VistA Imaging Exchange (VIX) Viewer Improvements

MAG*3.0*303

Production Operations Manual (POM)

November 2022

Version 5.0

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
11/01/2022	5.0	Update for MAG*3.0*303	VA IT VistA Imaging Technical team
06/01/2022	4.2	Updates for MAG*3.0*269 release date.	VA IT VistA Imaging Technical team
02/18/2022	4.1	Update for MAG*3.0*269 name	VA IT VistA Imaging Technical team
11/04/2021	4.0	Update for MAG*3.0*269	VA IT VistA Imaging Technical team
08/31/2021	3.0	Update for MAG*3.0*284	REDACTED
01/07/2021	2.0	Update for MAG*3.0*254	VA IT VistA Imaging Technical team
05/21/2020	1.0	Update for MAG*3.0*249	REDACTED
03/13/2019	0.15	Update for MAG*3.0*230	REDACTED
12/21/2018	0.10	Updated for MAG*3.0*221	REDACTED
4/11/2018	0.9	Updated for MAG*3.0*201	REDACTED
4/5/2018	0.8	Additional MAG*3.0*197 Updates	REDACTED
1/19/2018	0.7	Updated for MAG*3.0*197	REDACTED
11/14/2017	0.6	Additional MAG*3.0*185 Updates	REDACTED
10/17/2017	0.5	Updated for MAG*3.0*185	REDACTED
5/8/2017	0.4	Date and other minor updates	REDACTED
3/27/2017	0.3	Updated for MAG*3.0*177	REDACTED
2/10/2017	0.2	Initial draft	Development Team
9/23/2016	0.1	Initial draft	Development Team

NOTE: The revision history cycle begins once changes or enhancements are requested after the Production Operations Manual has been baselined.

Artifact Rationale

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

Table of Contents

1.   Introduction

This document explains how to maintain and administer the Veterans Health Information Systems and Technology Architecture (VistA) Imaging Exchange (VIX) service. The VIX is used to facilitate data sharing and exchange across organizational and functional boundaries. Currently, the VIX's primary purpose is to support image sharing between the Department of Veterans Affairs (VA) medical facilities and between VA and the Department of Defense (DoD) medical facilities. It is anticipated that the VIX's role will be expanded to support data sharing and exchange within a facility and between facilities. This document assumes that the VIX is installed and configured. For information about VIX system requirements, installation, and configuration, see the *[MAG*3.0*303 VIX Installation Guide.](#)*

1.1.   Intended Audience

This document is intended for VA staff responsible for managing a local VIX. It describes how remote VIXes log access to locally stored images. This document presumes a working knowledge of the VistA environment, VistA Imaging components and workflow, and Windows server administration.

2.   Routine Operations

2.1.   Administrative Procedures

2.1.1.   System Start-up

See the *VIX Administrator's Guide and the MAG*3.0*303 VIX Installation Guide.*

2.1.1.1.   System Start-Up from Emergency Shut-Down

See the *VIX Administrator's Guide and the MAG*3.0*303 VIX Installation Guide.*

2.1.2.   System Shut-down

See the *VIX Administrator's Guide and the MAG*3.0*303 VIX Installation Guide.*

2.1.2.1.   Emergency System Shut-down

See the *VIX Administrator's Guide and the MAG*3.0*303 VIX Installation Guide.*

2.1.3.   Back-up & Release

2.1.3.1.   Back-up Procedures

See the *VIX Administrator's Guide*

2.1.3.2.   Restore Procedures

N/A

2.1.3.3.   Back-up Testing

N/A

2.1.3.4.   Storage and Rotation

N/A

2.2.   Security / Identity Management

See the *VIX Administrator's Guide*

2.2.1.   Identity Management

See the *VIX Administrator's Guide*

2.2.2.   Access control

See the *VIX Administrator's Guide*

2.2.3.   VIX Interfaces

See the *VIX Administrator's Guide*

2.2.4.   Other VIX Components

See the *VIX Administrator's Guide*

2.2.5.   VIX Security Certificate

See the *VIX Administrator's Guide*

2.3. User Notifications

2.3.1. User Notification Points of Contact

Table 1: User Notification Points of Contact

Name	Organization	Phone	URL	Method (email/phone)	Priority	Time
REDACTED	REDACTED	REDACTED	REDACTED	Phone	Tier 3	N/A

2.4. System Monitoring, Reporting & Tools

See the *VIX Administrator's Guide*

2.4.1. Dataflow Diagram

See the *VIX Administrator's Guide*

2.4.2. Availability Monitoring

See the *VIX Administrator's Guide*

2.4.3. Performance/Capacity Monitoring

System performance can be assessed by the response times experienced by the end-user. The system resources are self-managed. The cache is sized not to exceed available storage sizes.

2.4.4. Critical Metrics

Table 2: Critical Metrics

System Accessibility	24/7
System Uptime	Based on VistA uptime
Online Operational Performance	Aggregate image throughput >5 Mb/s
Production Incidents	Fewer than 1/month

2.5. Routine Updates, Extracts, and Purges

N/A

2.6. Scheduled Maintenance

N/A

2.7. Capacity Planning

N/A

2.7.1. Initial Capacity Plan

The hardware was sized to service the estimated user demand based on an estimated number of requests during peak usage.

3. Exception Handling

Site personnel are expected to contact the Health, Clinical Services Diagnostics Team (previously known as Clin 3, the group name is SPM.Health.ClinSvs.Diag) via a Service Now ticket to resolve operation errors. Programmatic problems are triaged to developers.

3.1. Routine Errors

The system 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.

While the occasional occurrence of these errors may be routine, a large number of errors over a short period of time is an indication of a more serious problem. In that case, many errors need to be treated as an exceptional condition.

3.1.1. Security Errors

Since the system is a component of a larger system that is responsible for user-level security, it is expected that all errors related to security are handled by the controlling application. All security failures (e.g., inability to access resources or stored objects) are generally caused by the controlling application either incorrectly passing security tokens or failing user authentication. Other security issues are under the jurisdiction of the site VistA Imaging security that has already established protocols and procedures.

3.1.2. Time-outs

See the *VIX Administrator's Guide*

3.1.3. Concurrency

N/A

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 resolving significant errors, conditions, or other issues.

3.2.1. Application Error Logs

See the *VIX Administrator's Guide*

3.2.2. Application Error Codes and Descriptions

See *Section 3.2.1: Application Error Logs*

3.2.3. Infrastructure Errors

N/A

3.2.3.1. Database

The application installs SQLite a Structured Query Language (SQL) database that is completely self-managed. There are no site interactions required to maintain this database. The purpose of the database is to manage cached objects. The complete loss of this database is not a failure as it gets repopulated with each caching operation. The amount of data stored in the database and the cache is managed by the application based on available storage. No specific database errors are identified.

3.2.3.2. Web Server

Web Services are provided by the VIX using already deployed components. No other Commercial-Off-The-Shelf (COTS) components are required. Refer to the *VIX Administrator's Guide* for specific errors.

3.2.3.3. Application Server

N/A

3.2.3.4. Network

N/A

3.2.3.5. Authentication & Authorization

Refer to the *VIX Administrator's Guide.* The VIX services use pass-through authentication via security tokens. Errors manifest themselves as the inability to load images. Correction of these errors involve the controlling application or altering the site-specific settings in VistA Imaging.

3.2.3.6. Logical and Physical Descriptions

N/A

3.3. Dependent System(s)

The VIX Viewer is part of VistA Imaging components. The main system dependency is on VistA. Inability to access Vista is logged in the VIX logs, and alerts are sent via email.

3.4. Troubleshooting

Errors manifest themselves as the inability to load images. A review of the VIX error logs and transaction logs is the only tool available on the VIX to troubleshoot these conditions. Refer to the *VIX Administrator's Guide* for further details.

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

See *Section 2.1.1: System Start-up and Shut Down*

3.5.2. Restart after Database Restore

N/A

3.5.3. Back-out Procedures

However, if it is necessary to uninstall the MAG*3.0*303 VistA KIDS, you need to select the "Kernel Installation & Distribution System" menu option, "Backup a Transport Global" (see section 4.8.1, Step 4c of *MAG*3.0*303 Deployment, Installation, Back-Out, and Rollback Guide.*), before you uninstall the patch.

Administrators will need to use the PackMan function INSTALL/CHECK MESSAGE. Check MailMan messages for the backup message sent by the "Backup a Transport Global" function executed before the patch install.

1.   Select the **inbox** message shown below:

Backup of MAG*3.0*303 install on *mmm dd, yyyy   installer user name*

2.   Select the Xtract PackMan option.

3.   Select the Install/Check Message option.

4.   Enter "Yes" at the prompt.

5.   Enter "No" at the backup prompt. There is no need to back up the backup.

Enter message action (in IN basket): Ignore// Xtract PackMan

Select the PackMan function: ?

   Answer with PackMan function NUMBER, or NAME

   Choose from:

  1   ROUTINE LOAD

  2   GLOBAL LOAD

  3   PACKAGE LOAD

  4   SUMMARIZE MESSAGE

  5   PRINT MESSAGE

  6   INSTALL/CHECK MESSAGE

  7   INSTALL SELECTED ROUTINE(S)

  8   TEXT PRINT/DISPLAY

  9   COMPARE MESSAGE

Select PackMan function: Select PackMan function: 6 INSTALL/CHECK MESSAGE

Warning: Installing this message will cause a permanent update of globals

and routines.

Do you really want to do this? NO// YES<Enter>

Routines are the only parts that are backed up. NO other parts

are backed up, not even globals. You may use the 'Summarize Message'

option of PackMan to see what parts the message contains.

Those parts that are not routines should be backed up separately

if they need to be preserved.

Shall I preserve the routines on disk in a separate backup message? YES// NO

No backup message built.

Line 2   Message #42925   Unloading Routine   MAGxxxx (PACKMAN_BACKUP)

Select PackMan function: **<Enter>**

3.5.4.   Rollback Procedures

If it is necessary to uninstall the MAG*3.0*303 VIX, go to the Control Panel, choose Add/Remove Programs, and remove the MAG*3.0*303 VIX Service Installation Wizard. To backout the VIX and replace it with the prior version which was included in MAG*3.0*269, please see the *MAG*3.0*303 VIX Installation Guide* for more detail

4. Operations and Maintenance Responsibilities/RACI

This responsibility matrix defines the roles and responsibilities for supporting VistA patches as part of a deployed solution. This is a template of the standard support structure required for VistA patches; therefore, the Project Manager (PM) should note any deviations in responsibility from this standardized Field Operations responsibility matrix in the Operational Acceptance Plan (OAP).

VistA Patching is generally relegated to the sustainment of existing solutions but may also include emergency "hotfix" patches designed to remediate a noted deficiency within the solution. This Responsibility Matrix (Responsible, Accountable, Consulted, Informed, or RACI) (Table 3) is related to VistA patches released and supported at the national level (known as "Class I" patches), which are distributed to the entire Enterprise after testing and release management has been completed. VistA Patches are released via the FORUM, KERNEL, or via Secure File Transfer Protocol (SFTP) directly to the Field.

Table 3: Responsibility Matrix

	R	A	C	I
Entities involved with VistA Patching:				
SL = OI&T Service Lines	x			x
NSD = OI&T National Service Desk				
FCIO = Facility Chief Information Officer				x
SL = OI&T Service Lines				x
Application Service Line (**SL-ASL**)				x
SL = OI&T Service Lines				x
Core Systems Service Line (SL-Core)				
PS = OI&T Product Support				x
VHA = Local Facility medical staff (customer)				x

	R	A	C	I
FO = Field Operations				x
PD = OI&T Product Developer	x			
DSO = VHA Decision Support Office				x
HPS = Health Product Support		x		
Support				
Tier 1: NSD	x			
Tier 2: (local OI&T – FCIO/SL-ASL)	x			
Tier 3: HPS	x			
Tier 4: PD/Maintenance	x			

FO VistA Patching Responsibility Matrix	Production Environments
Application development	PD
Release Management	HPS
Rollback Plan	PD
Application installation	FCIO/SL-ASL
Application support	NSD, FCIO, SL, HPS, Vendor
Client/Server Update (where applicable)	SL-Core
OS Patching (where applicable)	SL-Core
Change Management	SL-ASL
Application Administration (Operations and Maintenance)	SL-ASL
Local Training for Front Line Staff	VHA
National Training (where applicable)	DSO

5. Approval Signatures

REVIEW DATE:

SCRIBE:

<mark>REDACTED</mark>   <mark>REDACTED</mark>

Signed: _____

Portfolio Director   Date

<mark>REDACTED</mark>   <mark>REDACTED</mark>

Signed: _____

Product Owner   Date

<mark>REDACTED</mark>   <mark>REDACTED</mark>

Signed: _____

Receiving Organization POC (Operations Support)   Date

<mark>REDACTED</mark>   <mark>REDACTED</mark>

Signed: _____

Operations Support POC   Date

<mark>REDACTED</mark>   <mark>REDACTED</mark>

Signed: _____

Project Manager   Date

A. References

- *[MAG*3.0*303 Deployment, Installation, Back-Out, and Rollback Plan](#)*
- *[VIX Administrator's Guide](#)*

B. Acronyms

Acronym	Definition
COTS	Commercial Off The Shelf
CVIX	Central Vista Imaging Exchange
DoD	Department of Defense
KIDS	Kernel Installation and Distribution System
OAP	Operational Acceptance Plan
PM	Program Manager
POM	Production Operations Manual
RACI	Responsible, Accountable, Consulted Informed
SFTP	Secure File Transfer Protocol
SQL	Structured Query Language
VA	Department of Veterans Affairs
VistA	Veterans Health Information Systems and Technology Architecture
VIX	VistA Imaging Exchange