VistA Audit Solution DG*5.3*1097

Deployment, Installation, Back-out, and Rollback Guide

June 2023

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
05/23/2023	1.0	Initial Draft	Booz Allen Hamilton

The Revision History pertains only to changes in the content of the document or any updates made after distribution. It does not apply to the formatting of the template.

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

List of Tables

1 Introduction

This document describes how to deploy and install the Veterans Health Information Systems and Technology Architecture (VistA) Registration patch DG*5.3*1097, as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort.

The guide includes information about system support, issue tracking, escalation processes, roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, reflecting the particulars of these procedures at a single or at multiple locations.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the VistA Audit Solution (VAS) patch DG*5.3*1097 will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

This patch has a dependency on VistA Registration 5.3 package (DG) patch DG*5.3*964. This released patch must be installed prior to installing DG*5.3*1097.

1.3 Constraints

This patch should be installed in all VA VistA production sites. This patch is intended for a fully patched VistA system.

2 Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	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
2	Local individual Veterans Administration Medical Centers (VAMCs)	Deployment	Determine and document the roles and responsibilities of those involved in the deployment	Planning
3	Field Testing (Initial Operating Capability (IOC)), Health Product Support Testing	Deployment	Test for operational readiness	Testing
4	Health Product Support and Field Operations	Deployment	Execute deployment	Testing
5	VAMCs	Installation	Plan and schedule installation	Deployment
6	VAS ATO Team	Installation	Ensure authority to operate and that certificate authority security documentation is in place	Deployment
7	VAS Team	Installation	Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes	Deployment
8	Health Product Support and the VAS development team.	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
9	VAS Team	Post Deployment	Hardware, Software and System Support	Warranty

3 Deployment

Deployment is planned as a concurrent online rollout. During Initial Operating Capability (IOC) testing and after National release, patch DG*5.3*1097 will be distributed via the FORUM Patch Module and may be deployed at any site without regard to deployment status at other sites.

3.1 Timeline

The deployment and installation are scheduled to run for a period of thirty (30) days. A detailed schedule will be provided during the build. A warranty period of ninety (90) days will follow the deployment and installation schedule to address any potential issues for the build.

3.2 Site Readiness Assessment

This section discusses the locations that will receive the DG*5.3*1097 patch deployment.

The DG*5.3*1097 patch must be manually installed or manually queued for installation at each VistA instance at which it is deployed, using the standard Kernel Installation and Distribution System (KIDS). The patch should be installed at all VA VistA instances running the VistA DG v.5.3 application and will update the Massachusetts General Hospital Utility Multi-Programming System (MUMPS) server software in each VistA instance's Registration namespace.

3.2.1 Deployment Topology (Targeted Architecture)

The DG*5.3*1097 patch should be installed in the VA VistA production environment at all sites.

3.2.2 Site Information (Locations, Deployment Recipients)

During IOC testing, the DG*5.3*1097 patch will be deployed at the following sites:

- Joseph Maxwell Cleland Atlanta VAMC, Decatur, GA
- C.W. Bill Young Dept of VAMC, Bay Pines, FL

Upon National release, the patch will be available for install at all sites running the VistA Registration v5.3 package. The software will be distributed as a PackMan message in FORUM.

3.2.3 Site Preparation

No special preparation is required by the site prior to deployment. The VA sites should follow the standard procedure currently being used for installation of VistA patches.

3.3 Resources

Deployment of the DG*5.3*1097 patch requires a fully patched VistA environment running the Registration v.5.3 package. No additional resources are required for patch installation.

3.3.1 Hardware

There are no special requirements regarding new or existing hardware capability. Existing hardware resources will not be impacted by the changes in this project.

3.3.2 Software

Refer to the following table (Table 2: Software Specifications) which describes the software specifications required at each site prior to deployment.

Table 2: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
Fully patched Registration package within VistA	N/A	5.3	N/A	N/A	N/A
DG*5.3*964	N/A	Nationally released version	N/A	N/A	N/A

See Table 1 for details about who is responsible for preparing the site to meet these software specifications.

3.3.3 Communications

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

3.3.3.1 Deployment / Installation / Back-out Checklist

The assigned Health Care Administration (HCA) team will deploy the patch DG*5.3*1097, which is 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, this information does not need to be manually tracked.

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

DG*5.3*1097, a patch to the existing VistA Registration 5.3 package, is installable on a fully patched MUMPS VistA system and operates on top of the VistA environment provided by the VistA infrastructure packages. The latter provides utilities that communicate with the underlying operating system and hardware, thereby providing Registration independence from variations in hardware and operating system.

4.2 Platform Installation and Preparation

Patch DG*5.3*1097 does not require any platform installation or preparation.

4.3 Download and Extract Files

Patch DG*5.3*1097 will be distributed via a PackMan message and can be retrieved from the NPM on FORUM.

4.4 Database Creation

The patch updates an existing VistA database, this section is not applicable.

4.5 Installation Scripts

The patch does not contain any installation scripts, this section is not applicable.

4.6 Cron Scripts

The patch does not contain any Cron scripts, this section is not applicable.

4.7 Access Requirements and Skills Needed for the Installation

Access to the National VA Network, as well as the local network of each site to receive DG patches, is required to perform the installation, as well as authority to install patches. Knowledge of, and experience with, the KIDS software is required. For more information, see Section V, Kernel Installation and Distribution System, in the Kernel 8.0 & Kernel Toolkit Version 7.3 Systems Management Guide.

4.8 Installation Procedure

This section provides step-by-step instructions for installing DG*5.3*1097. Instructions for installation are also detailed in the DG*5.3*1097 Patch Description in the NPM in FORUM.

4.8.1 Pre-Installation Instructions

This patch may be installed with users on the system although it is recommended that it be installed during non-peak hours to minimize potential disruption to users. The VAS export defaults to 'Don't generate or send data' during installation, minimizing potential user disruption. This patch should take less than 5 minutes to install. If desired, you may queue this installation.

Prior to installing DG*5.3*1097, a backup patch should be created that can be re-installed in the event that a new patch must be backed out (see the "Create a Local Patch Backup" section).

4.8.1.1 Create a Local Patch Backup

Perform the following procedure to create a Local Patch Backup:

1) From the KIDS Menu, select 'Installation'
2) Select 'Backup a Transport Global'
3) At the 'INSTALL NAME:' prompt, enter DG*5.3*1097
4) At the 'Backup Type: B//' prompt, enter B for build
5) At the 'Do you wish to secure this message?' prompt, enter NO
6) At the 'Send mail to:' prompt, enter a recipient who can install the backup build if necessary
7) At the 'And Send to:' prompt(s), optionally enter additional build recipients. Press <Enter> to continue to the next prompt.

4.8.2 VistA Patch DG*5.3*1097 Installation Instructions

1. Choose the PackMan message containing this build.
2. Choose the "INSTALL/CHECK MESSAGE PackMan" option to load the build.
3. From the Kernel Installation and Distribution System Menu, select the "Installation" Menu. From this menu,
    a. Select the "Verify Checksums in Transport Global" option to confirm the integrity of the routines that are in the transport global. When prompted for the INSTALL NAME enter the patch name, DG*5.3*1097.
    b. Select the "Backup a Transport Global" option to create a backup message. You can specify what to backup, the entire Build or just Routines. The backup message can be used to restore just the routines or everything that will restore your system to pre-patch condition. Select "B" for Build (including Routines) at the "Backup Type:" prompt.
    c. You may also elect to use the following options:
        i. Print Transport Global – This option will allow you to view the components of the KIDS build.

ii. Compare Transport Global to Current System – This option will allow you to view all changes that will be made when this patch is installed. It compares all of the components of this patch, such as routines, DDs, templates, etc.

4. Select the Install Package(s) option and choose the patch to install DG*5.3*1097.
5. If prompted 'Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO//', answer YES.
6. When prompted 'Want KIDS to INHIBIT LOGONs during the install? NO//', answer NO.
7. When prompted 'Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO//', answer NO.

4.8.3 Post Installation Instructions

After installation, the connection to the VAS web service should be verified.

4.8.3.1 Verify VAS Server Connectivity

Verify a successful connection to the VAS web service using the Web Server Manager [REDACTED] option.

1. Navigate to the Web Server Manager [REDACTED] option.

2. At the “Select Action:” prompt, enter “CK” for Check Web Service Availability.

3. At the “Select Web Server:” prompt, select the REDACTED from the list.

4. The message “REDACTED is available” should display, indicating the web service is connected and available. If an error message is displayed indicating the service is not available, log a Service Now (SNOW) ticket with a comment requesting the ticket be forwarded to VistA Audit Solution Assignment Group.

Example – Check Web Service Connection

```
Select OPTION NAME: REDACTED       Web Server Manager
Web Server Manager

Web Server Manager            May 06, 2023@09:57:25        Page:    1 of   2
                       REDACTED
                      Version: 1.0     Build: 9

 ID    Web Server Name           IP Address or Domain Name:Port
 1    * REDACTED                REDACTED.####:####
 2    * REDACTED                REDACTED.####:#### (SSL)
 3    * REDACTED                REDACTED.####:#### (SSL)
 4    * REDACTED                REDACTED.####.#### (SSL)

+         Legend:  *Enabled
AS  Add Server                          TS  (Test Server)
ES  Edit Server                         WS  Web Service Manager
DS  Delete Server                       CK  Check Web Service Availability
EP  Expand Entry                        LK  Lookup Key Manager
Select Action:Next Screen// CK   Check Web Service Availability
Select Web Server:  (1-4): 4..
```

```
Web Service Availability      May 06, 2023@09:57:31       Page:   1 of    1
Web Server:
 4    * REDACTED         REDACTED.address:port (SSL)

  1 REDACTED is available

          Enter ?? for more actions                                          >>>

Select Action:Quit//
```

4.9 Installation Verification Procedure

Following patch installation, the installation may be verified by using the "Install File Print" menu option in the "Utilities" submenu of the KIDS menu.

The existence of the VistA Audit Solution (VAS) options [REDACTED] menu in the Security Officer Menu [REDACTED] may also be used to verify successful installation.

4.10 System Configuration

No system configuration is required after deployment of the patch.

4.11 Database Tuning

No Database Tuning is required before or after deployment of the patch.

5 Back-out Procedure

Within context of this document, the term *back-out* pertains to a return to the last known good operational state of the software and appropriate platform settings.

5.1 Back-out Strategy

The back-out strategy will follow VA guidelines and best practices as referenced in the Enterprise Operations (EO) National Data Center Hosting Services document. The Back-Out strategy consists of restoring routine components by installing the backup created prior to patch installation.

5.2 Back-out Considerations

It is necessary to first determine if a wholesale back-out of the patch DG*5.3*1097 is needed or if it would be better to correct by means of applying a new version of the patch (if prior to national release) or employing a subsequent patch aimed at specific areas modified or affected by the original patch (after national release). A wholesale back-out of the patch will require a subsequent patch after national release. If the back-out is post-release of patch DG*5.3*1097, this patch should be assigned the status of "Entered in Error" in the FORUM NPM.

5.2.1 Load Testing

No load testing is required for patch DG*5.3*1097.

5.2.2 User Acceptance Testing

Results from the UAT will be available upon completion.

5.3 Back-out Criteria

Back-out criteria will follow VA guidelines and best practices as referenced in the EO National Data Center Hosting Services document.

Back-out criteria may include the following:

- The project is canceled.
- The requested changes implemented by DG*5.3*1097 are no longer desired by VA OIT.
- The patch produces catastrophic problems.

5.4 Back-out Risks

There are no known risks related to a back-out.

5.5 Authority for Back-out

The Portfolio Director, VA Project Manager, and Business Owner have the authority to require the back-out and accept the risks. Health Care Administration (HCA) will work to identify the problem and assist with implementation. This should be done in consultation with the development team and project stakeholders.

5.6 Back-out Procedure

The back-out plan for VistA applications is complex and not a 'one-size fits all' solution. After national release, the general strategy is to repair the code with a follow-up patch. The VAS development team recommends sites log a ticket with the Enterprise Service Desk (ESD) if it is a nationally released patch.

Prior to national release, backout may be performed by installing the backup of the build performed prior to installation, as well as manually removing the data dictionaries installed by the patch.

Steps – non-Data Dictionary backout:

1) Navigate to the Mailman menu.
2) Select the Mailman folder containing the patch backup created prior to install.
3) Select the message containing the patch backup created prior to install.
4) At the prompt "Enter message action:", enter "X" for Xtract KIDS.
5) At the prompt "Select PackMan function:", enter 6.
6) At the prompt, "OK to continue with Load?" enter "YES".

7) At the prompt, “Want to Continue with Load?”, enter “YES”.
8) Navigate to the Kernel Installation & Distribution System [XPD MAIN] menu.
9) Select the Installation menu.
10) Select the Install Package(s) option.
11) At the prompt “INSTALL NAME:”, enter DG*5.3*1097b.
12) At the prompt “Want KIDS to Rebuild Menu Trees Upon Completion of Install” enter “NO”.
13) At the prompt, “Want KIDS to INHIBIT LOGONs during the install” enter “NO”.
14) At the prompt, “Want to DISABLE Scheduled Options, Menu Options, and Protocols” enter “NO”.
15) At the “DEVICE” prompt, select a device or accept the default, “HOME”.

5.7 Back-out Verification Procedure

After backing out patch DG*5.3*1097 by installing the local patch created during pre-install (see Section 4.8.1), successful back-out is confirmed by verification of BEFORE checksums listed in the patch description on NPM in FORUM. This may be accomplished using the ‘Calculate and Show Checksum Values’ option.

The checksums produced should match the numeric portion of the BEFORE checksums in the DG*5.3*1097 patch description. For the routines that were new with DG*5.3*1097, the BEFORE checksums are ‘n/a’. If routine back-out was successful, the checksum will display as “Routine not in this UCI” in place of a checksum.

6 Rollback Procedure

Rollback pertains to data. This patch does not contain or install any new or modified data dictionaries or file entries.

6.1 Rollback Considerations

No new or modified data dictionaries or file entries are installed by DG*5.3*1097, so there are no rollback considerations.

6.2 Rollback Criteria

N/A.

6.3 Rollback Risks

N/A.

6.4 Authority for Rollback

If rollback were a consideration, the Portfolio Director, VA Project Manager, and Business Owner have the authority to require the rollback and accept the risks. This is not applicable for this patch.

6.5 Rollback Procedure

N/A.

6.6 Rollback Verification Procedure

N/A.

Appendix A: Acronyms

Table 4: Acronym Listing

Acronym	Definition
DIBRG	Deployment, Installation, Back-Out, and Rollback Guide
ESD	Enterprise Service Desk
HCA	Health Care Administration
IOC	Initial Operating Capability
KIDS	Kernel Installation and Distribution System
MUMPS	Massachusetts General Hospital Utility Multi-Programming System
N/A	Not Applicable
NPM	National Patch Module
OIT	Office of Information & Technology
PMO	Project Management Office
SQA	Software Quality Assurance
UAT	User Acceptance Testing
VA	Department of Veterans Affairs
VAMC	Veterans Administration Medical Center
VAS	VistA Audit Solution
VDL	VA Software Document Library
VistA	Veterans Health Information Systems and Technology Architecture