VistA Adaptive Maintenance (VAM) VA Enterprise Cloud (VAEC) Security

Deployment, Installation, Backout, and Rollback Guide (DIBR)



January 2020

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 01/30/2020 | 1.3 | Final document for VAM2-v1.0.0 | AbleVets |
| 11/04/2019 | 1.2 | Updated and delivered to the client | AbleVets |
| 08/02/2019 | 1.1 | Updated and delivered to the client | AbleVets |
| 05/02/2019 | 1.0 | Updated and delivered to the client | AbleVets |
| 01/03/2019 | 0.1 | Initial draft of the document | AbleVets |

Artifact Rationale

This document describes the deployment, installation, backout, and rollback plans for new products going into the VA Enterprise. The guide 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 Integration Process (VIP) Guide, the Deployment, Installation, Backout, and Rollback Guide 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

[1. Introduction 1](#_Toc31294957)

[1.1. Purpose 1](#_Toc31294958)

[1.2. Dependencies 1](#_Toc31294959)

[1.3. Constraints 1](#_Toc31294960)

[2. Roles and Responsibilities 2](#_Toc31294961)

[3. Deployment 2](#_Toc31294962)

[3.1. Timeline 2](#_Toc31294963)

[3.2. Site Readiness Assessment 3](#_Toc31294964)

[3.2.1. Deployment Topography (Targeted Architecture) 3](#_Toc31294965)

[3.2.2. Site Information (Locations, Deployment Recipients) 3](#_Toc31294966)

[3.2.3. Site Preparation 3](#_Toc31294967)

[3.3. Resources 3](#_Toc31294968)

[3.3.1. Facility Specifics 4](#_Toc31294969)

[3.3.2. Hardware 4](#_Toc31294970)

[3.3.3. Software 4](#_Toc31294971)

[3.3.4. Communications 4](#_Toc31294972)

[3.3.4.1. Deployment/Installation/Backout Checklist 5](#_Toc31294973)

[4. Installation 5](#_Toc31294974)

[4.1. Pre-installation and System Requirements 5](#_Toc31294975)

[4.2. Platform Installation and Preparation 5](#_Toc31294976)

[4.3. Download and Extract Files 5](#_Toc31294977)

[4.4. Database Creation 5](#_Toc31294978)

[4.5. Installation Scripts 6](#_Toc31294979)

[4.6. Cron Scripts 6](#_Toc31294980)

[4.7. Access Requirements and Skills Needed for the Installation 6](#_Toc31294981)

[4.8. Installation Procedures 6](#_Toc31294982)

[4.9. Installation Verification Procedures 6](#_Toc31294983)

[4.10. System Configuration 7](#_Toc31294984)

[4.11. Database Tuning 7](#_Toc31294985)

[5. Back-Out Procedure 7](#_Toc31294986)

[5.1. Back-Out Strategy 7](#_Toc31294987)

[5.2. Back-Out Considerations 7](#_Toc31294988)

[5.2.1. Load Testing 8](#_Toc31294989)

[5.2.2. User Acceptance Testing (UAT) 8](#_Toc31294990)

[5.3. Backout Criteria 8](#_Toc31294991)

[5.4. Backout Risks 8](#_Toc31294992)

[5.5. Authority for Backout 8](#_Toc31294993)

[5.6. Backout Procedures 8](#_Toc31294994)

[5.7. Backout Verification Procedures 8](#_Toc31294995)

[6. Rollback Procedures 9](#_Toc31294996)

[6.1. Rollback Considerations 9](#_Toc31294997)

[6.2. Rollback Criteria 9](#_Toc31294998)

[6.3. Rollback Risks 9](#_Toc31294999)

[6.4. Authority for Rollback 9](#_Toc31295000)

[6.5. Rollback Procedures 9](#_Toc31295001)

[6.6. Rollback Verification Procedures 9](#_Toc31295002)

[A. Appendix A: Acronyms and Abbreviations 10](#_Toc31295003)

Table of Tables

[Table 1: Roles and Responsibilities 2](#_Toc31295004)

[Table 2: Key Communication 4](#_Toc31295005)

[Table 3: Deployment/Installation/Backout Checklist 5](#_Toc31295006)

[Table 4: CloudFormation Stack Variables 7](#_Toc31295007)

[Table 5: Acronyms and Abbreviations 10](#_Toc31295008)

# Introduction

The Veterans Health Information Systems and Technology Architecture (VistA) Adaptive Maintenance (VAM) System is a cloud-native Platform as a Service (PaaS), deployed entirely and exclusively within the Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act of 1996 (HIPAA)-compliant VA Enterprise Cloud (VAEC), leveraging the Amazon Web Services (AWS) commercial cloud infrastructure and services.

VAM provides comprehensive, commercial cloud-based monitoring and security for all clients, applications, and users of the VistA Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for Enterprise Production use for all VistA systems migrated to the VAEC, leveraging FedRAMP High, VAEC-approved AWS Kinesis and AWS CloudWatch Logs.

VAM is a passive monitoring PaaS that mirrors VistA RPC traffic via AWS Kinesis to the AWS CloudWatch Logs, which is then interpreted by the RPC Monitor. AWS CloudWatch Logs are FedRAMP High certified and store all data in an encrypted form.

VAM is a 100% cloud-native, legacy-free, and non-invasive PaaS. VAM requires no change to any VistA system, nor to any end user client or application, allowing VAM to be safely and reliably deployed and scaled Enterprise-wide with minimal to no risk. Should VAM (RPC Mirror or Monitor) be disabled or deactivated, all RPC traffic flows between VistA and all its clients as usual, only without monitoring.

All of VAM’s functionality is contained exclusively and entirely as a PaaS within the VAEC, thus inheriting all security and compliance controls of the Federal Information Security Management Act of 2002 (FISMA) High VAEC. VAM has neither a connection with, nor does it share any information with, any organization, application, or system outside of the VAEC.

## Purpose

The purpose of the DIBR is to provide a single, common document that describes how, when, where, and to whom the VAM product will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The DIBR identifies resources, a communication plan, and a rollout schedule, and is a companion to the Project Charter and Management Plan, and the User Guide for this effort.

## Dependencies

VAM has neither dependencies on VistA updates nor external dependencies.

## Constraints

Changes to VAM introduced by this release do not affect the current Section 508 compliance. The Veterans Health Administration (VHA) recognizes that these cross-cutting legal requirements apply across the Enterprise for all developed electronic and Information Technology (IT). Enterprise-level requirements maintained by VHA Health IT, Software Engineering and Integration, and Enterprise Requirements Management ensure the compliance of these requirements.

# Roles and Responsibilities

Deployment and installation activities are performed by representatives from the teams listed in Table 1. This phase begins after the solution design.

Table : Roles and Responsibilities

| Team | Phase/Role | Tasks |
| --- | --- | --- |
| VAM Project Manager (PM) | Deployment | Plan and schedule deployment (including orchestration with vendors) |
| Test Sites | Production Testing | Test for operational readiness and provide concurrence |
| VIP Release Readiness Team | Deployment | Ensure collection of artifacts required for deployment |
| VAM Implementation Manager (IM) | Deployment | Confirm project is ready for national release |
| Facility Office of Information and Technology (OIT) Staff | Installation | Facilities will install the associated patches that pair with VAM. |
| Enterprise Services Engineering (ESE) and Desktop Device Engineering Client Services Group | Installation | Prepare the System Center Configuration Manager (SCCM) package for VAM installation |
| Office of Veterans Access to Care (OVAC) | Installation | Coordinate training |

# Deployment

This DIBR describes the associated patches necessary for a successful deployment. The deployment package is comprised of the VAM update.

The deployment of this release will be supported by a compliance period.

The VAM schedule and milestones for the deployment can be found on the project’s [GitHub workspace](https://github.com/vistadataproject/VAM2ProjectManagement).

## Timeline

The deployment and installation are scheduled to run for approximately four (4) weeks, as detailed in the project schedule. The updated GUI and associated patches will be installed in the Pre-Production environment first. Once the site has successfully installed and deployed the software in the Pre-Production environment and on end user desktops, the sites will install the software in their Production environments. The current plan calls for sites to request the deployment of the new GUI and patches, requiring coordination with the regional Enterprise Service Line (ESL) and the SCCM deployment teams. All locations should have the VAM associated patches installed in their Production environments prior to deployment.

## Site Readiness Assessment

The VAM system is deployed to the VistA production account in the VAEC, intended to monitor the network traffic of a production VAEC VistA. This is a novel project with an original deployment with no predecessors. The VAM system is a pure back-end system, deployed wholly in the VAEC environment, and therefore, does not include user interface or devices.

### Deployment Topography (Targeted Architecture)

Figure 1: Deployment Topology (Targeted Architecture)

A screenshot of a cell phone

Description automatically generated

### Site Information (Locations, Deployment Recipients)

Site information such as the Internet Protocol (IP) address, port number, and namespace of the Production environment is different at each VistA instance. Local site OIT personnel, working with local scheduling representatives, will determine the recipients of VAM. A list of the local sites can be found in the Appendix.

### Site Preparation

No additional preparation needs to occur at the production deployment site. The VAM system is intended to passively monitor traffic, with no impact to the existing, monitored VistA system.

## Resources

There will be a daily call set up for sites that are having install/deployment issues. If a site experiences issues, a ServiceNow ticket must be submitted for tracking and remediation purposes. The vendor will provide troubleshooting support during the daily Initial Operating Capacity (IOC) call.

### Facility Specifics

The following conditions will be assumed for VAM Release 1.0.0:

* All facilities deploying VAM will have a fully patched VistA account.
* VAM release patches will be installed by the compliance date.
* ESE will provide the SCCM package needed for the VAM release.
* OVAC will provide a training plan prior to deployment.

### Hardware

No hardware changes are necessary for VAM to function properly at each site.

### Software

Software specifications required at each site prior to deployment will be provided when available. The party(ies) responsible for preparing the site to meet the software specifications will be provided when available.

### Communications

The primary objective of the communication plan is to ensure the timely dissemination of information to stakeholders. Clear communication is necessary to ensure that schedules are aligned, and project milestones are met.

Project milestones and information will be shared with VA executives and external organizations, to notify the right audience, at the right time, using the appropriate communication method(s).

Table 2 identifies key project communication along with the owner, recipients, and the method(s) used to disseminate information.

Table : Key Communication

| Subject | Goal/Description | Initiator/Owner | Audience | Communication Method |
| --- | --- | --- | --- | --- |
| Installation instruction and support | Site requirements, instructions, and installation support (hardware, software, patches) | Team AbleVets, VHA Developers | IT, Operation Site Managers | VA Pulse, daily deployment call, IOC e-mail group |
| Deployment Schedule | Key dates and milestones, per site | OVAC | Project Team, stakeholders | Online schedule, daily deployment call |
| Training | Training development status, training dates, and trainees | OVAC | Project Team, stakeholders | VA Pulse, daily deployment call, deployment schedule |

#### Deployment/Installation/Backout Checklist

The table below outlines the coordination effort and documents for the day/time/individual when each activity is completed for VAM:

Table : Deployment/Installation/Backout Checklist

| Activity | Date | Time | Completed By |
| --- | --- | --- | --- |
| Deploy | 12/08/2019 | 9:00am HST | Cognosante DevOps |
| Back-Out | TBD | TBD | Facility OIT Staff |

# Installation

The following subsections detail the installation process and procedures for installing the VAM system resources via CloudFormation template.

## Pre-installation and System Requirements

Follow the steps below:

1. Collect the following information from the target VISTA system:

* VPC ID of the target VISTA front-end.
* Subnet of the target VISTA front-end.
* Elastic Network Interface (ENI) of the VISTA instance target (see the [Notes](https://github.com/vistadataproject/TrafficMirrorMonitor/wiki/Traffic-Mirror---AWS-Deployment-Procedure#notes) section first for prerequisites and constraints).

1. Create an IAM EC2 service role in the VISTA account with the following permissions:
   * EC2 instance create full access.
   * VPC Traffic Mirror resource full access.
   * S3 resource create/write full access.
2. The **Instance Profile ARN** of the created role, this is the value to use when filling out the CloudFormation parameters.

## Platform Installation and Preparation

This section is not applicable.

## Download and Extract Files

Download the latest CloudFormation JSON template file trafficMirrorMonitor\_CFTemplate.json from GitHub. The file can be downloaded using the following URL: <https://github.com/vistadataproject/VAM2ProjectManagement/Software/TrafficMirrorMonitor/scripts/trafficMirrorMonitor_CFTemplate.json>

## Database Creation

This section is not applicable.

## Installation Scripts

This section is not applicable. Installation and deployment are performed via CloudFormation template via the AWS Management Console.

## Cron Scripts

This section is not applicable.

## Access Requirements and Skills Needed for the Installation

The deployment must be performed by an administrative user within the VistA production VAEC account.

## Installation Procedures

First, you'll need to install the appropriate basic tools to support the retrieval and runtime the software:

> sudo yum -y install curl

> curl -sL https://rpm.nodesource.com/setup\_10.x | sudo -E bash -

> sudo yum -y install nodejs git

The software depends on an open-source NodeJS PCAP library, which compiles a native library. To get the appropriate tools installed on an Amazon Linux EC2 instance, this will typically entail installing additional development tools as follows:

> sudo yum-config-manager --enable rhel-6-server-optional-rpms

> sudo yum -y install libpcap-devel

> sudo yum-config-manager --disable rhel-6-server-optional-rpms

> sudo yum install -y make glibc-devel gcc patch gcc-c++

Once you've done that, clone this repo and install the software:

> git clone https://github.com/vistadataproject/TrafficMirrorMonitor

> cd TrafficMirrorMonitor

> npm install

> npm run build

You'll also need to have a valid S3 bucket that the **Traffic Mirror Monitor** can write to.

## Installation Verification Procedures

To verify the installation, follow the steps below:

1. Open an SSH session into each created EC2 instance, then issue the following command in the console:

pm2 status

1. Verify that the traffic-mirror process shows up as running in the status window
2. Verify that data is being properly written to the system S3 bucket by issuing the following command in the SSH session console:

aws s3 ls s3://traffic-mirror-<<VAM System Name>>-<<Environment Type>>

1. “VAM System Name” and “Environment Type” are the values set in section 4.8 Installation Procedures.
2. Verify that S3 objects are listed as a result of the command.

## System Configuration

The **Traffic Mirror Monitor** is configurable via variables set when deploying the CloudFormation stack:

Table : CloudFormation Stack Variables

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| System Name | String | Identifier of the VistA system to use for the CloudFormation stack. |
| Environment | String | Type of deployment environment |
| VPC ID | String | Virtual Private Cloud (VPC) ID of the target VISTA instance |
| Subnet ID | String | Subnet ID of the front-end VistA instance |
| ENI ID #1 | String | Elastic Network Interface ID #1 |
| ENI ID #2 | String | Elastic Network Interface ID #2 |
| SSH Key Name | String | Name of the SSH key to associate with user access to the EC2 instances created by the stack |
| Instance Profile ID | String | Instance profile ARN to use for the EC2 role applied to the Auto-scaling launch config. |

## Database Tuning

This section is not applicable.

# Back-Out Procedure

## Back-Out Strategy

The backout strategy is to uninstall the newly deployed VAM system components and restore the previously deployed version.

## Back-Out Considerations

The consideration for performing a back-out is that VAM does not operate as intended when tested.

Because the VAM system is totally passive, system back-out can be performed by deleting the existing CloudFormation stack, using the methods built in via AWS CloudFormation. This will have no impact on production VistA systems.

### Load Testing

Prior to production deployment, load testing was performed against a pre-production deployment that mirrored the production VistA architecture.

A test harness was uses to create the following connection profile to exercise the VAM traffic mirroring system:

* 500 concurrent TCP connections to VistA.
* Connections made at a rate of one (1) connection per second up to 500 connections.
* Each connection maintained an average data rate of 250 payload bits/second.
* The overall test lasted for 30 minutes.

During the course of the load test, the VAM system reported no errors and both CPU and memory usage by the Traffic Mirror software remained under 75% maximum.

### User Acceptance Testing (UAT)

This section is not applicable. VAM does not provide a user interface.

## Backout Criteria

The criterion for backing out of the new installation is that VAM does not operate as intended during installation verification testing.

## Backout Risks

A backout is performed to remove the installed components if the VAM deployment did not pass the installation verification procedures. The backout procedures are followed by a rollback to restore the previously deployed version of VAM. The risks for executing the backout are minimal because a backout is performed during planned downtime when users are not accessing the system. Once the restored system is online and validated, user access continues.

If a backout is initiated later in the deployment window, restoration time may exceed the downtime planned for deployment. This risk is mitigated by scheduling deployments for weekends and other times when expected usage levels are low.

## Authority for Backout

If a backout is necessary, the VA PM provides the approval to back the product out of Production.

## Backout Procedures

The following AWS URL describes the procedures to delete a CloudFormation stack: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-delete-stack.html>

## Backout Verification Procedures

Verify in the AWS CloudFormation console that the VAM CloudFormation stack was successfully deleted

# Rollback Procedures

## Rollback Considerations

The consideration for performing a rollback is that VAM does not operate as intended when tested following an update to the system.

Because the VAM system is totally passive, system roll-back can be performed by rolling back the existing CloudFormation stack, using the methods built in via AWS CloudFormation. This will have no impact on production VistA systems.

## Rollback Criteria

The criterion for a rollback is that VAM does not operate as intended during installation verification testing.

## Rollback Risks

A rollback is performed to remove the installed components if the VAM deployment did not pass the installation verification procedures. The rollback procedures restore the previously deployed version of VAM. The risks for executing the rollback are minimal because a rollback is performed during planned downtime when users are not accessing the system. Once the restored system is online and validated, user access continues.

If a rollback is initiated later in the deployment window, restoration time may exceed the downtime planned for deployment. This risk is mitigated by scheduling deployments for weekends and other times when expected usage levels are low.

## Authority for Rollback

If a rollback is necessary, the VA PM provides the approval.

## Rollback Procedures

The following AWS URL describes the procedures to rollback a CloudFormation stack: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-rollback-triggers.html>

## Rollback Verification Procedures

Verify in the AWS CloudFormation console that the VAM CloudFormation stack was successfully rolled back to the previous version.

1. Appendix A: Acronyms and Abbreviations

The table below lists the acronyms and abbreviations used throughout this document.

Table : Acronyms and Abbreviations

|  |  |
| --- | --- |
| Acronym | Definition |
| ARN | AWS Resource Name |
| AWS | Amazon Web Services |
| CPU | Central Processing Unit |
| DIBR | Deployment, Installation, Backout, and Rollback |
| EC2 | Elastic Cloud Compute |
| ENI | Elastic Network Interface |
| ESE | Enterprise Services Engineering |
| ESL | Enterprise Service Line |
| FedRAMP | Federal Risk and Authorization Management Program |
| FISMA | Federal Information Security Management Act of 2002 |
| GUI | Graphical User Interface |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| IM | Implementation Manager |
| IAM | Identity and Access Management |
| IOC | Initial Operating Capacity |
| IT | Information Technology |
| OIT | Office of Information and Technology |
| OVAC | Office of Veterans Access to Care |
| PaaS | Platform as a Service |
| PM | Project Manager, Program Manager |
| RPC | Remote Procedure Call |
| S3 | Simple Storage Service |
| SCCM | System Center Configuration Manager |
| SSH | Secure Shell |
| TCP | Transmission Control Protocol |
| URL | Uniform Resource Locator |
| VA | Department of Veterans Affairs |
| VAEC | VA Enterprise Cloud |
| VAM | VistA Adaptive Maintenance |
| VHA | Veterans Health Administration |
| VIP | Veteran-focused Integration Process |
| VistA | Veterans Health Information Systems and Technology Architecture |