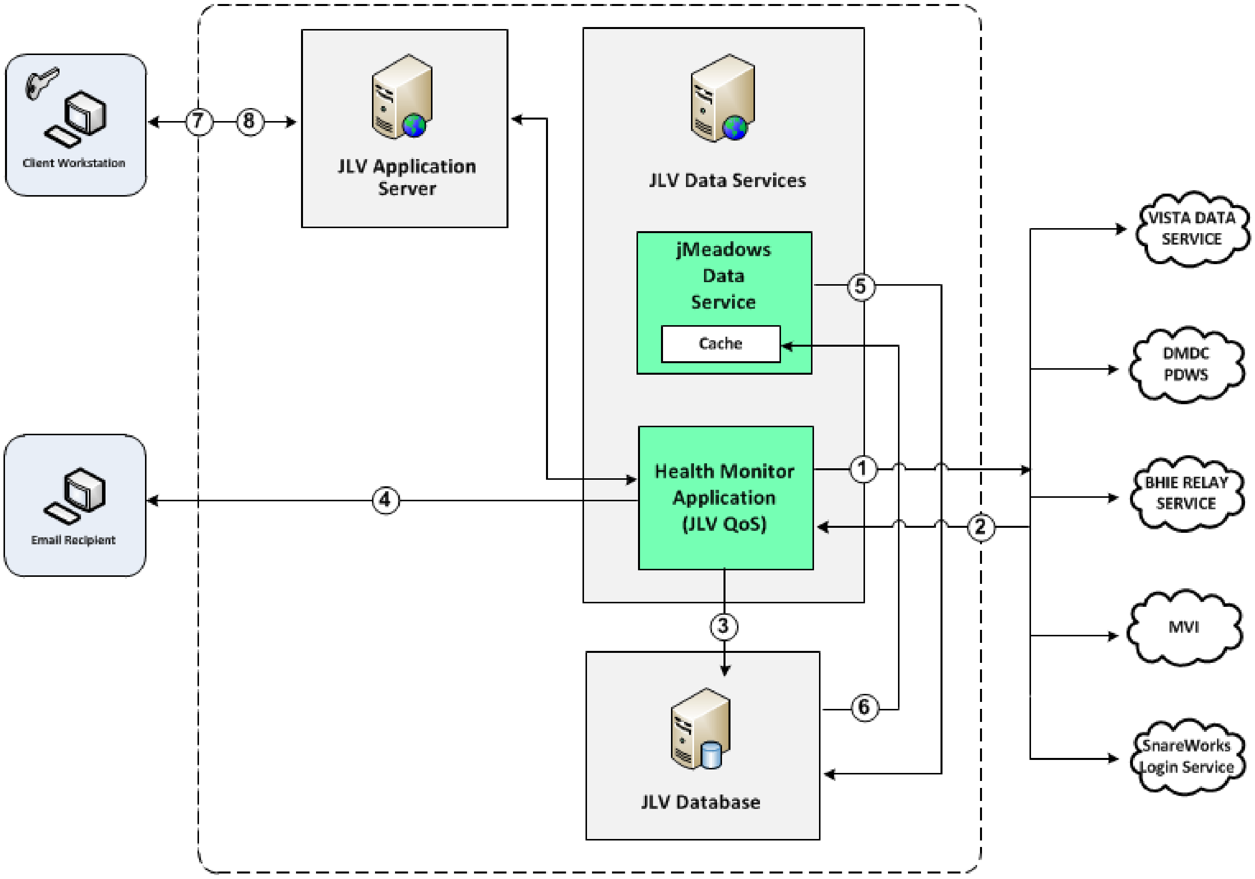
Refer to Section 3.2.1 Application Error Logs for more information on audit logs and server logs.

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

2.4.1. Dataflow Diagram

Figure 3 represents the system status check sequence performed by the QoS Service. Refer to Section 2.4.2, Availability Monitoring.

Figure 3: System Status Check Sequence



2.4.2. Availability Monitoring

The JLV QoS Service monitors the availability of the following services:

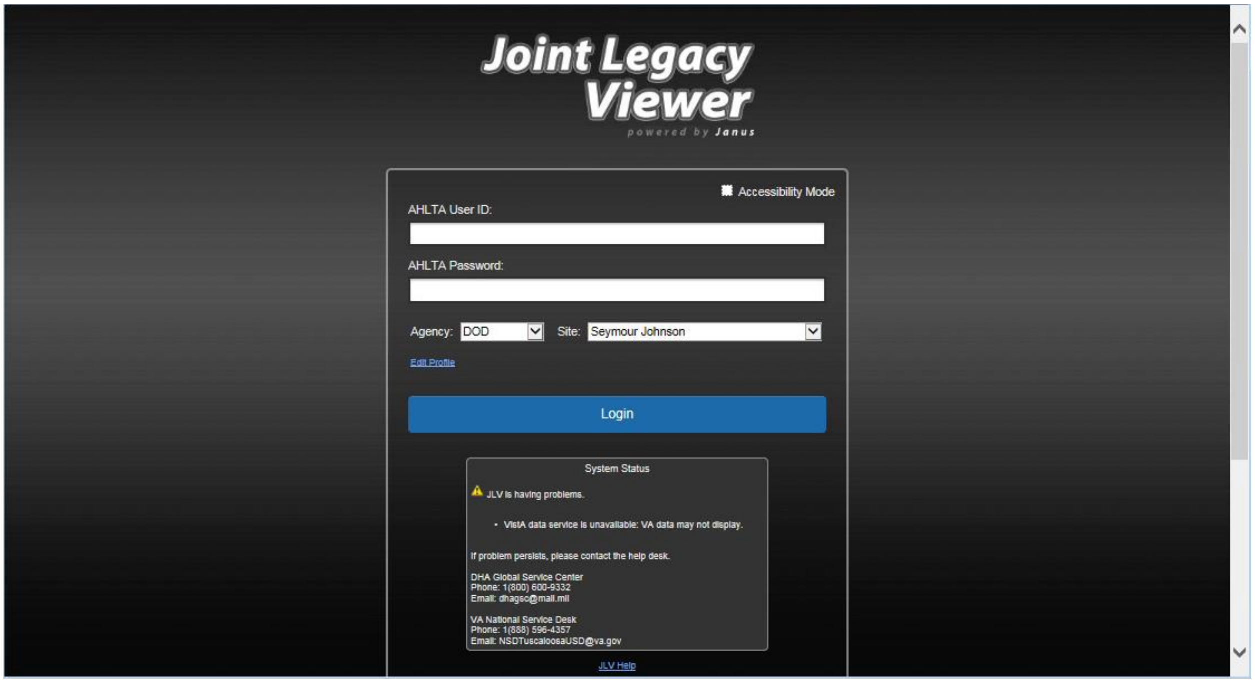
- Master Veteran Index (MVI)
- Patient Discovery Web Service (PDWS)
- Relay Service
- SnareWorks Login Service (DoD user authentication)
- VistA Data Service
- jMeadows Data Service

The following figures display sample system status messages seen by JLV users.

Figure 4 displays a sample system status messages on the Login page.

Figure 5 displays a sample system status messages on the Portal page.

Figure 4: Sample System Status Message on Login Page



■ Accessibility Mode

AHLTA User ID:

AHLTA Password:

Agency: DOD Site: Seymour Johnson

System Status

JLV is having problems.

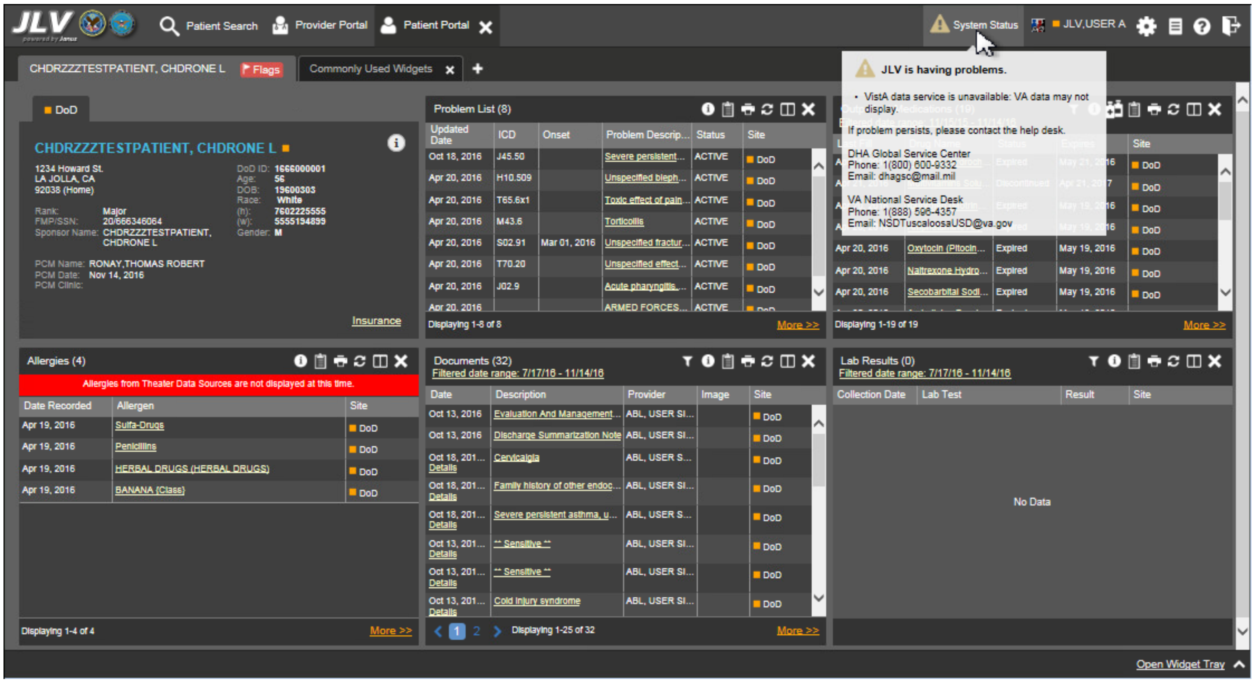
- VistA data service is unavailable: VA data may not display.

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 5: Sample System Status Message on Portal Page



JLV is having problems.

- VistA data service is unavailable: VA data may not display.

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

CHDRZZZTESTPATIENT, CHDRONE L

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

Rank: Major
FMP/SSN: 20/666346064
Sponsor Name: CHDRZZZTESTPATIENT, CHDRONE L

DoD ID: 1666000001
Age: 56
DOB: 19600303
Race: White
(h): 7602225555
(w): 5555194899
Gender: M

PCM Name: RONAY,THOMAS ROBERT
PCM Date: Nov 14, 2016
PCM Clinic:

Problem List (8)

Updated Date	ICD	Onset	Problem Descrip...	Status	Site
Oct 18, 2016	J45.50		Severe persistent...	ACTIVE	■ DoD
Apr 20, 2016	H10.509		Unspecified bleph...	ACTIVE	■ DoD
Apr 20, 2016	T65.6x1		Toxic effect of pain...	ACTIVE	■ DoD
Apr 20, 2016	M43.6		Torticollis	ACTIVE	■ DoD
Apr 20, 2016	S02.91	Mar 01, 2016	Unspecified fractur...	ACTIVE	■ DoD
Apr 20, 2016	T70.20		Unspecified effect...	ACTIVE	■ DoD
Apr 20, 2016	J02.9		Acute pharyngitis,...	ACTIVE	■ DoD
Apr 20, 2016			ARMED FORCES...	ACTIVE	■ DoD

Displaying 1-8 of 8 More >>

Last Fill	Drug Name	Status	Expires	Site
				■ DoD
				■ DoD
				■ DoD
				■ DoD
Apr 20, 2016	Oxytocin (Pitocin...	Expired	May 19, 2016	■ DoD
Apr 20, 2016	Naltrexone Hydro...	Expired	May 19, 2016	■ DoD
Apr 20, 2016	Secobarbital Sodi...	Expired	May 19, 2016	■ DoD

Displaying 1-19 of 19 More >>

Allergies (4)

Allergies from Theater Data Sources are not displayed at this time.

Date Recorded	Allergen	Site
Apr 19, 2016	Sulfa-Drugs	■ DoD
Apr 19, 2016	Penicillins	■ DoD
Apr 19, 2016	HERBAL DRUGS (HERBAL DRUGS)	■ DoD
Apr 19, 2016	BANANA (Class)	■ DoD

Displaying 1-4 of 4 More >>

Documents (32)
Filtered date range: 7/17/16 - 11/14/16

Date	Description	Provider	Image	Site
Oct 13, 2016	Evaluation And Management...	ABL, USER SI...		■ DoD
Oct 13, 2016	Discharge Summarization Note	ABL, USER SI...		■ DoD
Oct 18, 201... Details	Cervicalgia	ABL, USER S...		■ DoD
Oct 18, 201... Details	Family history of other endoc...	ABL, USER SI...		■ DoD
Oct 18, 201... Details	Severe persistent asthma, u...	ABL, USER S...		■ DoD
Oct 13, 201... Details	** Sensitive **	ABL, USER SI...		■ DoD
Oct 13, 201... Details	** Sensitive **	ABL, USER SI...		■ DoD
Oct 13, 201... Details	Cold injury syndrome	ABL, USER SI...		■ DoD

< 1 2 > Displaying 1-25 of 32 More >>

Lab Results (0)
Filtered date range: 7/17/16 - 11/14/16

Collection Date	Lab Test	Result	Site

No Data

2.4.2.1. Domain-Level Availability Monitoring

JLV includes **Interface Status** buttons in the toolbar of multiple Patient Portal widgets that display the status of the data source for that clinical domain.

There are two conditions:

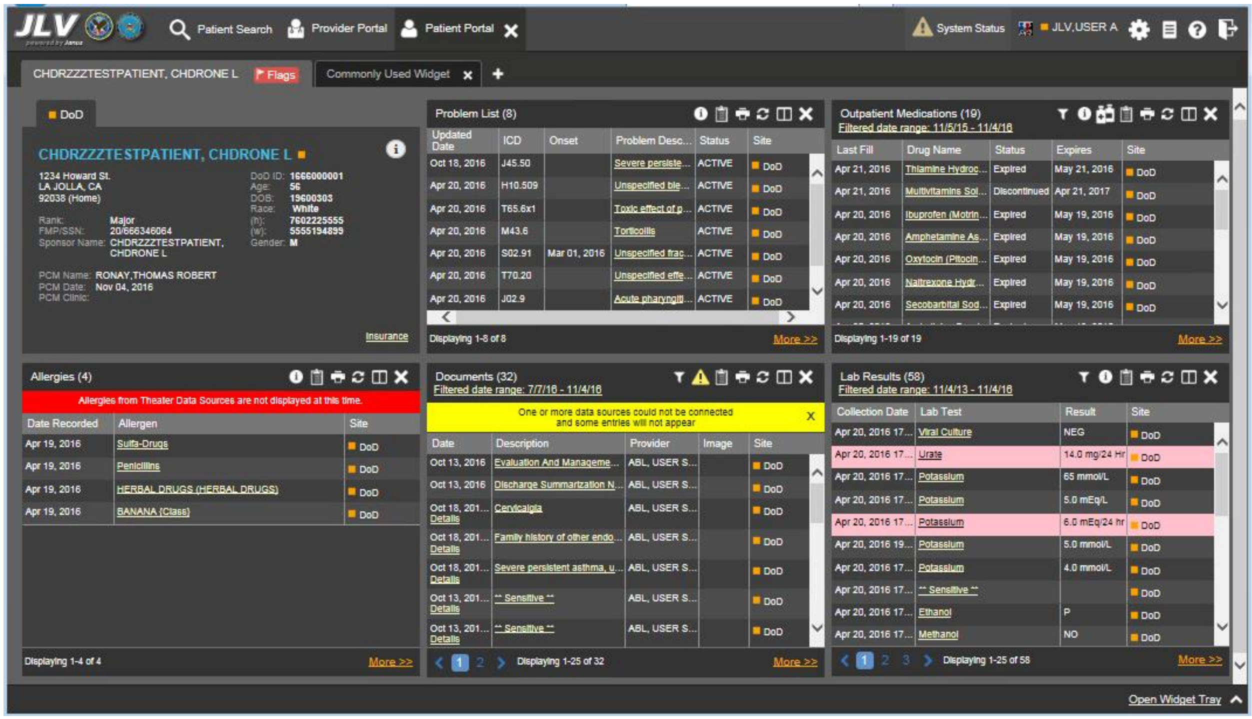
The information icon ⓘ indicates all sources are available.

The warning icon ⚠ indicates one or more data sources are unavailable.

A yellow banner (Figure 6) will also be displayed over a widget when one or more sources are unavailable, indicating sources could not be connected and some records may not appear.

Both icons provide status for DoD, VA, and community partner data sources. Clicking either status icon will open the Interface Status details in a separate window (as seen in Figure 7). Interface status details accessed from the widget show connection status at the domain level.

Figure 6: Sample Interface Status Notification (Yellow Banner)



CHDRZZZTESTPATIENT, CHDRONE L

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

Rank: Major
FMP/SSN: 20/666346064
Sponsor Name: CHDRZZZTESTPATIENT, CHDRONE L

DoD ID: 1666000001
Age: 56
DOB: 19600303
Race: White
(h): 7602225555
(w): 5555194899
Gender: M

PCM Name: RONAY,THOMAS ROBERT
PCM Date: Nov 04, 2016
PCM Clinic:

Problem List (8)

Updated Date	ICD	Onset	Problem Desc...	Status	Site
Oct 18, 2016	J45.50		Severe persiste...	ACTIVE	DoD
Apr 20, 2016	H10.509		Unspecified ble...	ACTIVE	DoD
Apr 20, 2016	T65.6x1		Toxic effect of p...	ACTIVE	DoD
Apr 20, 2016	M43.6		Torticollis	ACTIVE	DoD
Apr 20, 2016	S02.91	Mar 01, 2016	Unspecified frac...	ACTIVE	DoD
Apr 20, 2016	T70.20		Unspecified effe...	ACTIVE	DoD
Apr 20, 2016	J02.9		Acute pharyngiti...	ACTIVE	DoD

Displaying 1-8 of 8 More >>

Outpatient Medications (19)
Filtered date range: 11/5/15 - 11/4/16

Last Fill	Drug Name	Status	Expires	Site
Apr 21, 2016	Thiamine Hydroc...	Expired	May 21, 2016	DoD
Apr 21, 2016	Multivitamins Sol...	Discontinued	Apr 21, 2017	DoD
Apr 20, 2016	Ibuprofen (Motrin...	Expired	May 19, 2016	DoD
Apr 20, 2016	Amphetamine As...	Expired	May 19, 2016	DoD
Apr 20, 2016	Oxytocin (Pitocin...	Expired	May 19, 2016	DoD
Apr 20, 2016	Naltrexone Hydr...	Expired	May 19, 2016	DoD
Apr 20, 2016	Secobarbital Sod...	Expired	May 19, 2016	DoD

Displaying 1-19 of 19 More >>

Allergies (4)

Allergies from Theater Data Sources are not displayed at this time.

Date Recorded	Allergen	Site
Apr 19, 2016	Sulfa-Drugs	DoD
Apr 19, 2016	Penicillins	DoD
Apr 19, 2016	HERBAL DRUGS (HERBAL DRUGS)	DoD
Apr 19, 2016	BANANA (Class)	DoD

Displaying 1-4 of 4 More >>

Documents (32)
Filtered date range: 7/7/16 - 11/4/16

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

Date	Description	Provider	Image	Site
Oct 13, 2016	Evaluation And Manageme...	ABL, USER S...		DoD
Oct 13, 2016	Discharge Summarization N...	ABL, USER S...		DoD
Oct 18, 201... Details	Cervicalgia	ABL, USER S...		DoD
Oct 18, 201... Details	Family history of other endo...	ABL, USER S...		DoD
Oct 18, 201... Details	Severe persistent asthma, u...	ABL, USER S...		DoD
Oct 13, 201... Details	** Sensitive **	ABL, USER S...		DoD
Oct 13, 201... Details	** Sensitive **	ABL, USER S...		DoD

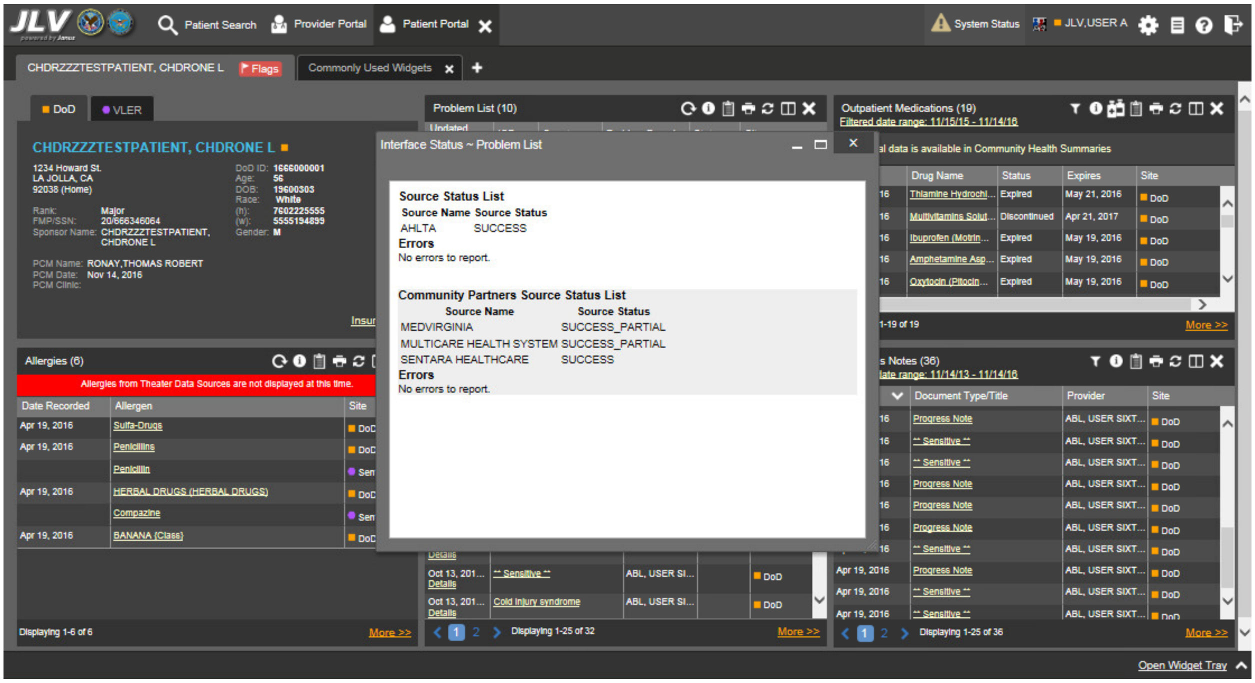
< 1 2 > Displaying 1-25 of 32 More >>

Lab Results (58)
Filtered date range: 11/4/13 - 11/4/16

Collection Date	Lab Test	Result	Site
Apr 20, 2016 17...	Viral Culture	NEG	DoD
Apr 20, 2016 17...	Urate	14.0 mg/24 Hr	DoD
Apr 20, 2016 17...	Potassium	65 mmol/L	DoD
Apr 20, 2016 17...	Potassium	5.0 mEq/L	DoD
Apr 20, 2016 17...	Potassium	6.0 mEq/24 hr	DoD
Apr 20, 2016 19...	Potassium	5.0 mmol/L	DoD
Apr 20, 2016 17...	Potassium	4.0 mmol/L	DoD
Apr 20, 2016 17...	** Sensitive **		DoD
Apr 20, 2016 17...	Ethanol	P	DoD
Apr 20, 2016 17...	Methanol	NO	DoD

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

Figure 7: 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 will be recorded to a file in the D:\Log directory on the server where the services are installed. Sample log file output for the jMeadows Data Service is provided in

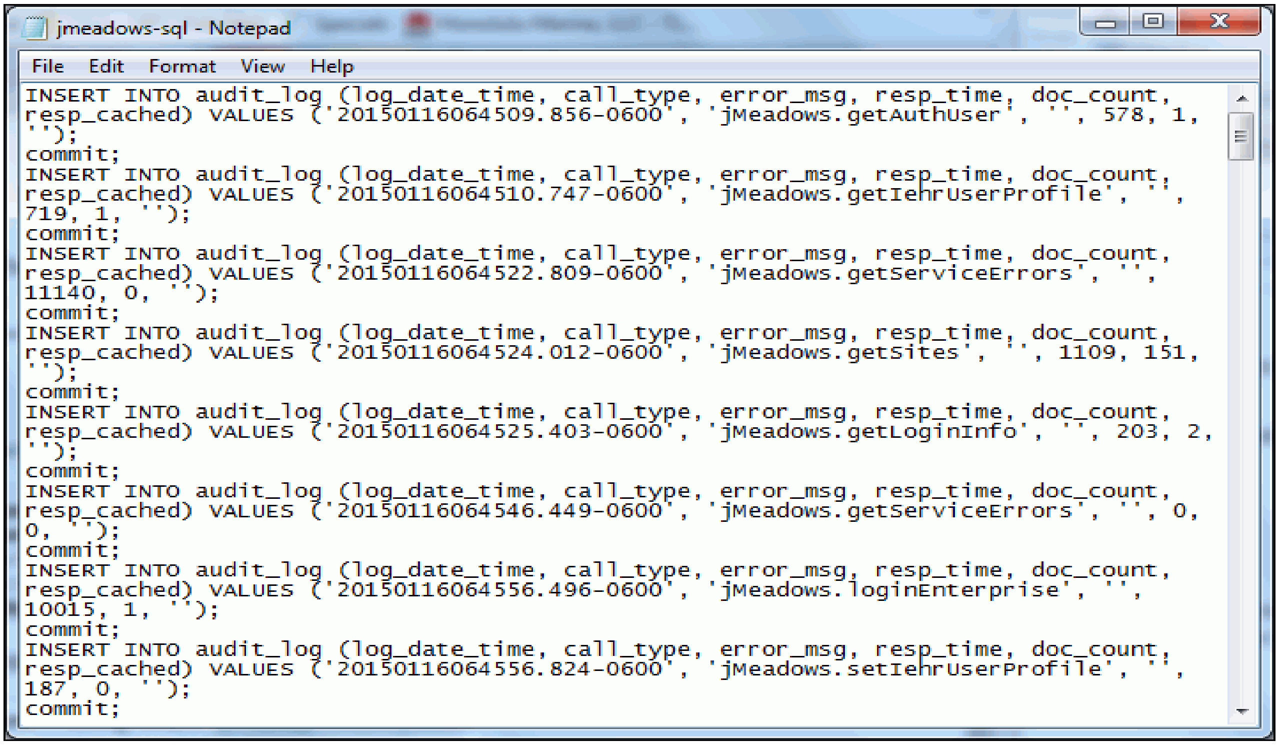
Table 4.

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

Sample query time log file output for the jMeadows Data Service is provided in Figure 8.

Figure 8: Sample jMeadows_logOutput



```
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064509.856-0600', 'jMeadows.getAuthUser', '', 578, 1,
'');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064510.747-0600', 'jMeadows.getIehrUserProfile', '',
719, 1, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064522.809-0600', 'jMeadows.getServiceErrors', '',
11140, 0, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064524.012-0600', 'jMeadows.getSites', '', 1109, 151,
'');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064525.403-0600', 'jMeadows.getLoginInfo', '', 203, 2,
'');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064546.449-0600', 'jMeadows.getServiceErrors', '', 0,
0, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064556.496-0600', 'jMeadows.loginEnterprise', '',
10015, 1, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064556.824-0600', 'jMeadows.setIehrUserProfile', '',
187, 0, '');
commit;
```

2.4.4. Critical Metrics

- VA providers, Veterans Health Administration (VHA) users, or members of the Veterans Benefits Administration (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 by a VBA user. This includes the identification of the individual whose PHI was accessed, the identification of the VBA user who accessed the information, and identification of the specific PHI accessed.
- User access to sensitive DoD data. DoD and VA users will be 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 and then opens the same record/views the record a second time, the user will be asked to agree to be audited again.
- For sensitive DoD data, the following information will be captured for each attempt to access sensitive data whether successful or unsuccessful:
  - Organization (e.g., VHA, VBA, DoD)
  - Username
  - User SSN/Electronic Data Interchange Personal Identifier (EDIPI) (DoD only)
  - User PIV (VA only)
  - User Location
  - Patient (Patient Last, First Name, MI; SSN/EDIPI (DoD only), MVI (VA only) DOB)

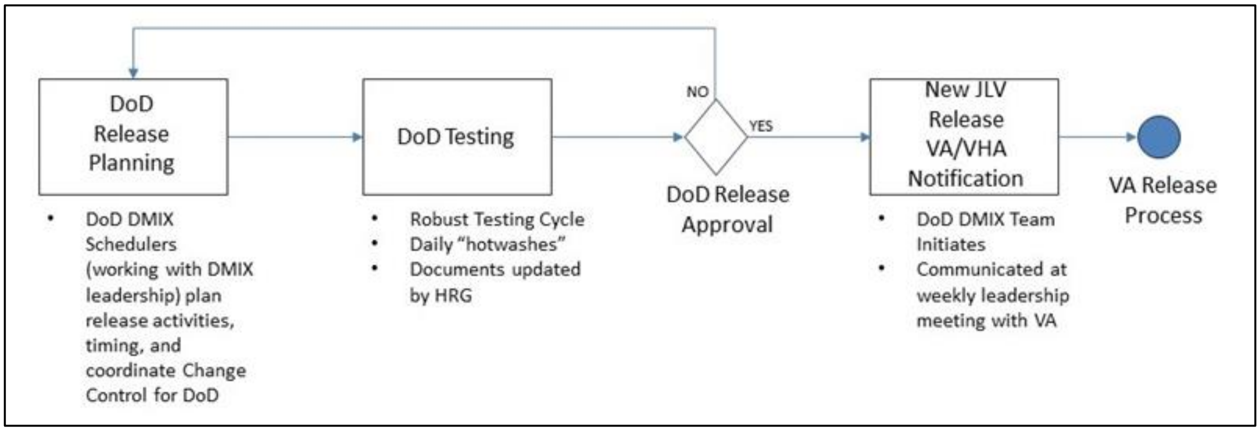
- Sensitive data accessed (e.g., unique note identifier)
- Date/Time accessed
- Reason for Break the Glass (BTG) (e.g., Emergent Care, Clinical Care, or Authorized Administrative Use).

2.5. Routine Updates, Extracts and Purges

2.5.1. Routine Updates

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

Figure 9: Patching Process for DoD and VA Components


DoD Release Planning
DoD DMIX Schedulers (working with DMIX leadership) plan release activities, timing, and coordinate Change Control for DoD
DoD Testing
Robust Testing Cycle
Daily "hotwashes"
Documents updated by HRG
NO
YES
DoD Release Approval
New JLV Release VA/VHA Notification
DoD DMIX Team Initiates
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 Government project manager or the DoD Government 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 will extract the requested data and send the data in an encrypted method to the requestor. Refer to Section 3.2.1 Application Error Logs for more information on audit logs and server logs.

2.5.3. Purges

JLV does not purge data or audits log entries from the JLV database or other system components.

2.6. Scheduled Maintenance

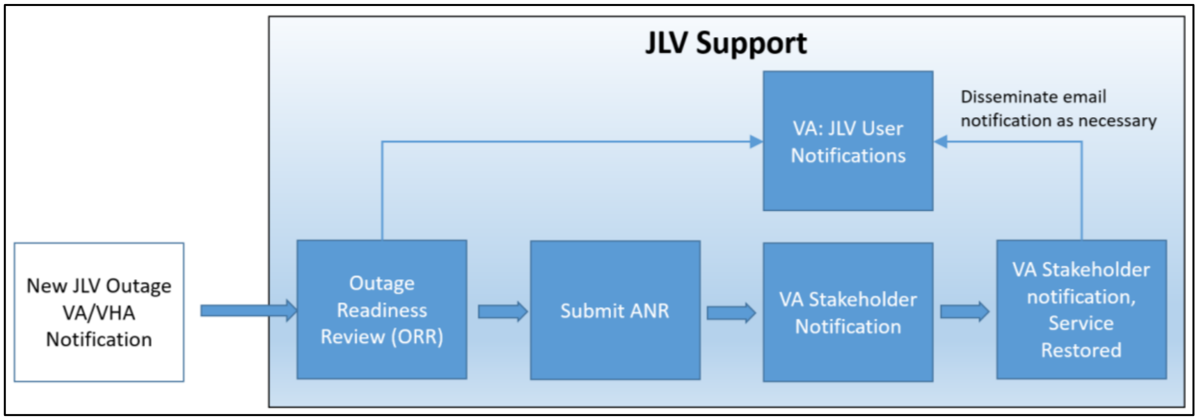
The JLV Support team is comprised Systems/Network/Security Engineers and Systems Administrators at AbleVets and HRG and lead by Operations Lead Rich Lukens and Integration Lead Michael Cardenas as primary JLV Support point of contacts.

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

- JLV Support Team, notifies the VA stakeholders listed in Table 3, when the JLV system is restored to service.
- The VA notifies the JLV users of both pending system downtime when JLV is unavailable and when the system is restored.

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/outages on external components outside of 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 on-boarding, and user behaviors on a weekly basis. Server resource and JLV application data are collected by AITC Monitoring group using Computer Associates (CA) Application Performance Management (APM) suite. For JLV, CA APM monitors, stores data, and sends off alerts to notify members of an email 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, typically quarterly updates. 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 only require the user to retry an operation. The following subsections describe these errors, their causes, and what, if any, response an operator needs to take.

3.1. Routine Errors

While the occasional occurrence of these errors may be routine, getting a large number of an individual errors over a short period of time is an indication of a more serious problem. In that case the error needs to be treated as a significant error. Refer to Section 3.2, Significant Errors.

3.1.1. Security Errors

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

- Session security: By 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. Also, if in some instance the session-id were to be obtained, the user cannot paste it as part of a URL string to gain access.
- Data Encryption: Using Secure Sockets Layer (SSL) with Transport Layer Security (TLS) 1.0 ensures that all server communication is encrypted, which limits the ability to perform Man-in-the-Middle (MITM) attacks.
- Database Encryption at Rest: Using Microsoft SQL Server Transparent Data Encryption (TDE) Encryption level Advanced Encryption Standard (AES) 256-bit to encrypt Personally Identifiable Information (PII)/PHI data at rest.
- Schema Validation: Web Services used in JLV employ Schema Validation. This helps prevent Denial of Service (DoS) attacks by preventing the invocation of Extensible Markup Language (XML) bombs.

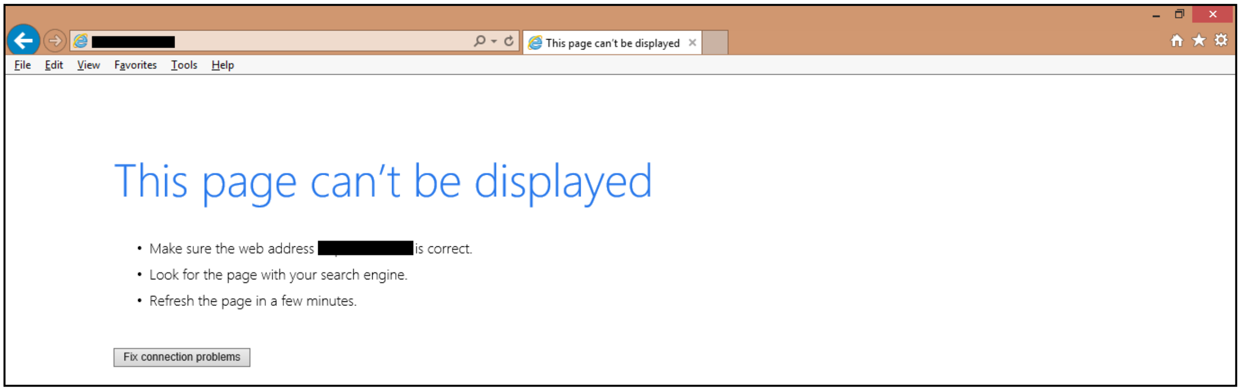
3.1.2. Time-outs

Figure 11 describes a possible time-out error.

3.1.2.1. Web Application Time Out

If users encounter a web browser time out error as pictured below when accessing the correct URL, it indicates that the JLV web application services are not running or a network outage.

Figure 11: Internet Explorer Timeout Notification



This page can’t be displayed

- Make sure the web address [redacted] is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

To resolve, attempt to remote desktop into each JLV web application server and ensure the WebLogic services are running. If WebLogic services are determined to be running, contact Enterprise Operations to verify correct operation of the Global Traffic Manager.

3.1.3. Concurrency

Resolution of concurrent record access is handled by the underlying system of record that is being queried (VistA, DES), not JLV.

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.

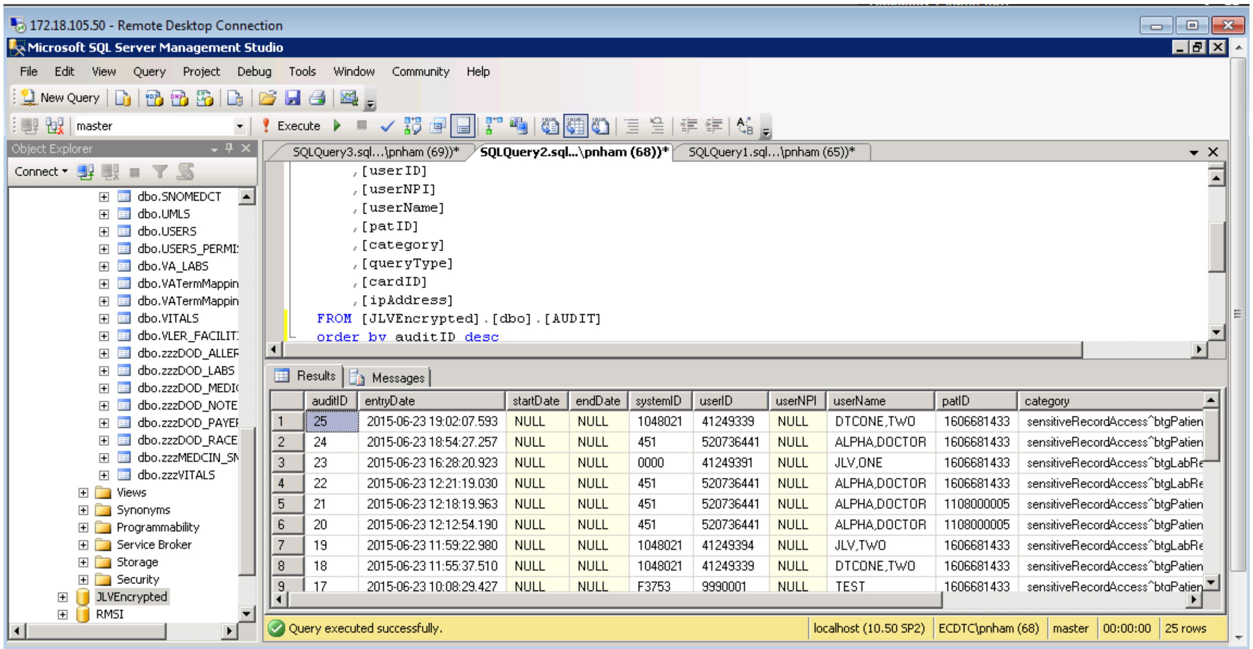
3.2.1. Application Error Logs

jMeadows retains user actions within the JLV application. 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 logons, and 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, which contains both DoD and VA user IDs and user names.

Figure 12: Sample Audit Log



```
      ,[userID]
      ,[userNPI]
      ,[userName]
      ,[patID]
      ,[category]
      ,[queryType]
      ,[cardID]
      ,[ipAddress]
  FROM [JLVEncrypted].[dbo].[AUDIT]
  order by auditID desc
```

	auditID	entryDate	startDate	endDate	systemID	userID	userNPI	userName	patID	category
1	25	2015-06-23 19:02:07.593	NULL	NULL	1048021	41249339	NULL	DTCONE,TWO	1606681433	sensitiveRecordAccess^btgPatien
2	24	2015-06-23 18:54:27.257	NULL	NULL	451	520736441	NULL	ALPHA,DOCTOR	1606681433	sensitiveRecordAccess^btgPatien
3	23	2015-06-23 16:28:20.923	NULL	NULL	0000	41249391	NULL	JLV,ONE	1606681433	sensitiveRecordAccess^btgLabRe
4	22	2015-06-23 12:21:19.030	NULL	NULL	451	520736441	NULL	ALPHA,DOCTOR	1606681433	sensitiveRecordAccess^btgLabRe
5	21	2015-06-23 12:18:19.963	NULL	NULL	451	520736441	NULL	ALPHA,DOCTOR	1108000005	sensitiveRecordAccess^btgPatien
6	20	2015-06-23 12:12:54.190	NULL	NULL	451	520736441	NULL	ALPHA,DOCTOR	1108000005	sensitiveRecordAccess^btgPatien
7	19	2015-06-23 11:59:22.980	NULL	NULL	1048021	41249394	NULL	JLV,TWO	1606681433	sensitiveRecordAccess^btgLabRe
8	18	2015-06-23 11:55:37.510	NULL	NULL	1048021	41249339	NULL	DTCONE,TWO	1606681433	sensitiveRecordAccess^btgPatien
9	17	2015-06-23 10:08:29.427	NULL	NULL	F3753	9990001	NULL	TEST	1606681433	sensitiveRecordAccess^btgPatien

```
Query executed successfully.   localhost (10.50 SP2)   ECDTC\pnham (68)   master   00:00:00   25 rows
```

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

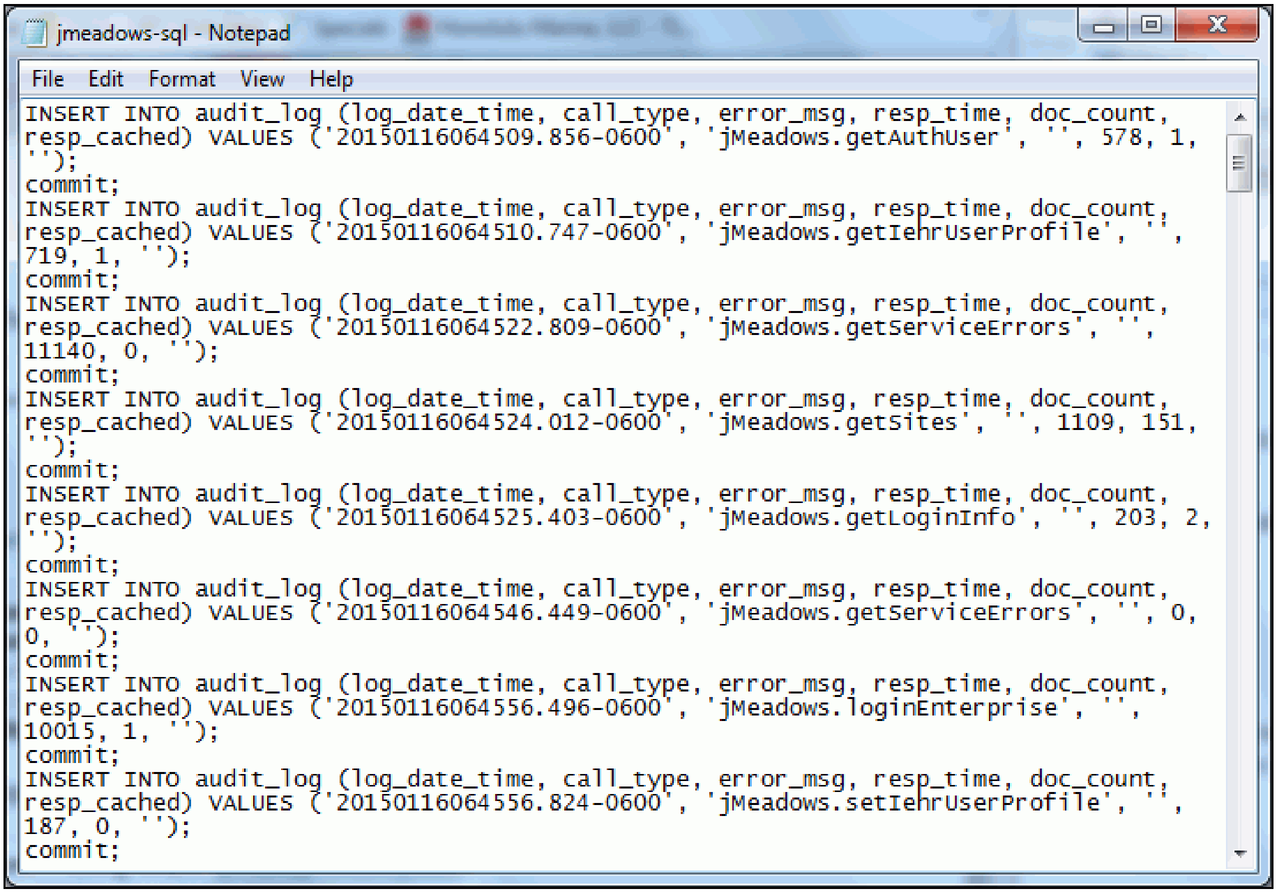
Table 5 includes the response time log location.

Table 5: 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

Sample query time log file output for the jMeadows Data Service is provided in Figure 13.

Figure 13: Sample jMeadows Log Output



```
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064509.856-0600', 'jMeadows.getAuthUser', '', 578, 1,
'');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064510.747-0600', 'jMeadows.getIehrUserProfile', '',
719, 1, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064522.809-0600', 'jMeadows.getServiceErrors', '',
11140, 0, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064524.012-0600', 'jMeadows.getSites', '', 1109, 151,
'');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064525.403-0600', 'jMeadows.getLoginInfo', '', 203, 2,
'');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064546.449-0600', 'jMeadows.getServiceErrors', '', 0,
0, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064556.496-0600', 'jMeadows.loginEnterprise', '',
10015, 1, '');
commit;
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count,
resp_cached) VALUES ('20150116064556.824-0600', 'jMeadows.setIehrUserProfile', '',
187, 0, '');
commit;
```

3.2.2. Application Error Codes and Descriptions

JLV does not implement standardized error codes.

3.2.3. Infrastructure Errors

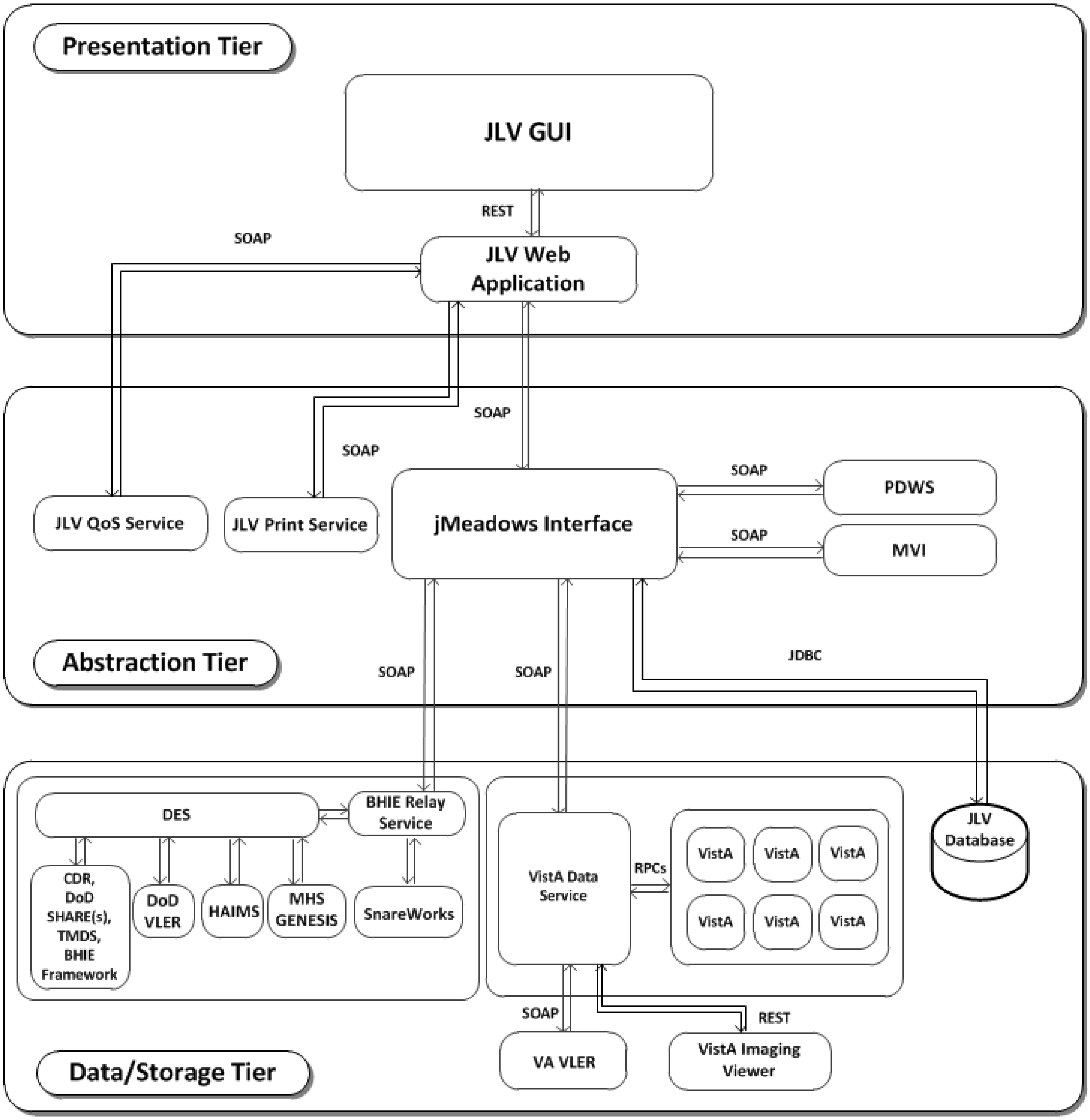
3.2.3.1. Database

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 electronic healthcare records from DoD, VA, and VLER electronic health record (EHR) 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 14). Only the JLV web application and components of the JLV system, including the jMeadows Data Service, connect to and utilize the JLV database.

Figure 14: JLV Architecture



3.2.3.2. Web Server

JLV does not use a special-purpose web server. In VA environments, the application server WebLogic functions as the web server.

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, refer to Understanding WebLogic Logging Services.[1]

3.2.3.4. Network

Enterprise JLV utilizes the network infrastructure provided by the AITC and PITC data centers.

3.2.3.5. Authentication and Authorization

The JLV system restricts access to the JLV GUI to authorized users within the VA and DoD enterprise. For VA users, the access method will be direct to the JLV web application through a URL provided by system administrators. After reaching the JLV Login page:

- JLV requires a VA PIV card and PIN to log in along with the user's local existing VistA/CPRS Access and Verify codes (for VHA/clinical users) or the user's existing VistA/CAPRI Access and Verify codes (for VBA/benefits users).

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

User access control for VA users can be configured by system administrators, but it is not enabled by default. For VA users, VA Identity and Access Management (IAM) maintains the whitelist, a master list of authorized JLV users. VA IAM administers the JLV whitelist by leveraging stored procedures within the JLV database to add users, remove users, and update or change user entries within the JLV database. If needed, the JLV Support Team (or a designated system administrator) can manually add individual VA users to the whitelist.

A user must insert his/her PIV card into the computer before entering the URL of the JLV application into a browser window. The onscreen JLV login pages guide the user through the login process, including, where necessary, fields to enter user credentials such as PIV PIN, agency, and site. A detailed overview of this process from the user's perspective is included in the Joint Legacy Viewer (JLV) 2.5.1 User Guide. Once submitted, the document will be available on the TSPR[2].

3.2.3.6. Logical and Physical Descriptions

JLV is a software application, logical and physical descriptions are not applicable.

3.3. Dependent System(s)

Table 6 lists the other VA systems on which JLV depends. It also includes the errors related to each dependent system and remedies available to system administrators.

[1] See Understanding WebLogic Logging Services

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

Table 6: JLV Dependent Systems

Other VA System	Related Error(s)	Available Remedies
Master Veteran Index (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 will follow a triage process to determine the root cause of the error and contact 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 will follow a triage process to determine the root cause of the error and contact POC for external system as needed.
Virtual Lifetime Electronic Record (VLER)	If the VA VLER service is not available, the Community Health Summaries and Documents – VA widget will display the message *Something went wrong: Internal Server Error (500)*	Tier 3 system engineers will follow a triage process to determine the root cause of the error and contact POC for external system as needed.

3.4. Troubleshooting

Tier 1 troubleshooting can be can be found in the CA Service Desk Manager by searching for JLV in the Knowledge tab. Tier 1 is handled by the National Service Desk (NSD) 855-673-4357. Refer to Table 7 for additional contact information.

All Tier 2 and 3 support and troubleshooting is handled directly with the application developers.

The following can also be performed to validate the operational status:

- Validate and test the application using test patients CHDR 1 and CHDR 2:
  1. Validate Patient Search PDWS.
  2. Validate VA MVI.
  3. Validate the VistA Data Service by ensuring VA data is being returned.
  4. Validate the Relay Service by ensuring DoD data is being returned.
  5. Validate that VA Terminology mapping is occurring.
  6. Validate that DoD Terminology mapping is occurring.
  7. Validate the Health Monitor service.

3.5. System Recovery

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

3.5.1. Restart after Non-Scheduled 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 Start-up for guidance.

3.5.2. Restart after Database Restore

Refer to Section 2.1.1 System Start-up for the system start up procedures.

3.5.3. Back-out Procedures

These procedures are dependent on each specific release. Please refer to the JLV 2.5.1 Deployment, Installation, Backout, and Rollback Guide, pertaining to the version to be rolled back. Once submitted, the document will be available on the TSPR.

3.5.4. Rollback Procedures

These procedures are dependent on each specific release. Please refer to the JLV 2.5.1 Deployment, Installation, Backout, and Rollback Guide, pertaining to the version to be rolled back. Once submitted, the document will be available on the TSPR.

4. Operations and Maintenance Responsibilities

JLV operational roles and responsibilities are summarized in TTable 7.

Table 7: Operations and Maintenance Responsibility Matrix

Name/Organization	Phone Number	E-mail Address
VA National Service Desk - NSD – Region and Tuscaloosa (Tier 1 for VA Users)	855-673-4357	NSDTuscaloosaUSD@va.gov
DoD Military Health System (MHS) Service Desk (Tier 1. For DoD Users)	800-600-9332	servicecenter@dha.mil
VA - JLV Project Office (VA OIT and VHA Stakeholders)	N/A	N/A
Elizabeth (Betsy) Green	504-885-3298	elizabeth.green4@va.gov
Latricia (Renae) Facundus	202-695-9180	Latricia.facundus@va.gov
Rachel Wiebe	206-462-0131	rachel.wiebe@va.gov
Jerald Rutherford	708-955-9545	jerald.rutherford@va.gov
Amanda Cournoyer	202-480-7370	Amanda.Cournoyer@va.gov
DoD - JLV Project Office (Defense Medical Information Exchange [DMIX] Stakeholders)	N/A	N/A
Michael Zrimm	703-588-5716	michael.p.zrimm.civ@mail.mil
Tiffani Horne	571-858-1631	tiffani.k.horne.ctr@mail.mil

Name/Organization	Phone Number	E-mail Address
Defense Manpower Data Center (DMDC) PDWS (Technical Issues and Support Contacts)	DMDC Service Desk: 703-578-5050	N/A
Daniel Vidosic	858-621-3632	daniel.p.vidosic.civ@mail.mil
Ms. Dickie England	706-294-8851	dickie.w.england.civ@mail.mil
David Wolf	831-583-4128	david.l.wolf24.ctr@mail.mil
Lynn Deglin	831-583-2500	lynn.a.deglin.ctr@mail.mil
Data Exchange Service (DES) - DoD Adaptor (Technical Issues and Support Contacts)	N/A	N/A
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)	N/A	N/A
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)	N/A	N/A
Courtney Rive	757-772-0701	courtney.rive@va.gov
Mayank Acharya	818-804-9928	mayank.acharya@va.gov
Basavaraj "Raj" Devershetty	813-842-3432	basavaraj.devershetty@va.gov
Enterprise Operations (EO) (Technical Issues and Support Contacts)	N/A	N/A
Gene Sanchez	512-981-4798	gene.sanchez@va.gov
MVI (VA) (Technical Issues and Support Contacts)	N/A	In VA Remedy assigned under: Department of Veterans Affairs - Development - DEV-Person Service
Jason Boire	O:503-747-6883 C:240-381-6087	Jason.Boire@va.gov
Danny Reed	205-943-2415	Danny.Reed@va.gov
Cory Chin	407-593-1963	Cory.Chin@va.gov
William (Bill) Hunt	304-680-4301	William.Hunt4@va.gov
DoD Network - Space and Naval Warfare Systems (SPAWAR) Virtual Private Network (VPN) (Technical Issues and Support Contacts)	N/A	In DoD Remedy assigned under: SPAWARVPN

Name/Organization	Phone Number	E-mail Address
Shay McFatridge	Mobile: 210-845-4256 Work: 843-708-9321	shay.mcfatridge.ctr@nsoc.health.mil
Hugh Schmidt	N/A	hugh.schmidt.ctr@nsoc.health.mil
DoD Network - Network Security Operations Center (NSOC) (Technical Issues and Support Contacts)	800-600-9332, Option 9, then 3, then 2	N/A
Gupreet Brar	N/A	gurpreet.brar.ctr@nsoc.health.mil
VA Network – NSOC (Technical Issues and Support Contacts)	855-673-4357, Option 6, then 4	In VA Remedy assigned under: VA NSOC Business Partner Extranet (BPE) Operations -OR- Network Support Center (NSC) BPE Operations
VA Network - NSOC (Technical Issues and Support Contacts)	304-260-6685	VANSOCBPEOperations@va.gov
Craig Wasson (Triple-I/VA-NSOC)	304-262-5226	craig.wasson@va.gov

5. Approval Signatures

REVIEW DATE:

SCRIBE:

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: 2016.12.09 10:11:58 -05'00'

Portfolio 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: 2016.12.08 13:34:00 -05'00'

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: 2016.12.07 07:17:36 -07'00'

Receiving Organization (Operations Support) Date

Signed: ______________________________

Product Support Date

A. Appendix A: Acronyms and Abbreviations

Table 8 provides a list of the acronyms and abbreviations used in this document.

Table 8: Acronyms and Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
AHLTA	Armed Forces Health Longitudinal Technology Application
AITC	Austin Integration Technology Center
APM	Application Performance Management
BTG	Break the Glass
CA	Computer Associates
CAPRI	Compensation and Pension Records Interchange
CPRS	Computerized Patient Record System
DoD	Department of Defense
EDIPI	Electronic Data Interchange Personal Identifier
EHR	Electronic Health Record
EO	Enterprise Operations
GUI	Graphical User Interface
GTM	Global Traffic Manager
IAM	VA Identity Access Management
JLV	Joint Legacy Viewer
MESOC	Military Health System Enterprise Services Operations Center
MITM	Man-In-The-Middle
MS	Microsoft
MVI	Master Veteran Index
PDWS	Patient Discovery Web Service
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PITC	Philadelphia Information Technology Center
POC	Point of Contact
SSL	Secure Sockets Layer
SQL	Microsoft Structured Query Language
TDE	Server Transparent Data Encryption
TLS	Transport Layer Security
TSPR	Technical Services Project Repository

Acronym	Description
VA	Veterans Administration
VBA	Veterans Benefits Administration
VLER	Virtual Lifetime Electronic Record
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VSA-P2	VistA Services Assembler Phase 2
XML	Extensible Markup Language