Joint Longitudinal Viewer (JLV) 2.9.4

Production Operations Manual (POM)

May 2021

Version 1.0

Department of Veterans Affairs

Revision History

Date	Version	Description	Author
05/13/2021	1.0	Updated after adjudication meeting	Liberty ITS
05/07/2021	0.3	Updated from SME feedback	Liberty ITS
04/29/2021	0.2	Updated from Reviewer feedback	Liberty ITS
04/28/2021	0.1	Initial draft of document from last approved	Liberty ITS

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

Born from a joint Department of Defense (DOD)–Department of Veterans Affairs (VA) venture called JANUS, Joint Longitudinal Viewer (JLV) was directed by the Secretary of the VA and the Secretary of Defense in early 2013 to further support interoperability between the two departments. JLV is a centrally hosted, Java-based web application managed as two similar but distinct products - one tailored for DoD use and another tailored for VA use. Each JLV product is deployed to its respective DoD and VA hosting environments. Although separately hosted, the respective applications use several shared data services. The browser-based Graphical User Interface (GUI) provides an integrated, read-only view of Electronic Health Record (EHR) data from the VA, DOD, and community partners within a single application.

JLV eliminates the need for VA and DOD clinicians to access disparate viewers. The GUI retrieves clinical data from several native data sources and systems, then presents it to the user via widgets, each corresponding to a clinical data domain.

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 blue circle indicates VA data; an orange square indicates DOD data; a purple hexagon indicates community partner data; and a green triangle indicates Cerner Millennium Federal Electronic Health Record (FEHR) data.

Figure 1 depicts the main application window, comprised of the Patient Portal (details displayed) and widgets. The widgets retrieve clinical data from sources in real time, displaying them in a unified, chronological view.

Figure 1: The JLV Patient Portal
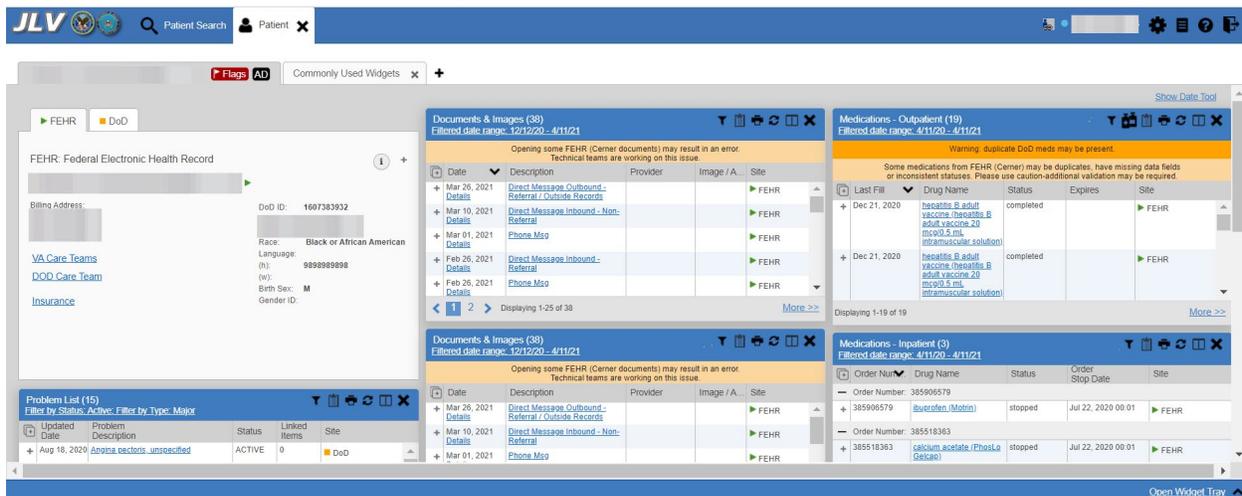
2.   Routine Operations

System administrators perform routine operations to maintain the configuration, upkeep, and reliable operation of computer systems. System administrators also ensure that the performance, uptime, resources, and security of the systems meet the needs of the end users.

2.1.   Administrative Procedures

JLV Support and VA Infrastructure Operations (IO) system administrators maintain the servers that house JLV's VA Production environments. Table 1 lists the JLV Production environments and owners.

Table 1: Current Production Environments

Production Environment	Owner
Austin Information Technology Center (AITC)	VA
Philadelphia Information Technology Center (PITC)	VA

A detailed list of the servers referenced throughout the system startup procedures can be found in the *JLV AITC and PITC Production Virtual Machine (VM) Inventory Report* (REDACTED) and the *JLV 2.9.4 Deployment, Installation, Backout and Rollback Guide (DIBRG)*, (REDACTED.[1])

2.1.1.   System Startup

1. Start the JLV database (DB) servers (performed by IO)

    a. The DB server processes are configured to run as system services and are automatically started with the DB servers

    b. Validation:

        i.   Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the DB servers are up and operational

        ii. Log in to each DB server to validate that the MS SQL Server service is started; if the service has started, it signifies that the DB servers are up and operational

        iii. Log in to each DB server, open the SQL Server Management Studio (SSMS) and connect to the DB; the connection is successful if the DB servers are up and operational

2. Start the Veterans Information Systems and Technology Architecture (VistA) Data Service (VDS) servers

    a. The service processes are configured to run as system services and are automatically started with the VDS servers

    b. Validation:

        i.   Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the VDS servers are up and operational

        ii. Review each of the WebLogic-managed VDS server application logs for connection and/or application errors

3. Start the JLV jMeadows servers

    a. The service processes are configured to run as system services and are automatically started with the servers

    b. Validation:

---

[1] **NOTE:** Access to the VA JLV Product Repository on GitHub is restricted and must be requested.

- i. Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the jMeadows servers are up and operational
- ii. Review each of the WebLogic-managed jMeadows server application logs for connection and/or application errors

4. Start the Electronic Health Record Modernization (EHRM) Service servers
   a. The service processes are configured to run as system services and are automatically started with the EHRM Service servers
   b. Validation:
      - i. Startup is validated through the successful smoke test of the application; loading Cerner Millennium FEHR data confirms the EHRM Service servers are up and operational
      - ii. Review each of the Tomcat-managed EHRM Service server application logs for connection and/or application errors

5. Start the Report Builder servers
   a. The service processes are configured to run as system services and are automatically started with the servers
   b. Validation:
      - i. Startup is validated through the successful smoke test of the application; loading a document into Report Builder and testing the print feature confirms that the Report Builder servers are up and operational
      - ii. Review each of the WebLogic-managed Report Builder server application logs for connection and/or application errors

6. Start the JLV front-end web servers and the Apache Single Sign-On Internal (SSOi) servers
   a. The service processes are configured to run as system services and are automatically started with the servers
   b. Validation:
      - i. Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the dependent backend JLV systems are up and operational
      - ii. Review each WebLogic-managed web server for connection and/or application errors
   c. Access and launch the JLV Universal Resource Locator (URL), also referred to as the Global Traffic Manager (GTM) URL [REDACTED] in a web browser
   d. Log in as a Veterans Health Administration (VHA) user with a VHA test account:
      - i. Verify that the JLV Login page displays as expected and that the system status indicates services are online and connected
   e. Log in as a Veterans Benefits Administration (VBA) Compensation and Pension Record Interchange (CAPRI)-Claims user with a VBA test account:
      - i. Verify that the JLV Login page displays as expected and that the system status indicates services are online and connected

2.1.1.1. System Startup from Emergency Shutdown

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

2.1.1.2. Enable SSOi Bypass on Apache Servers

JLV provides the capability to bypass the standard VA SSOi service. When bypass is enabled, users are prompted to use their PIV card certificate to authenticate against the JLV database.

Bypass is enabled by an operating system service swap, where the SSOi Apache service is stopped and the SSOi Bypass Apache service is started.

1. Enable SSOi Bypass
   a. Start bypass:
      i.   dzdo service ssoi stop
      ii. dzdo service ssoi-bypass start
   b. Start SSOi:
      i.   dzdo service ssoi-bypass stop
      ii. dzdo service ssoi start

2.1.2. System Shutdown

Shutdown procedures are performed during a published maintenance window, when there are fewer users accessing the system, to avoid impacting transactions in progress.

Use this shutdown sequence:

1. Shut down the SSOi servers
2. Shut down the JLV front-end web servers
3. Shut down the VDS servers
4. Shut down the jMeadows/Quality of Service (QoS) servers
5. Shut down the EHRM Service servers
6. Shut down the Report Builder servers
7. Shut down the DB servers

2.1.2.1. Emergency System Shutdown

Shut down all servers in any order.

A detailed list of the servers referenced throughout this POM can be found in the VA JLV Sharepoint site. JLV Sharepoint

2.1.3. Backup and Restore

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

The JLV DB can be recovered from an existing backup (.bak) file. Production systems are currently configured to back up the DB daily.

The active transaction log (known as the tail of the log) must be backed up under the full or bulk-logged recovery model before a DB can be restored in SSMS. Access to the certificate or asymmetric key that was used to encrypt the DB is needed to restore a DB that is encrypted. Without the certificate or asymmetric key, the DB cannot be restored. As a result, the certificate used to encrypt the DB key must be retained for as long as the backup is needed. IO maintains local and offline backups of the DB keys.

2.1.3.1. Backup Procedures

The backup of the JLV DB is configured to run, automatically, daily. The DB servers are backed up at the VA data centers by the AITC/PITC systems administrators, using the IO backup solution. The DB servers also have a MS SQL DB maintenance that automatically backs up the DB to the following location on each server:

- E:\DBBackups
- E:\DBBackups\TransactionLogs

A detailed list of the servers referenced throughout this POM can be found in the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

2.1.3.2. Restore Procedures

The items necessary for the recovery of the DBs are:

- DB backup (.bak) file of the JLV DB
- Backup of encryption keys for the JLV DB

Restore a full DB backup:

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

Figure 2: Database Names Tree

4. Click **Restore Database**
5. Use the **Source** section on the **General** page to specify the source and location of the backup sets to restore; select the following options:
   a. Click the **Browse** (...) button to open the **Select Backup Devices** dialog box
   b. Select **File** in the **Backup Media Type** box, then click **Add**
   c. Navigate to the location of the backup file (.bak) of the JLV DB, then click **OK**

d. After you add the devices you want to the **Backup Media Type** box, click **OK** to return to the **General** page

e. Select the name of the DB to restore (JLV) in the **Source: Device: Database** list box

Figure 3: Source/Device/Database Dialog Box
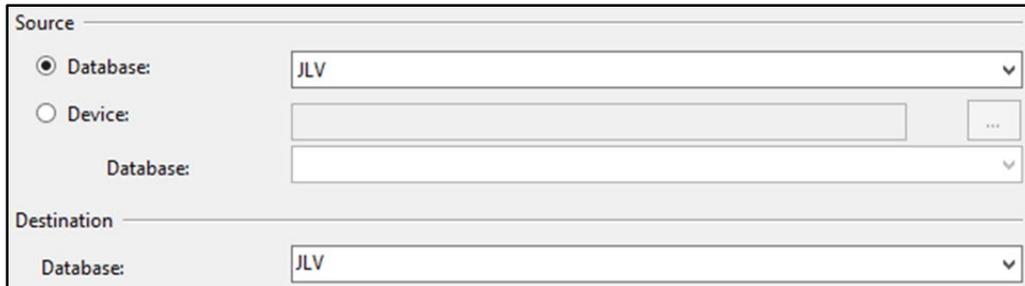
6. The **Database** box in the **Destination** section automatically populates with the name of the DB to be restored

a. Select JLV from the dropdown list

7. Leave the default as the last backup taken in the **Restore To** box, or click on **Timeline** to access the **Backup Timeline** dialog box to manually select a point in time to stop the recovery action

8. Select the backups to restore in the **Backup Sets to Restore** grid

a. This grid displays the backups available for the specified location

b. By default, a recovery plan is suggested; to override the suggested recovery plan, you can change the selections in the grid

Figure 4: Restore Plan Dialog Box

Figure REDACTED due to PII

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

9. Alternatively, click **Files** in the **Select a Page** pane to access the **Files** dialog box

a. Restore the DB to a new location by specifying a new restore destination for each file in the **Restore the database files as** grid

2.1.3.3. Backup Testing

Backups of all the Production VMs and DBs servers are done at the VA data centers by the PITC/AITC systems administrators. Backups are taken daily. Tests of those backups are done by IO. IO validates all software/configurations are restored from the expected configuration and confirms configuration files contain server specific settings. DB Backups are restored to the non-live backup DB servers to test restore procedures and integrity of the backup files. The testing of the DB restoration process is performed once every quarter and/or during each deployment of the JLV application. JLV administrators validate that data in the DB contains up-to-date entries for the user profiles and audit logging.

A detailed list of the servers referenced throughout this POM can be found in the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

JLV Support and IO confirm the application server starts as expected, which is validated through logs and through smoke test of the application. JLV Support and IO also validate DB operations through smoke test of the application.

2.1.3.4. Storage and Rotation

IO 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

JLV restricts access to the GUI to authorized users within the VA. Users access JLV via a URL.

Users are authenticated through the SSOi system, which allows them to link their Personal Identity Verification (PIV) card to their VistA account using their Access and Verify codes. Once linked, users may log in directly to the Patient Portal, with just their PIV and PIN and without their Access and Verify codes. When authenticating users with SSOi, JLV attempts to retrieve agency and site profile information from the SSOi system. When enabled, users are authenticated through SSOi (default).

SSOi Bypass is used as a failover authentication mechanism if Identity and Access Management's (IAM) SSOi services are unavailable. If SSOi Bypass (failover) is enabled, users must present their PIV card and Personal Identification Number (PIN) or their Windows authentication credentials before gaining access to the JLV Login page, where they will need to enter their Access and Verify codes.

PIV exempt users are prompted for their Windows username and password before continuing to the JLV Login page. If a user selects Windows authentication and is not PIV exempt, the authentication fails and the SSOi Bypass message, *"Access denied. You are not an authorized user."* appears.

JLV requires that VA users provide the following credentials at the Login page:

- **VHA/Clinical Users:** The user's local existing VistA Access and Verify codes
- **VBA/Benefits Users:** The user's existing National Claims VistA Access and Verify codes

Access control and authentication takes place before JLV displays any data. The user is authenticated to their host EHR system, granting them access to the presentation layer. jMeadows retrieves the user's profile information from the JLV DB based on their credentials. The user's default host location, custom widget layout, and other user data are returned. See [Access Control](#) for more information. [Table 2](#) provides a user authentication and login overview.

Table 2: User Authentication and Login Overview

User	Context Root	Authentication Overview
VBA/ CAPRI-Claims	/JLV	**The VA SSOi system is enabled for CAPRI users:** • The user is prompted to enter their PIV and PIN • CAPRI-Claims users are authenticated through SSOi • If the user's PIV is not linked to Claims (e.g., first time login), the user is prompted to identify their home site and will be asked to provide their Access/Verify login credentials on the Login page • If the user has linked their PIV to their home site (e.g., subsequent logins), JLV validates their credentials against their local VA Claims system **If SSOi Bypass is enabled (failover):** • VBA/CAPRI-Claims users are authenticated through JLV using their PIV and PIN • If a user is PIV exempt, the user is prompted for their Windows username and password • JLV receives the VBA/CAPRI-Claims user's e-mail address • The user enters their VistA/CAPRI Access and Verify codes in the Login page fields • JLV validates these credentials against the user's local VA system and users proceed to the JLV Provider Portal
VHA	/JLV	**When SSOi is enabled (default):** • VHA users are authenticated through SSOi using their PIV and PIN • IAM authenticates VHA users and users proceed to the JLV Provider Portal **If SSOi Bypass is enabled (failover):** • VHA users are authenticated through JLV using their PIV and PIN • If a user is PIV exempt, the user is prompted for their Windows username and password • JLV receives the VHA user's e-mail address • The user enters their VistA/CPRS Access and Verify codes in the Login page fields • JLV validates these credentials against the user's local VistA and users proceed to the JLV Provider Portal

2.2.1. Identity Management

Users with a valid VA PIV card and PIN can access JLV.

2.2.2. Access Control

JLV access control for VA users consists of IAM validating the user's PIV card and PIN (SSOi) or JLV validating the user's email address from the user's PIV card, PIV PIN, and CPRS or CAPRI access and verify codes (SSOi Bypass). If the user provides an invalid PIN or access and verify codes an error message is presented above the Access/Verify code fields on the Login page. Table 3 summarizes the JLV system components and the settings utilized for access control.

Table 3: Access Control Design

Component	Description
Configuration settings	A configuration setting within the *appconfig-production.properties* file that enables access control: • *Enable VA Access Control, On/Off*; This setting enables access control for VA users

2.3. User Notifications

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

🛈 **NOTE:** The VHA JLV team is responsible for notifying end users.

2.3.1. User Notification Points of Contact

Table 4 details the current notification list for alerting for VA stakeholders of JLV scheduled downtime. The list is maintained by JLV Support.

Table 4: JLV Scheduled Downtime Notification List (VA Stakeholders)

Name	Organization	Email Address
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED

Name	Organization	Email Address
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	SMS	REDACTED
REDACTED	SMS	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED

2.3.2. JLV QoS Mail Groups

VA: **Liberty Team:**

REDACTED   REDACTED

DOD:

REDACTED

2.3.3. Scheduled Downtime Notifications

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

> **ⓘ** **NOTE:** JLV Support depends on the receipt of timely information from dependent systems and infrastructure. Not all systems and/or infrastructure teams provide downtime notices to JLV Support. Detailed information, such as organization, frequency of planned downtime, and points of contact (POCs), is available in Appendices A, B, and C for each of the dependent systems and other infrastructure.

Figure 5 shows a typical calendar of regularly scheduled downtimes for JLV and external systems. Refer to the detailed list following the calendar mockup for a complete list of planned downtimes.

Figure 5: Mockup of Regularly Scheduled Downtimes
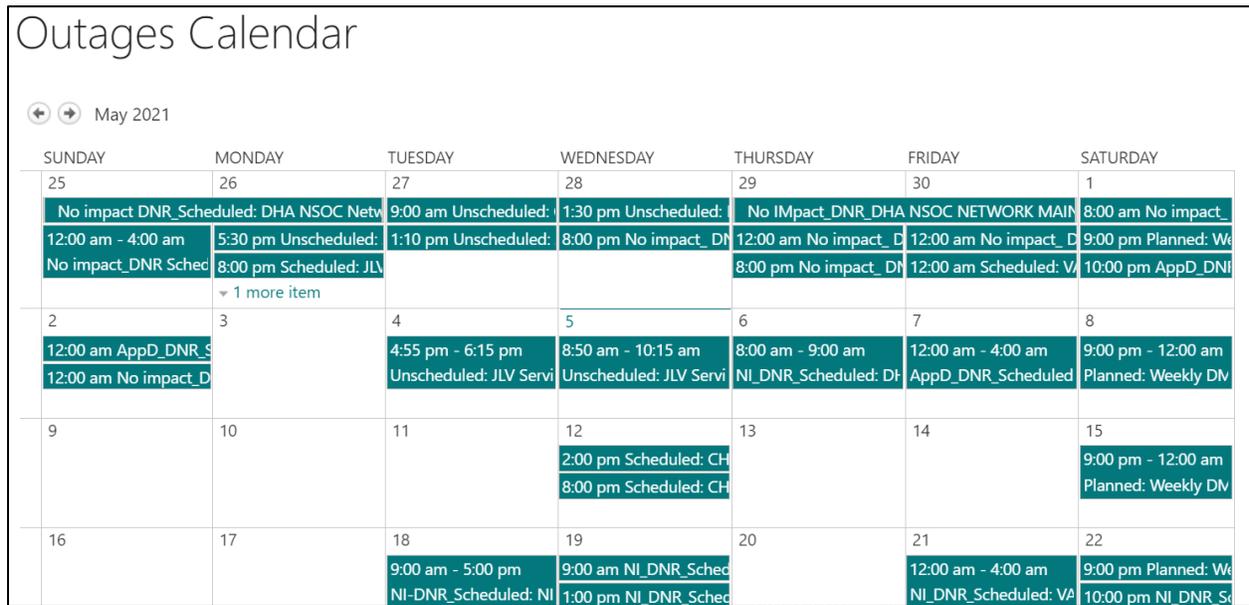
The following list details the maintenance notices currently known to JLV Support.

- **JLV**
  REDACTED
- **IO (AITC/PITC)**
  REDACTED
- **VA Authentication Federation Infrastructure (VAAFI)**
  REDACTED
- **MPI (VA and DOD)**
  REDACTED

- **VA/DOD Gateway**

  REDACTED

- **Military Health System (MHS) Enterprise Services Operations Center (MESOC) / Defense Information Systems Administration (DISA)**

  REDACTED

- **PDWS / Defense Manpower Data Center (DMDC)**

  REDACTED

- **CAPRI:** JLV Support does not currently receive a distribution notice

  REDACTED

- **VistAs:** JLV Support does not currently receive a distribution notice

  REDACTED

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

- 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 (see Table 4) when the JLV system is restored to service

The process flow shown in Figure 6 was designed primarily for *JLV code-driven patch releases* and is used 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 6: Scheduled Downtime Notification Process
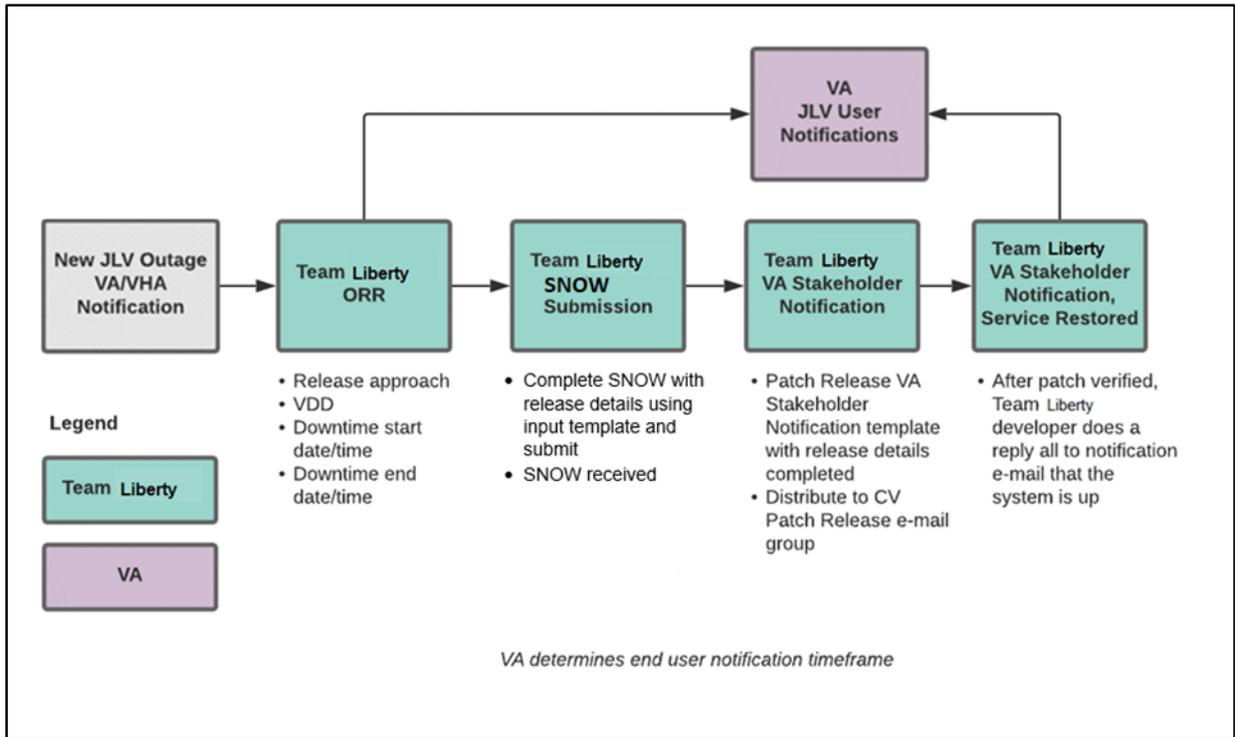
While all JLV scheduled downtime communications follow a similar format, each is tailored to the specific activity and system/service affected.

2.3.3.1. Service Now (SNOW) Process

2.3.3.1.1. Creating a new Release

Once the team has decided to develop and make available a group of changes as a Release, a person from the team will enter a new Release into Service Now.

For detailed instructions on how to add a new Release to SNOW, please consult the following work instruction: WI - How to Create a Release Request.

Figure 7: Service Now (SNOW) Process
Figure REDACTED due to PII

2.3.3.2. Patch Release Notification E-mail (Example)

All,

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

- The CHG number is **CHGxxxxx**
- The ServiceNow Ticket number is **INCxxxxxxx**
- JLV Enterprise Patch version x.x.x.x.x will be released to DOD and VA Production environments on <Day>, <Month> <Day>, <Year> starting at <Time 24-hour clock> (Time

am/pm) ET. Patching is expected to be completed by <u><Time 24-hour clock> (Time am/pm)</u> <u>ET, <Day>, <Month> <Day>, <Year></u>. JLV-Enterprise will be unavailable during this time.

2.3.4. Unscheduled Outage Notifications

2.3.4.1. Initial Response to Issues Within 30 Minutes of Alert

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

1. If a QoS e-mail is received and errors have **not** been cleared within 30 minutes of receipt of the initial error alert, proceed to Step 2
2. Within 30 minutes of the initial error e-mail, JLV Support (Table 14) sends an e-mail to the JLV stakeholders (Table 4), stating that the Support team is investigating the issue
   a. Using the e-mail example below, tailored to the specific activity and the system(s)/service(s) that are affected

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

Subject: JLV Outage Notification

All,

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

The error detail is: <Error from QoS>

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

- PDWS: the users' ability to perform a patient search
- MPI: the users' ability to retrieve VA records
- VDS: the users' ability for VA users to log in and retrieve VA records
- VistA Host: the ability for JLV to retrieve records for the specified host
- BHIE Relay Service (BRS): the users' ability to retrieve DOD records
- Database: the ability for the application to check the authorized users list, retrieve a user's profile, generate a site list for the log in, and the ability for JLV to log auditing records
- SnareWorks: the ability for DOD users to log in
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to JLV until service is restored
- CAPRI: the ability for JLV to authenticate VBA users
- BRS/DES: the users' ability to retrieve DOD, FEHR, and Community Partner records

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

Thank you.

2.3.4.2.   Outage Escalation to External Teams

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

1. Send an e-mail to the applicable external service group as specified in Table 14
2. Request the status of the issue within 2 hours of the initial alert
   a. Copy JLV Support (Table 14)
   b. Use the e-mail example(s) below, tailored to the specific activity and system(s)/service(s) that are affected

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

Subject: JLV Service Verification Request

All,

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

The error detail is: <Error from QoS>

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

- PDWS: the users' ability to perform a patient search
- MPI: the users' ability to retrieve VA records
- VDS: the VA users' ability to authenticate and to retrieve VA records
- VistA Host: the ability for JLV to retrieve records for the specified VistA host
- CAPRI: the ability for JLV to authenticate VBA users
- BRS/DES: the users' ability to retrieve DOD, FEHR, and Community Partner records
- SnareWorks: the ability for DOD users to authenticate
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to JLV until service is restored

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

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

Thank you for your assistance in troubleshooting this issue.

1. Generate a trouble ticket (VA or DOD) and assign it to the appropriate application team
2. Send a notification to the JLV stakeholders (Table 4) with all pertinent information
   a. Use the e-mail example(s) below, tailored to the specific activity and system(s)/service(s) that are affected

2.3.4.2.2.   Outage Update E-Mail (Example)

Subject ALERT: JLV Service Degradation - (Affected Service) errors - (insert error start time YYYYMMDD 24:00 ET)

All,

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

The error detail is: <Error from QoS>

- PDWS: the users' ability to perform a patient search
- MPI: the users' ability to retrieve VA records
- VDS: the VA users' ability to authenticate and to retrieve VA records
- VistA Host: the ability for JLV to retrieve records for the specified VistA host
- CAPRI: the ability for JLV to authenticate VBA users
- BRS/DES: the users' ability to retrieve DOD, FEHR, and Community Partner records
- SnareWorks: the ability for DOD users to authenticate
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to JLV until service is restored

The JLV Engineering team has determined the following:

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

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

Thank you.

1. Continue monitoring the issue
2. Provide updates every **2 hours** to the JLV stakeholders (Table 4) until issue is resolved:
   a. REDACTED
   b. REDACTED
   c. REDACTED
   d. REDACTED
   e. REDACTED

JLV Support Hours: 24x7x365

2.3.5. Announcement Banners

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

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

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

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

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

The following announcement banners are prioritized:

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

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

1. Display announcement banners by severity
    a. Add a prefix category (Patient Safety, Issue, Outage, Maintenance, etc.) to the announcement banner titles and content to further differentiate context and priority
2. Post only those alerts that impact end users
    a. Informational announcement banners for maintenance events where there is no expected or an inconsequential impact should not be posted
3. Set an expiration date for announcement banners, and remove them as soon as possible after the event has completed or the issue has been corrected

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

- JLV Project Support Team: Maintenance-related notifications that impact end users
- VHA JLV Team: Notifications regarding patient safety and other critical issues that impact end users

Table 5 lists the announcement banner content for maintenance events with expected user impact and for special events and issues.

Table 5: Announcement Banner Content for Maintenance Events Impacting End Users

Maintenance Event Titles (50-character limit)	"More" Hyperlink Expanded Content (255-character limit)
MAINTENANCE DOD Patient Identity System-5/17-5/18 **More**	**Maintenance window:** 05/17/18 9pm ET–05/18/18 12pm ET **Impact:** JLV will be available for use, but users may experience problems with patient lookups/patient search using DOD EDIPI or issues viewing DOD patient demographics.
MAINTENANCE VA Patient Identity System -5/17 **More**	**Maintenance window:** 05/17/18 9pm ET–05/18/18 12pm ET **Impact:** Users may experience problems with patient search: CPRS via CCOW may display VA data only; DOD EDIPI or recently viewed list may display DOD data only; SSN[2] searches may display no data.
MAINTENANCE DOD Theater Records System– 5/21-5/22 **More**	**Maintenance window:** 05/21/18 9pm ET–05/22/18 12pm ET **Impact:** Records from DOD theater systems may be unavailable. These include records from an area where military events were occurring at the time of care delivery (e.g., wartime).
MAINTENANCE Community Partner System—6/29 **More**	**Maintenance window:** 06/29/18 8pm ET–06/29/18 11 pm ET **Impact:** JLV will be available for use, but the Community Health Summaries & Documents widget may not retrieve records. If you experience this problem, please try again later.
ISSUE Please Check Federal EHR/MHS GENESIS Widget Date Filter	An error caused Federal EHR/MHS GENESIS widgets added to workspaces before 6/28/18 to display only the past 4 months instead of 1/1/17-present. To correct this, click the funnel-shaped filter icon and manually adjust the dates or close/re-add the widget.
PATIENT SAFETY Contrast Allergies	JLV is currently not displaying VA allergies for Contrast media entered through the Radiology option "Update Patient Record" [RA PTEDIT]. Until further notice, please use CPRS RDV to check for Contrast allergies from other VA sites.
ISSUE Imaging not available to Claims/CAPRI users	VA images are not currently being displayed in JLV. The issue is being analyzed and a patch to resolve the issue will be deployed as soon as possible. Please use a standalone AWIV for VA imaging access. **NOTE:** Affects VBA (Claims) Only
OUTAGE Community Partner Records	VA is currently unable to retrieve records from community partners. Engineers are working to restore connections as quickly as possible. (add details on anticipated resolution, etc. if available).

2.3.5.1. Placing Announcement Banners

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

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

---

[2] Social Security Number (SSN)

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

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

The resulting announcement banner, as viewed on the application Login page, is shown in Figure 8.

Figure 8: User-facing Banner on the JLV Login Page
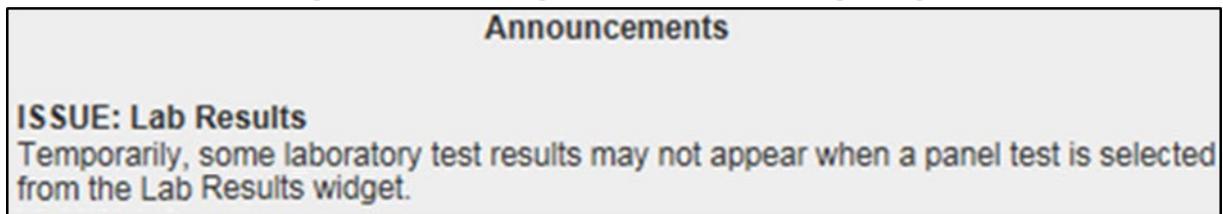
2.3.5.2.   Removing Announcement Banners

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

2.3.5.2.1.   Manual Removal

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

Manual removal is accomplished by accessing the DB tables and manually changing the end date (shown in red text below) to match the start date associated with the announcement banner to be removed. Database entries demonstrating the announcement banner prior to (Table 6) and after (Table 7) manual removal follow.

Table 6: Database Table Entry Prior to Manual Removal

Start Date	End Date	Title	Announcement Banner Text
2018-10-17	2018-10-30	ISSUE: Lab Results	Temporarily, some laboratory test results may not appear when a panel test is selected from the Lab Results widget.

Table 7: Database Table Entry After Manual Removal

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

2.3.5.2.2. Automatic Expiration

Automatic expiration of an announcement banner occurs when the designated end date (shown in red text below) of the announcement banner has been reached. Expiration dates are set based on when the issue can be resolved by an authorized member of JLV Support. A DB entry demonstrating a planned maintenance announcement banner is shown in Table 8.

Table 8: Database Table Entry for a Planned Maintenance Announcement Banner

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

2.3.5.3. Announcement Banner Extensions

If a service degradation or other event will exceed the planned end date (shown in red text below) of an existing announcement banner, JLV Support can manually extend the duration of the announcement banner by changing the end date (shown in red text below) to a date in the future. Database entries demonstrating the announcement banner prior to (Table 9) and after a date extension (Table 10) follow.

Table 9: Database Table Entry as Initially Posted

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

Table 10: Database Table Entry After a Date Extension Update

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

2.4. System Monitoring, Reporting, and Tools

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

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

2.4.1. Dataflow Diagram

The data retrieval sequence is detailed in the *JLV 2.9.4 System Design Document*. Once approved, all project documentation is available on the VA JLV Product Repository on GitHub. See Administrative Procedures for the link to the repository.

2.4.2. Availability Monitoring

QoS monitors the health of JLV and checks for the availability or disruption of dependent services within the systems in DOD and/or VA environments (Table 11: Services Monitored by QoS).

Table 11: Services Monitored by QoS

Service	Description
DMDC PDWS	Patient look up
MPI (VA)	Retrieves VA patient ID
BRS (DES)	Connects to DES and DOD VLER
JLV DB Server	Contains JLV DB information
jMeadows Data Service	Connects to MPI, PDWS, DB, BRS, EHRM Service, and Report Builder
VDS	VA Log in/Data
EHRM Service	Connects to jMeadows, Joint HIE via Fast Healthcare Interoperability Resources (FHIR), and Cerner Millennium via Cerner FHIR Application Program Interface (API)

Figure 9: System Status Check Sequence
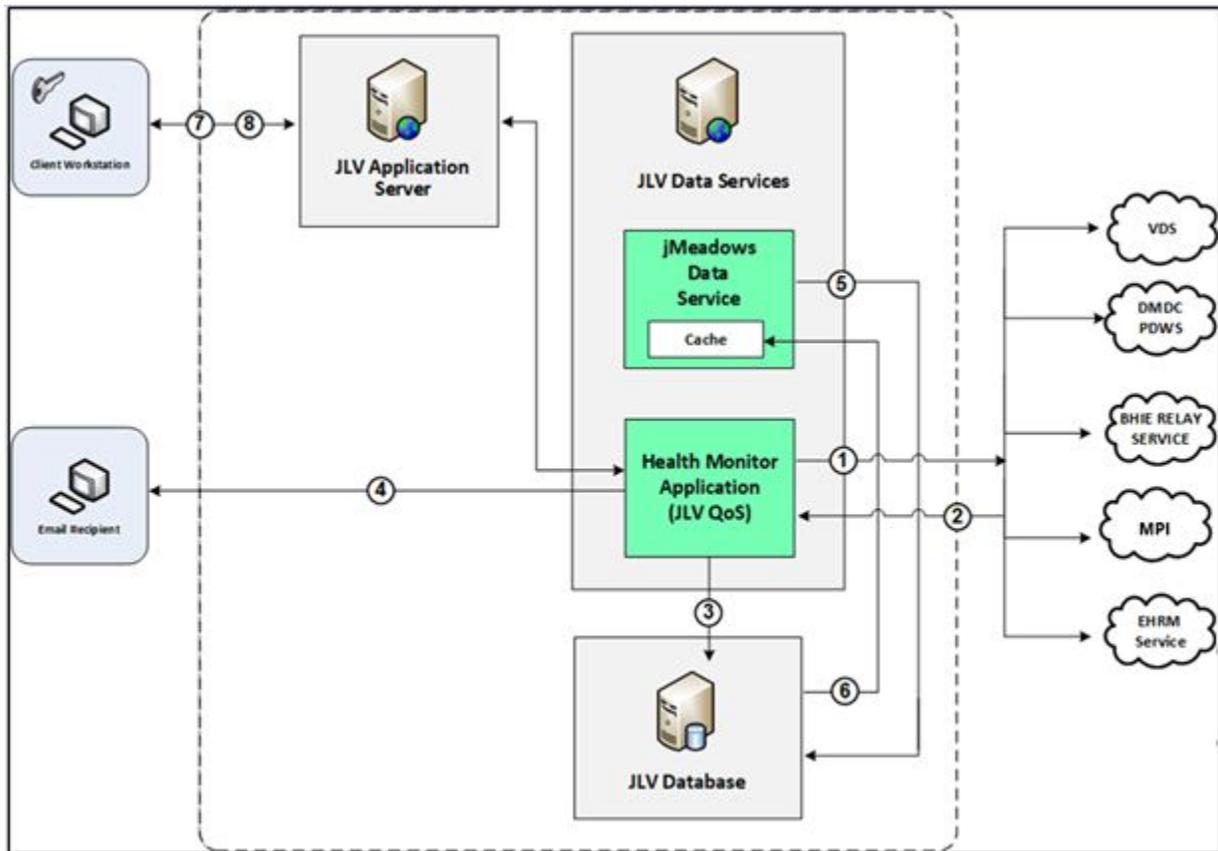
System status checks ([Figure 9](#)) are performed as follows:

1. The Health Monitor pings the monitored services every 5 minutes
2. The Health Monitor receives a system status from each monitored service and reports the status of JLV systems to JLV Support via e-mail
3. System status events are written to the QOS_LOGS table within the JLV DB
4. The Health Monitor sends an automated e-mail notification every 6 hours, unless a status change is detected
    a. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset
    b. The next e-mail is generated after 6 hours if no further system status changes are detected
    c. When all errors are cleared, an e-mail is sent stating that no errors are detected
5. The jMeadows Data Service pings the JLV DB every 2 minutes for status checks
6. The jMeadows Data Service stores the data returned from the JLV DB in an internal cache, the jMeadows Data Service cache
7. When a user accesses the JLV **Login** page, JLV requests and receives system status data from the jMeadows Data Service cache
8. During active user sessions, JLV requests system status data from the jMeadows Data Service cache every 5 minutes

a. Current system status is retrieved from the cache and sent to the JLV GUI

Figure 10 depicts a system status message displayed on the JLV **Login** page.

Figure 10: System Status Message on the JLV Login Page

Figure REDACTED due to PII

Figure 11 shows a system error status displayed on the JLV **Patient** portal page, which presents only if the system status is yellow or red. If the system does not detect a service connection error, no notice displays.

Figure 11: System Status Message on the Patient Portal Page
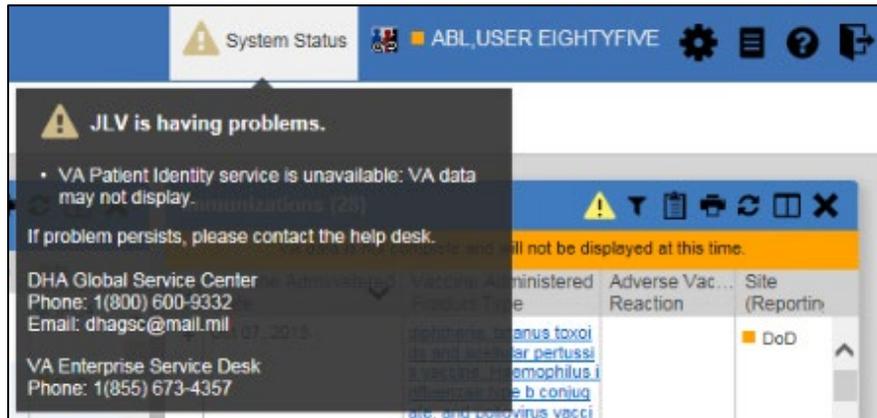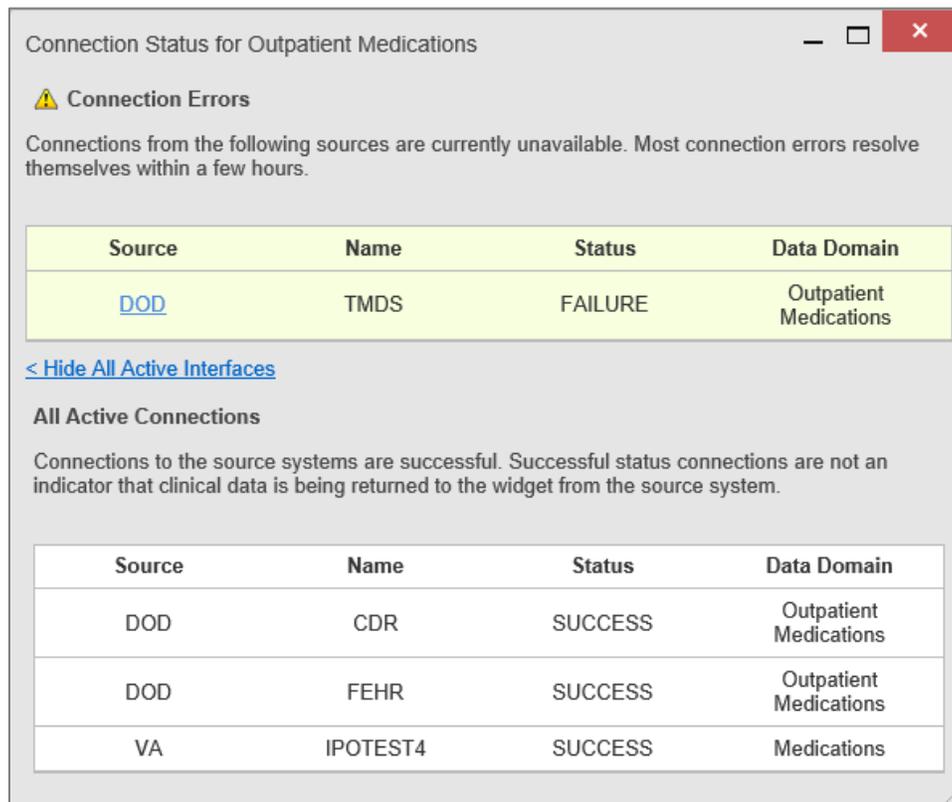

2.4.2.1.   Domain-Level Availability Monitoring

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

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

Both icons are used to provide status for VA, DOD, and community partner data sources. Clicking the status icon opens interface status details in a separate window, as shown in Figure 12.

Figure 12: Connection Status Details

2.4.3. Performance/Capacity Monitoring

Query times for each web service call in to the Relay Service, jMeadows, EHRM Service, and VDS are recorded to a file in the D:\Log directory on the server, where the services are installed. Refer to 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 multiple views in the same user session. When a user opens and closes a sensitive record, then reopens 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 SSN
- User PIV, if known, for VA users
- User location
- Patient last name, first name, middle initial (MI), SSN, MPI, date of birth (DOB)
- Sensitive data accessed
- Date/time of access
- Reason for access (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, shown in Figure 13.

Figure 13: Patching Process for VA and DOD Components
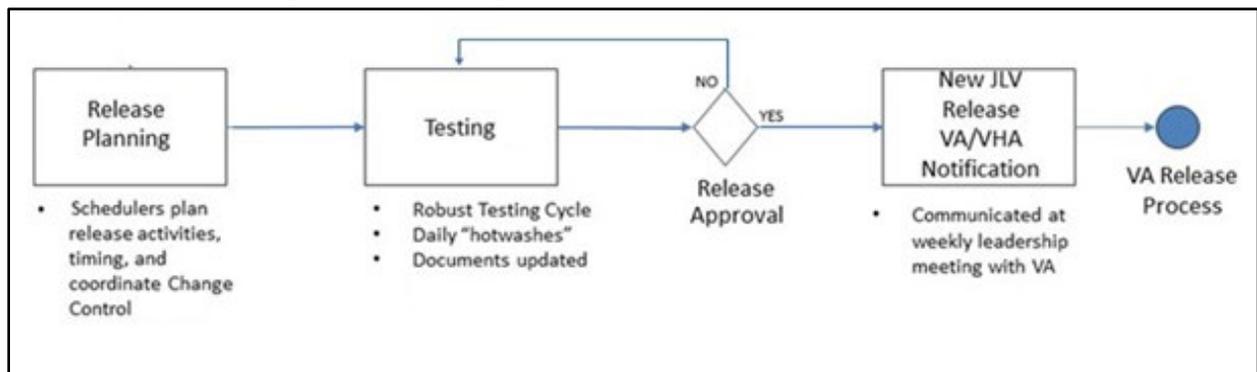
2.5.2. Extracts

Extracts of the JLV audit logs and server logs are available by request only, on an as-needed basis. The VA project manager (PM) must approve requests for extracts. Approvals are dependent on the type of request and the organization of the requester. Once a request is approved, an authorized system administrator extracts the requested data and sends it to the requestor via an encrypted method. Refer to Application Error Logs for more information on audit and server logs.

2.5.3. Purges

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

2.6. Scheduled Maintenance

Scheduled downtime typically occurs after 08:00 pm ET, and service is restored by 8:00 am ET. Any planned downtimes, (within VA control), outside of these hours requires justification and approval by the VHA JLV Team and the Office of Information and Technology (OIT) PM.

Figure 14 depicts the JLV process for monitoring, analyzing, and initiating the notification for an outage.

ℹ️   **NOTE:** IAM/SSOi Bypass is not monitored in this release.

Figure 14: Scheduled Downtime and Unscheduled Outage Overview
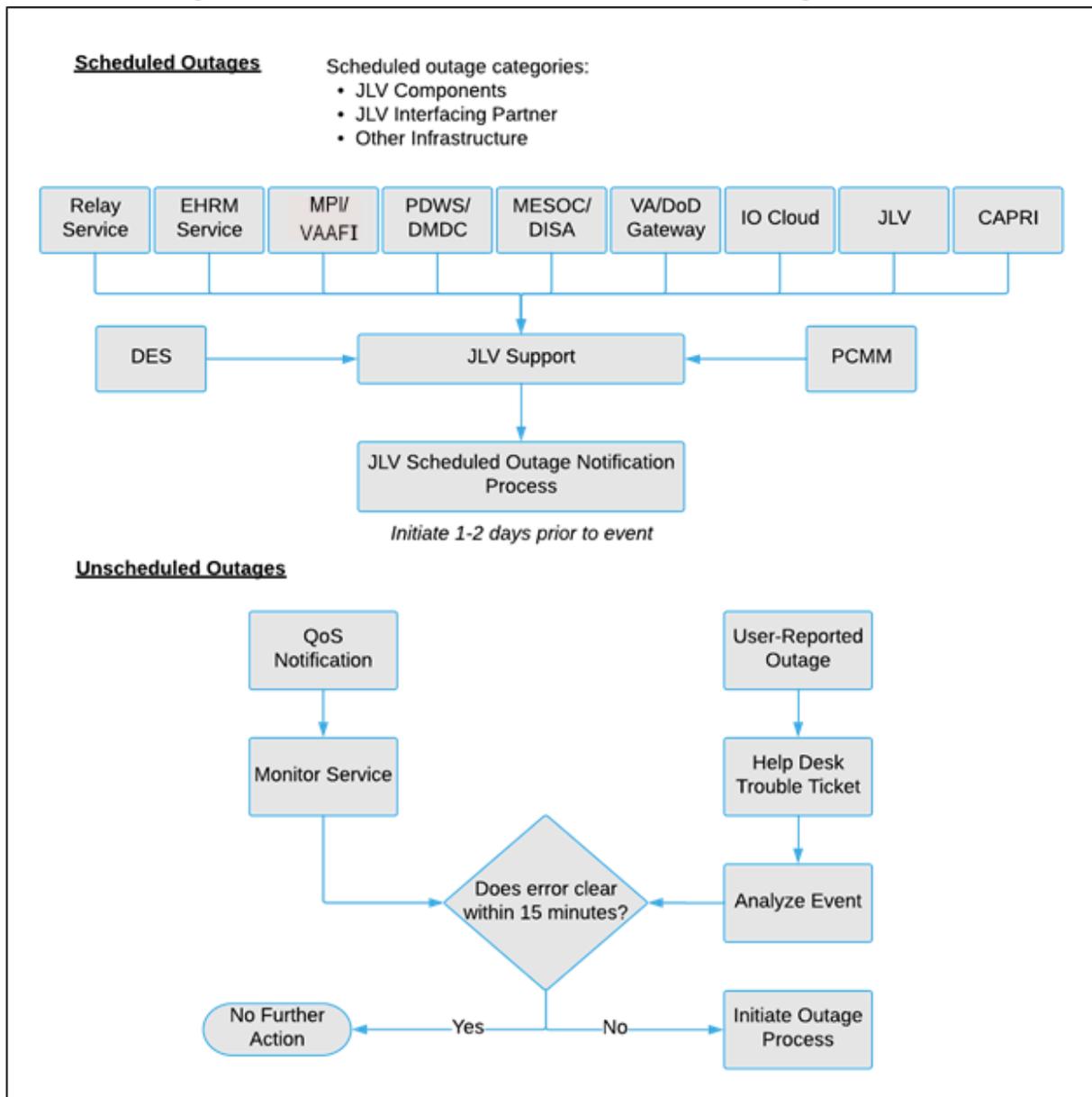
2.7.   Unscheduled Outage Triage Process

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

ℹ️   **NOTE:** The QoS tool is the primary means of monitoring the JLV application. The processes described in the following sections are specific

to the QoS tool and its related incident responses. The VHA JLV team is responsible for notifying end users.

2.7.1. Outage Triage Timeline

The JLV outage triage process is executed by JLV Support in coordination with the VA JLV interface systems teams (e.g., MPI), as necessary.

The following steps represent routine system monitoring:

1. Monitor e-mail to see if the JLV application corrects itself
   a. Wait 15 minutes to see if a QoS e-mail arrives indicating that there are no errors (e.g., *Cloud—JLVQoS Report: NO ERRORS DETECTED)*
   b. Check junk e-mail folder for QoS alerts
2. If a QoS e-mail is received indicating "*NO ERRORS DETECTED,"* the system is connected and executing properly

Figure 15: Outage Event Activities and Timeline
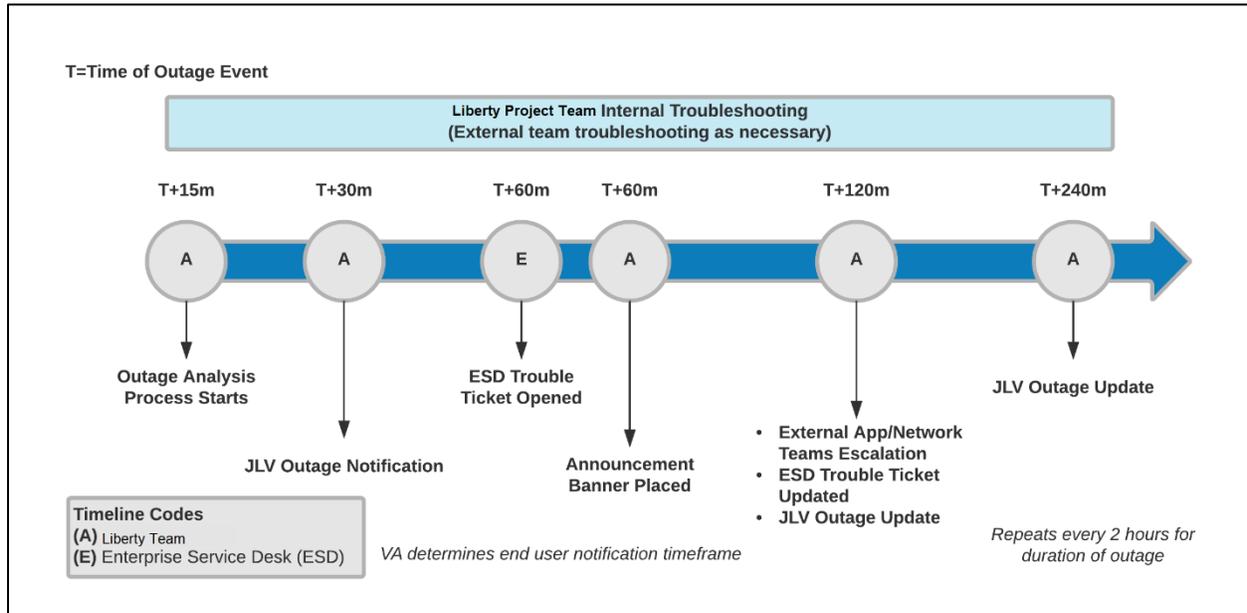
2.7.2. Escalation

The escalation process typically follows this progression:

1. The problem is reported
   a. QoS reports a problem that remains unresolved for over 30 minutes (See [Availability Monitoring](#))
   -OR-
   b. A JLV user calls the ESD and opens a trouble ticket

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

2. JLV Support analyzes the problem and determines whether to initiate the triage process
3. Once the triage process is initiated, JLV Support follows the analysis and notification timeline and escalation (as necessary) processes, and includes external systems teams ([Figure 15](#))

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

2.7.3. Issue Resolution and After Action

The following steps are taken after the issue is resolved:

1. After the issue is resolved, determine if the root cause was *internal* to the JLV application
   a. If the problem was with an *external system/service*, obtain the root cause from the applicable team ([Table 14](#))
2. Send an e-mail to the JLV stakeholders ([Table 4](#)) stating that JLV is back online and available for use
   a. Include the root cause of the issue and details of the fix required to resolve the issue, if available

2.8. Capacity Planning

JLV monitors the application performance, user onboarding, and user behaviors on a weekly basis. Server resources and JLV application data are collected by the enterprise monitoring group, using the AppDynamics monitoring tools. AppDynamics monitors and stores data and sends alerts to notify members of an e-mail distribution group when any metric exceeds its upper or lower boundary.

2.8.1. Initial Capacity Plan

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

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 users and do not compromise the operational state of the system. Most errors are transient in nature and are resolved by the user trying to execute an operation again. The following subsections describe these errors, their causes, and what, if any, response an operator should take.

3.1. Routine Errors

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

3.1.1. Security Errors

One possible security error an end user may encounter is an invalid login error. Causes of such an error include the user attempting to access JLV before they are authorized to do so (*Access denied. You are not an authorized user.)* or mistyping their Access and/or Verify code (*Invalid Access/Verify Codes*). A user's login credentials will be locked by the VistA service to which JLV connects after five incorrect login attempts (*Device/Internet Protocol (IP) address is locked due to too many invalid sign-on attempts.*). If this occurs, the user contacts the ESD and opens a service request ticket. The user's local VistA administrator can unlock their account.

3.1.2. Timeouts

Each subsection describes a possible timeout error.
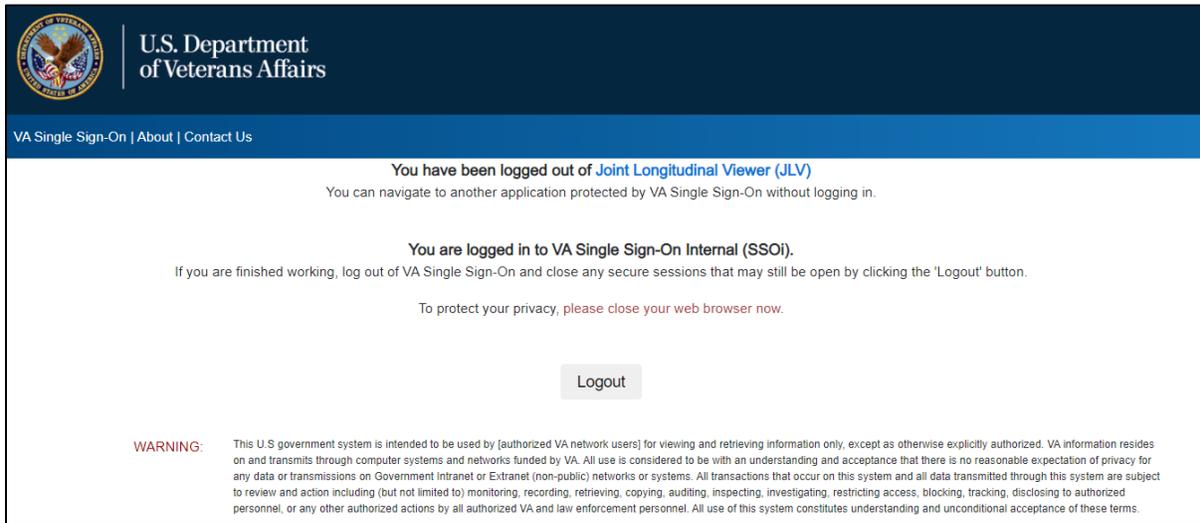
3.1.2.1. Application Timeout

JLV has a timeout feature that is set to 60 minutes of inactivity. If users leave the JLV application idle for 55 minutes, they receive the Session Timeout Notification (Figure 16). If the user would like to extend the session, they can click the OK button to continue using JLV.

Figure 16: Session Timeout Notification
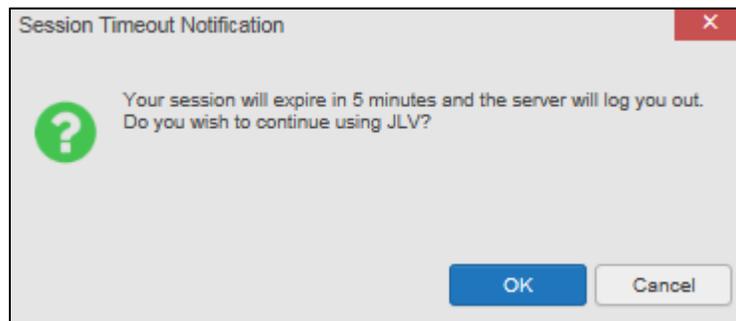
If the user does not interact with the Session Timeout Notification message within the 60-minute time limit, the JLV session times out (Figure 17). The user must then close the browser, reopen the browser, and log back in to JLV.

Figure 17: Session Timeout (SSOi)

3.1.2.2.   Connection Errors

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

Either the JLV Support team or the active site's system administrators may attempt to remote desktop in to each JLV application server to ensure the WebLogic services are running. If they are running, system administrators contact IO to verify that the GTM is operating correctly.

JLV may also report timeouts to external systems within widgets by displaying a message that one or more data sources could not be connected (Figure 18).

Figure 18: Connection Error

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

3.1.3.   Concurrency

Resolution of concurrent EHR access is handled by the underlying system of record that is being queried. The JLV Engineering team optimizes the stored procedures for user profiles in the DB to avoid concurrency contention, based on application and system metrics, degradation, and user load. Remediation depends on the identified root cause.

3.2.   Significant Errors

Significant errors are defined as errors or conditions that affect 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 JLV. 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 logins, and the identity of the information system component where the event occurred.

Each time an attempt is made to interface with jMeadows, whether it is a service communication or a user searching for a patient, the activity is logged and stored in the JLV DB. The purpose of retention is for traceability; specifically, to show what calls/actions were made, where, by whom, and when they terminated. Each query for data is audited and each has the user ID linked to it. Only one audit log is produced that contains both VA and DOD user IDs and user names.

Query times for each web service call in to the Relay Service, jMeadows, and VDS are recorded to a file in the D:\Log directory on the server, where the services are installed. A log file output for the jMeadows Data Service can be seen in Figure 19. Table 12 lists response time log locations.

Table 12: Response Time Log Location

Data Service	Log File Name
EHRM Service	(hostname)_ehrm-sql.txt
jMeadows Data Service	(hostname)_jmeadows-sql.txt
Relay Service	bhie-sql.txt
VDS	(hostname)_vds-sql.txt

Figure 19: jMeadows Log Output

The QoS service deployed with JLV monitors the availability of the 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 DB and are displayed in JLV.

Service interruptions detected by the QoS service are reported to JLV Support and IO via e-mail. An automated e-mail notification is sent every 6 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset. The next e-mail is generated after 6 hours if no further system status changes are detected. The QoS service does not send service interruption notices to external systems or services.

For detailed information on service interruption notifications and sample e-mail messages, please see the system design specifications and diagrams that can be found in the VA JLV Product Repository on GitHub. See Administrative Procedures for the link to the repository.

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

3.2.3. Services Infrastructure Errors

3.2.3.1. DB

The JLV DB is a relational DB used to store user profile information and audit data. It also stores VA and DOD terminology mappings (both local terminology and national standards). The DB does NOT store, neither long term nor temporarily, patient or provider EHRs from VA, DOD, and community partner data through the Joint HIE.

The JLV DB sits on a dedicated server within a deployed JLV environment, alongside the server hosting the JLV application and VDS (Figure 20). Only the JLV application and components of the JLV system, including the jMeadows Data Service, connect to and utilize the JLV DB.

Figure 20: JLV Architecture and Components[3]

---
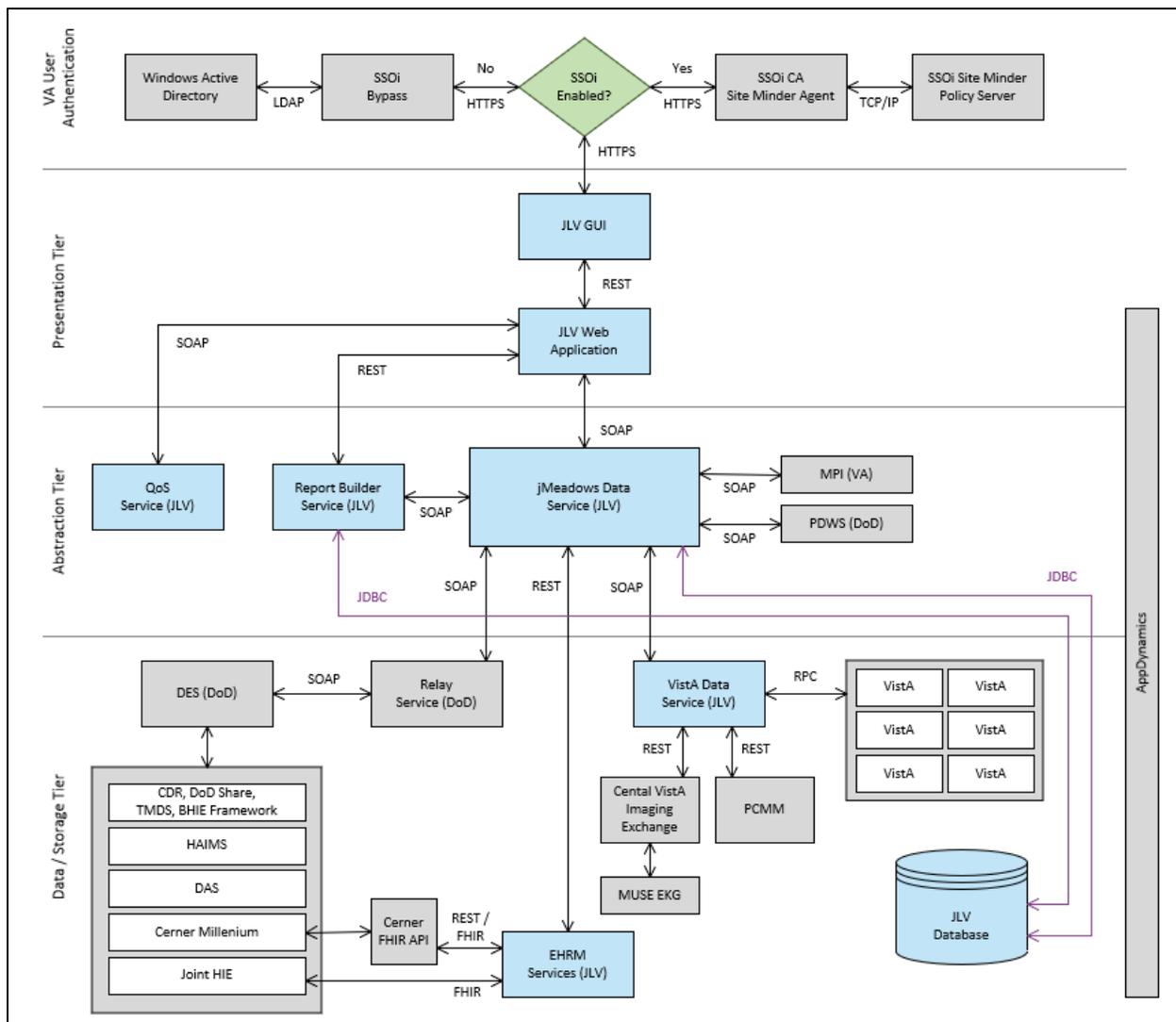
[3] Active Directory (AD), Computer Associates (CA), Central VistA Imaging Exchange (CVIX), Data Access Service (DAS), Enterprise Common Access Card (CAC) Registration Service (ECRS), Electronic Health Record

For detailed information about errors and events for the SQL Server DB Engine, please see the website [MS Developer Network Database Engine Events and Errors](#).[4]

The JLV DB has a table to audit user actions within the application within the AUDIT DB table. This table collects system usage data and provides the JLV Support team the ability to create reports and extract pertinent information from the DB, as needed. A sample of the Audit log can be seen in [Figure 21](#).

Figure 21: Audit Log

Figure REDACTED due to PII

3.2.3.2.   Web Server

JLV uses Oracle WebLogic as its web server in the VA environment. JLV does not implement any custom WebLogic error handling or reporting. Please refer to the [Oracle WebLogic Server Error Messages Reference](#)[5] for more information.

3.2.3.3.   Application Server

JLV uses Oracle WebLogic as its application server in the VA environment. JLV does not implement any custom WebLogic for error handling or reporting. Please refer to the Oracle WebLogic Server Error Messages Reference for more information. See [Web Server](#) for the link to the resource.

3.2.3.4.   Network

JLV utilizes the network infrastructure provided at 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 (A&A)

Users must provide their PIV and PIN to log in via SSOi. If credentials are not found the message, "*Not a valid Access Code/Verify Code pair*" displays.

A&A error messages are:

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

A detailed overview of the login process from the user's perspective is provided in the *JLV 2.9 User Guide*. Once approved, all project documentation is available on the VA JLV Product

---

Modernization (EHRM), Healthcare Artifact and Image Management Solution (HAIMS), HyperText Transfer Protocol Secure (HTTPS), Java DB Connectivity (JDBC), Lightweight Directory Access Protocol (LDAP), Military Health System (MHS), Remote Procedure Calls (RPCs), REpresentational State Transfer (REST), Simple Object Access Protocol (SOAP), Transmission Control Protocol (TCP)

[4] https://msdn.microsoft.com/en-us/library/ms365212(v=sql.110).aspx
[5] https://docs.oracle.com/middleware/11119/wls/WLMCT/RMI.html

Repository on GitHub. See Administrative Procedures for the link to the repository, and refer to Security/Identity Management for detailed information.

3.2.3.6. Logical and Physical Descriptions

System design specifications and diagrams can be found in the VA JLV Product Repository on GitHub. See Administrative Procedures for the link to the repository.

3.3. Dependent System(s) and Services

Table 13: JLV Dependent Systems and Services 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. Tier 3 system engineers follow a triage process to determine the root cause of the error and coordinate with the Point of Contact (POC) for the external systems, as needed.

Table 13: JLV Dependent Systems and Services

Other VA System	Related Error(s)
BRS	**DOD, Federal EHR, and Community Partner data in widgets is currently unavailable**. The source connection is down and DOD, Cerner, and community partner records of all types from all sites may not display.
Cerner FHIR API	**Federal EHR (Cerner) is currently unavailable.** The source connection is down and some Federal EHR data may not display.
CVIX	If the CVIX service is not available, a message states, *"There was an issue retrieving the CVIX URL."*
LDAP	This service is used between the SSOi Bypass Service and Windows Active Directory within VA environments for the purposes of authenticating PIV cards and PINs when SSOi is unavailable.
MPI	The JLV QoS Service monitors MPI availability. When MPI is unavailable, the message, *"MPI Service may be offline or unavailable,"* is shown in System Status. Refer to Domain-Level Availability Monitoring.
Primary Care Management Module (PCMM)	If PCMM is unavailable, JLV displays the error message: "**The connection to PCMM is unavailable.** The patient's assigned clinical teams may not display."
Site VistA instances	VistA connection errors are reported through interface status notifications for each clinical domain. Refer to Domain-Level Availability Monitoring.
SSOi	If this service is enabled and the SSOi Policy Server is not available, VA users cannot gain access to JLV.

3.4. Troubleshooting

Tier 1 troubleshooting contact information can be found in CA SDM by searching for *JLV* in the **Knowledge** tab. Tier 1 troubleshooting support is handled through the ESD at 855-673-4357. Refer to Table 14 for additional contact information.

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

Tier 3 support and troubleshooting is handled directly by JLV Support.

3.5. System Recovery

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

3.5.1. Restart After an Unscheduled System Interruption

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

3.5.2. Restart after DB Restore

Refer to System Startup for the system startup procedures.

3.5.3. Backout Procedures

Backout procedures vary depending on the specific release. Please see the *JLV Deployment, Installation, Backout, and Rollback Guide* specific to the version to be backed out for more information. Once approved, all project documentation is available on the VA JLV Product Repository on GitHub. See Administrative Procedures for the link to the repository.

3.5.4. Rollback Procedures

Rollback procedures are dependent on each specific release. Please see the *JLV DIBRG* specific to the version to be rolled back for more information. Once approved, all project documentation is available on the VA JLV Product Repository on GitHub. See Administrative Procedures for the link to the repository.

4. Operations and Maintenance Responsibilities

Operations and maintenance roles and responsibilities for JLV are summarized in Table 14.

Table 14: Operations and Maintenance Responsibility Matrix

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
REDACTED	Tier 1 support for VA Users	REDACTED	REDACTED
REDACTED	Tier 1 support for DOD Users	REDACTED	REDACTED
VA JLV Project Office	**VA OIT and VHA Stakeholders**		
REDACTED	JLV PM	REDACTED	REDACTED
REDACTED	Program Specialist	REDACTED	REDACTED
REDACTED	Senior JLV Analyst	REDACTED	REDACTED
REDACTED	Program Analyst	REDACTED	REDACTED
REDACTED	Senior Clinical Subject Matter Expert		REDACTED

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
REDACTED	CLIN 3		REDACTED
DOD JLV Project Office	**DMIX Stakeholders**		
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
Liberty Team	**JLV Support**		
REDACTED	Contract Program Manager (PgM)	REDACTED	REDACTED
REDACTED	Contract PM	REDACTED	REDACTED
REDACTED	Contract PM	REDACTED	REDACTED
REDACTED	JLV Operations Lead	REDACTED	REDACTED
REDACTED	JLV Operations	REDACTED	REDACTED
REDACTED	JLV Operations	REDACTED	REDACTED
REDACTED	JLV Operations	REDACTED	REDACTED
REDACTED	JLV Operations	REDACTED	REDACTED
DMDC	**PDWS Technical Issues and Support Contacts**	**703-578-5050**	
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
DES	**DOD Adapter Technical Issues and Support Contacts**		
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
DOD DISA	**Technical Issues and Support Contacts**		
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
VAAFI	**Data Power Technical Issues and Support Contacts**		
REDACTED	VAAFI Lead	REDACTED	REDACTED
REDACTED	Deputy PM SSOi	REDACTED	REDACTED
REDACTED	VAAFI	REDACTED	REDACTED
REDACTED		REDACTED	REDACTED

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
IO	**Technical Issues/ Support Contacts**	**N/A**	**N/A**
REDACTED	Analyst	REDACTED	REDACTED
REDACTED	WebLogic / Java Admin	REDACTED	REDACTED
REDACTED	Windows Admin	REDACTED	REDACTED
REDACTED	Linux Admin	REDACTED	REDACTED
MPI (VA)	**Technical Issues/ Support Contacts**	**N/A**	**In VA Remedy assigned under: VA - Development - DEV-Person Service**
REDACTED	Lead Developer/ Architect	REDACTED	REDACTED
REDACTED	MPI point of contact	REDACTED	REDACTED
REDACTED	MPI point of contact	REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED	VistA Imaging	REDACTED	REDACTED
VA Network—NSOC	**Technical Issues/Support Contacts**	REDACTED	**In VA Remedy: VA NSOC Business Partner Extranet (BPE) Operations -OR- Network Support Center (NSC) BPE Operations VANSOCBPEOperations@va.gov**
REDACTED	Triple-I/VA-NSOC	REDACTED	REDACTED
DOD Network Space & Naval Warfare Systems (SPAWAR) Virtual Private Network (VPN)	**Technical Issues and Support Contacts**		**In VA Remedy: SPAWARVPN**
REDACTED		REDACTED	REDACTED
REDACTED			REDACTED
DOD NSOC	**Technical Issues and Support Contacts**	800-600-9332 Option 9, then 3, then 2	
REDACTED			REDACTED

Appendix A.   Approval Signatures

Signed:_____

REDACTED

Signed:_____

REDACTED

Appendix B.   Acronyms and Abbreviations

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

Table 15: Acronyms and Abbreviations

Acronym	Description
A&A	Authentication and Authorization
AD	Active Directory
AITC	Austin Information Technology Center
API	Application Program Interface
APM	Application Performance Management
BHIE	Bidirectional Health Information Exchange
BPE	Business Partner Extranet
BRS	BHIE Relay Service
CA	Computer Associates
CAC	Common Access Card
CAPRI	Compensation and Pension Records Interchange
CDR	Clinical Data Repository
CHCS	Composite Health Care System
CHG	Change Order
CVIX	Central VistA Imaging Exchange
DAS	Data Access Service
DB	Database
DES	Data Exchange Service
DIBRG	Deployment, Installation, Backout, and Rollback
DISA	Defense Information Systems Administration
DMDC	Defense Manpower Data Center
DMIX	Defense Medical Information Exchange
DOB	Date of Birth
DOD	Department of Defense
ECRS	Enterprise CAC Registration Service
EHR	Electronic Health Record
EHRM	Electronic Health Records Modernization
ESD	Enterprise Service Desk
FEHR	Federal Electronic Health Record
FHIR	Fast Healthcare Interoperability Resources
GB	Gigabytes
GUI	Graphical User Interface
GTM	Global Traffic Manager

Acronym	Description
HAIMS	Healthcare Artifact and Image Management Solution
HIE	Health Information Exchange
HPS	Health Product Support
HTML	Hypertext Markup Language
HTTPS	HyperText Transfer Protocol Secure
IAM	Identity and Access Management
ICN	Integration Control Number
IEN	Internal Entry Number
IO	Infrastructure Operations
IP	Internet Protocol
JDBC	Java Database Connectivity
JLV	Joint Longitudinal Viewer
LDAP	Lightweight Directory Access Protocol
MedCOI	Medical Community of Interest
MESOC	MHS Enterprise Services Operations Center
MHS	Military Health System
MI	Middle Initial
MS	Microsoft
MPI	Master Person Index
NSC	Network Support Center
NSOC	Network Security Operations Center
OIT	Office of Information Technology
ORR	Outage Readiness Review
PCMM	Primary Care Management Module
PDWS	Patient Discovery Web Service
PHI	Protected Health Information
PIN	Personal Identification Number
PITC	Philadelphia Information Technology Center
PIV	Personal Identity Verification
PM	Project Manager
POC	Point of Contact
POM	Production Operations Manual
QoS	Quality of Service
RAM	Random Access Memory
REST	REpresentational State Transfer
RPC	Remote Procedure Call
SDM	Service Desk Manager
SNOW	Service Now

Acronym	Description
SOAP	Simple Object Access Protocol
SPAWAR	Space and Naval Warfare Systems
SQL	MS Structured Query Language
SSMS	SQL Server Management Studio
SSN	Social Security Number
SSOi	Single Sign on Internal
TCP	Transmission Control Protocol
TMDS	Theater Medical Data Store
URL	Universal Resource Locator
VA	Department of Veterans Affairs
VAAFI	VA Authentication Federation Infrastructure
VBA	Veterans Benefits Administration
VDS	VistA Data Service
VHA	Veterans Health Administration
VistA	Veterans Information Systems and Technology Architecture
VM	Virtual Machine
VPN	Virtual Private Network