VistA Audit Solution (VAS 1.0)
Deployment, Installation, Back-out, and Rollback Guide

February 2023

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
02/15/2023	1.9	Minor updates to document	VAS Team
10/22/2022	1.8	Updated document	VAS Team
03/01/2022	1.7	Updated document	VAS Team
02/17/2022	1.6	Updates throughout document	VAS Team
02/15/2022	1.6	Updated Sections 3.2.1, 3.3.3.	VAS Team
10/20/2021	1.5	Updated Sections 4,5 and 6	VAS Team
10/14/2021	1.4	Updated Sections 2,3, 3.1, 3.3.4	VAS Team
10/1/2021	1.3	Updated Sections 3 & 3.2.2	VAS Team
09/13/2021	1.2	Updated Sections 1.2, 1.3, 3.2, 3.2 and added Section 8 for Acronyms	VAS Team
08/18/2021	1.1	Updated Sections 4.5 and 4.8	VAS Team
06/24/2021	1.0	Initial Issue	VAS Team

Table of Contents

List of Tables

1 Introduction

The Veterans Information System and Technology Architecture (VistA) Audit Solution (VAS) is a real-time web-based interface.

It provides a nationwide Health Insurance Portability and Accountability Act (HIPAA) compliant Audit Tracking Solution with the ability to track and report on access logs for patient's Personal Identifiable Information (PII)/ Protected Health Information (PHI) data across all VistA instances. VAS end-users are Privacy Officers (PO) and Information Systems Security Officers (ISSO) and their authorized representatives who need the ability to view the log of Create, Read, Update and/or Delete (CRUD) operations on patient information to respond to Freedom of Information Act (FOIA), HIPAA, employee and Inspector General (IG) requests. This data originates from VistA and flows through in-memory database servers to be stored in the Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS). VAS web-based User Interface will access and display the data stored in AWS.

Authorized VAS users may view the patient data that was accessed and modified as well as the individual that performed the actions.

1.1 Purpose

The VAS Deployment, Installation, Back-Out, Rollback Guide v1.0 documents the steps and procedures required to deploy and install various components of VAS 1.0.

1.2 Dependencies

There are three dependencies for VAS 1.0 are:

- Hardware Requirements
- Software Requirements
- Installation of DG*5.3*964 patch

1.3 Constraints

To deploy into the target physical environment, installers require following access:

- A Personal Identity Verification (PIV) card for Authentication
- Zero account access is required for authorization to install and deploy software configuration changes on the systems
- Electronic Permission Access System (ePAS) authorization to the environment
- Secure Shell (SSH) key for environment access

2 Roles and Responsibilities

Table 1: DIBRG Roles and Responsibilities

Team	Phase/Role	Tasks	Project Phase
Austin Information Technology Center (AITC)	Deployment	Direct and manage all activities including orderly shutdown, startup, configuration, and deployment tasks	Planning
Philadelphia Information Technology Center (PITC)	Deployment	Direct and manage all activities including orderly shutdown, startup, configuration, and deployment tasks	Planning
Veterans Affairs Enterprise Cloud (VAEC)	Deployment	Provides GovCloud support for AWS services	Planning
OIT Enterprise Program Management Office (EPMO)	Deployment	Participate in planning meetings, communicate to stakeholders the start/end of deployment and pertinent details of the current status of the System of Systems	Planning
VA Office of Information and Technology (OIT), VA OIT Health Product Support, and Project Management Office (PMO)	Deployment	Plan and schedule deployment (including orchestration with vendors)	Planning
Local individual Veterans Administration Medical Centers (VAMCs)	Deployment	Determine and document the roles and responsibilities of those involved in the deployment	Planning
Field Testing (Initial Operating Capability (IOC)), Health Product Support Testing	Deployment	Test for operational readiness	Completed
Health Product Support and Field Operations	Deployment	Execute deployment	Deployment
VAMCs	Installation	Plan and schedule installation	Deployment
VAS ATO Team	Installation	Obtain authority to operate and that certificate authority security documentation is in place	Deployment
VAS Team	Installation	Coordinate knowledge transfer with the team responsible for user training	Deployment
VAS Team	Post-Deployment	Hardware, Software, and System Support	Warranty

3 Deployment

Deployment is planned as a concurrent online rollout. Detailed deployment information for the VAS 1.0 User Interface is located in the Department of Veterans Affairs Github repository for VAS. Detailed instructions for creating a new GitHub account and requestion access to the VA organization's GitHub can be reviewed in the VA GitHub Handbook.

WEBS is the VistA namespace assigned for VAS and all releases involving VAS will be communicated nationally to VistA sites through the release of informational WEBS patches. The initial release of VAS 1.0 is being released with patch WEBS*1*1 and DG*5.3*964.

3.1 Timeline

The deployment and installation are scheduled to run for a period of thirty (30) days. The deployment of the VAS User Interface will be accomplished in conjunction with the installation and national release of VistA patch DG*5.3*964.

3.2 Site Readiness Assessment

The deployment is taking place within the REDACTED on AITC and PITC sites. The target servers are on-premises machines and REDACTED. The site names and locations are listed in section 3.2.2.

3.2.1 Deployment Topology (Targeted Architecture)

The current detailed architecture information for VAS 1.0 is available in the Department of Veterans Affairs Github repository for VAS.

3.2.2 Site Information (Locations, Deployment Recipients)

The deployment is taking place at the following data centers:
- AITC
- PITC
- AWS

The Initial Operating Capability (IOC) Test Sites are:
- Cloud Sites
  - VA Texas Valley Coastal Bend Health Care System, Harlingen TX (740)
- On Premises (On-Prem) Sites
  - Central Arkansas Veterans Healthcare System John L. McClellan Memorial Veterans Hospital, Little Rock AR (598)
  - James A. Haley Veterans' Hospital, Tampa FL (673)

3.2.3 Site Preparation

No special preparation is required by the site prior to deployment.

3.3 Resources

The list of the resources are as follows:

3.3.1 Facility Specifics

There are no facility-specific features required for deployment.

3.3.2 Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table 2: Hardware Requirements

Required Hardware	Model	Version	Configuration	Manufacturer	Other
REDACTED	REDACTED	REDACTED	REDACTED		N/A
REDACTED	REDACTED	REDACTED	REDACTED		N/A

3.3.3 Software

Detailed software requirements for VAS 1.0 can be reviewed as part of the REDACTED in the VAS GitHub repository.

3.3.4 Communications

Sites participating in IOC field testing will use the "Patch Tracking" Outlook message to communicate with the VAS team, the developers, and product support personnel.

3.3.4.1 Deployment / Installation / Back-out Checklist

The assigned Health Information Governance (HIG) team will deploy the WEBS*1*1 and DG*5.3*964 patches, which are tracked nationally for all Veterans Administration Medical Centers (VAMCs) in the National Patch Module (NPM) in FORUM. FORUM automatically tracks the patches as they are installed in the different VAMC production systems. A report in FORUM can be run to identify when the patch was installed in VistA production at each site. A report can also be run to identify which sites have not currently installed the patch in their VistA production system. Therefore Table 3 below is not needed to manually track installation.

Table 3: Deployment / Installation / Back-out Checklist

Activity	Day	Time	Individual who completed task
Deploy	N/A	N/A	N/A
Install	N/A	N/A	N/A
Back-Out	N/A	N/A	N/A

4 Installation

4.1 Pre-installation and System Requirements

All requirements are available in the Department of Veterans Affairs Github repository for VAS (code) Readme folder.

4.1.1 Patch Dependencies

Patch DG*5.3*964 must be installed for VAS 1.0

4.2 Platform Installation and Preparation

All requirements are available in the Department of Veterans Affairs Github repository for VAS (code) Readme folder.

4.3 Download and Extract Files

Actions to download and extract files does not apply to VAS 1.0.

4.4 Database Creation

The required DG*5.3*964 patch updates an existing VistA database and therefore this section is not applicable.

The details are in the README (Code Repository) in GitHub for VAS .

4.5 Installation Scripts

Any Installation Scripts are in Github repository for VAS.

4.6 Cron Scripts

Any Cron scripts are available in GitHub repository for VAS.

4.7 Access Requirements and Skills Needed for the Installation

An individual will require access to the National VA Network, Veterans Affairs Organization GitHub access, as well as access to the VAS-Code private GitHub repository.

Additionally, a full-spectrum Developer with advanced knowledge and skills in Knowledge system, Docker Containers, AWS, databases, Apache hypertext server, and Linux system administration. An AWS Administrator is required to resolve any issue for COPY command.

If COPY command error(s) are received, then a ServiceNow (SNOW) ticket will need to be submitted to resolve COPY command error(s).

4.8 Installation Procedure

4.8.1 Redis Enterprise Installation Procedure

All the Redis Enterprise Installation Procedure are located in GitHub repository for VAS. For convenience steps are stated below:

1) Download the installation package of the Redis Enterprise Software from any of the supported platform on Redis Labs

        a.   Prepare to install on Linux

             i.   Disable Linux swap on all nodes by running the below commands

            ii.   sudo swapoff -a

          iii.   sudo sed -i.bak '/ swap / s/^(.*)$/#1/g' /etc/fstab

2) Install Redis Software on Linux

        a.   Extract the .tar installation file and make sure to be in the right directory. Run command: tar vxf <tarfile name>

        b.   Finally, to install Redis Enterprise Software,

             i.   Execute: sudo ./install.sh -y

3) Setup a three-node cluster on Redis Enterprise user interface

        a.   By navigating to https://<Server IP address of Redis Software>:8443 for example https://10.224.155.107:8443 where 10.224.155.107 is the server IP in which Redis Software has been installed.

        b.   Join other nodes to cluster after creating the cluster on master node.

4) Create Redis Database (DB) VistA Audit Solution (VAS) DB on the UI and configure endpoints and replication on the cluster

4.9 Installation Verification Procedure

The software is set up and configured in the central enterprise wide server. Hence no installation verification is required.

4.10 System Configuration

The individual Microservice configuration is available in the Department of Veterans Affairs Github repository for VAS (code).

4.11 Data Tuning

Database Tuning does not apply.

5 Back-out Procedure

Within context of this document, the term back-out pertains to a return to the last known good operation state of the software and appropriate platform settings. This does not apply for VAS 1.0 as the application resides in the Cloud.

6 Rollback Procedure

This section does not apply to VAS 1.0 as the application is in the Cloud.

Appendix A: Acronyms

Table 4: Acronym Listing

Acronym	Definition
AITC	Austin Information Technology Center
AWS	Amazon Web Services
CRUD	Create, Read/Inquire, Update, and Delete
DG	Registration package
DIBRG	Deployment, Installation, Back-Out, and Rollback Guide
ePAS	Electronic Permission Access System
EPMO	Enterprise Program Management Office
FOIA	Freedom Of Information Act
GUI	Graphic User Interface
HCS	Healthcare System
HIG	Health Information Governance
HIPAA	Health Insurance Portability and Accountability Act
IG	Inspector General
IOC	Initial Operating Capability
ISSO	Information System Security Officer
MUMPS	Massachusetts General Hospital Utility Multi-Programming System
N/A	Not Applicable
NPM	National Patch Module
OIT	Office of Information & Technology
PHI	Protected Health Information
PII	Personal Identifiable Information
PITC	Philadelphia Information Technology Center
PIV	Personal Identity Verification
PMO	Project Management Office
PO	Privacy Officer

Acronym	Definition
SNOW	ServiceNow
SSH	Secure Shell
UI	User Interface
VA	Department of Veterans Affairs
VAEC	Veterans Affairs Enterprise Cloud
VAMC	Veterans Administration Medical Center
VAS	VistA Audit Solution
VistA	Veterans Health Information Systems Technology Architecture