**VistA Adaptive Maintenance VAEC Security**

**(VAM)**

Production Operations Manual (POM)



Department of Veterans Affairs

Office of Information & Technology

Contract No: VA118-16-D-1009

task Order: 36C10B19F10090015

Deliverable: CLIN0005AA

Date: 05-02-2019

Version 1.0

Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 05-02-2019 | 1.0 | Draft | AbleVets |

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 1](#_Toc7434267)

[2. Routine Operations 1](#_Toc7434268)

[2.1. Administrative Procedures 1](#_Toc7434269)

[2.1.1. System Start-up 1](#_Toc7434270)

[2.1.1.1. System Start-Up from Emergency Shut-Down 1](#_Toc7434271)

[2.1.2. System Shut-down 2](#_Toc7434272)

[2.1.2.1. Emergency System Shut-down 2](#_Toc7434273)

[2.1.3. Back-up & Restore 2](#_Toc7434274)

[2.1.3.1. Back-Up Procedures 2](#_Toc7434275)

[2.1.3.2. Restore Procedures 2](#_Toc7434276)

[2.1.3.3. Back-Up Testing 2](#_Toc7434277)

[2.1.3.4. Storage and Rotation 2](#_Toc7434278)

[2.2. Security / Identity Management 2](#_Toc7434279)

[2.2.1. Identity Management 2](#_Toc7434280)

[2.2.2. Access control 3](#_Toc7434281)

[2.3. User Notifications 3](#_Toc7434282)

[2.3.1. User Notification Points of Contact 3](#_Toc7434283)

[2.4. System Monitoring, Reporting & Tools 3](#_Toc7434284)

[2.4.1. Dataflow Diagram 5](#_Toc7434285)

[Figure 1: VAM Architecture diagram with Security Boundaries and Data Flow Diagram 6](#_Toc7434286)

[Table 1: Data Flow 6](#_Toc7434287)

[2.4.2. Availability Monitoring 6](#_Toc7434288)

[2.4.3. Performance/Capacity Monitoring 6](#_Toc7434289)

[2.4.4. Critical Metrics 7](#_Toc7434290)

[2.5. Routine Updates, Extracts and Purges 7](#_Toc7434291)

[2.6. Scheduled Maintenance 7](#_Toc7434292)

[2.7. Capacity Planning 7](#_Toc7434293)

[2.7.1. Initial Capacity Plan 7](#_Toc7434294)

[3. Exception Handling 7](#_Toc7434295)

[3.1. Routine Errors 7](#_Toc7434296)

[3.1.1. Security Errors 8](#_Toc7434297)

[3.1.2. Time-outs 8](#_Toc7434298)

[3.1.3. Concurrency 8](#_Toc7434299)

[3.2. Significant Errors 8](#_Toc7434300)

[3.2.1. Application Error Logs 8](#_Toc7434301)

[3.2.2. Application Error Codes and Descriptions 8](#_Toc7434302)

[3.2.3. Infrastructure Errors 8](#_Toc7434303)

[3.2.3.1. Database 8](#_Toc7434304)

[3.2.3.2. Web Server 8](#_Toc7434305)

[3.2.3.3. Application Server 9](#_Toc7434306)

[3.2.3.4. Network 9](#_Toc7434307)

[3.2.3.5. Authentication & Authorization 9](#_Toc7434308)

[3.2.3.6. Logical and Physical Descriptions 9](#_Toc7434309)

[3.3. Dependent System(s) 9](#_Toc7434310)

[3.4. Troubleshooting 9](#_Toc7434311)

[3.5. System Recovery 9](#_Toc7434312)

[3.5.1. Restart after Non-Scheduled System Interruption 9](#_Toc7434313)

[3.5.2. Restart after Database Restore 9](#_Toc7434314)

[3.5.3. Back-out Procedures 9](#_Toc7434315)

[3.5.4. Rollback Procedures 10](#_Toc7434316)

[4. Operations and Maintenance Responsibilities 10](#_Toc7434317)

[5. RACI Matrix Template 10](#_Toc7434318)

[6. Approval Signatures 11](#_Toc7434319)

# Introduction

This document describes how to maintain the components of the VistA Adaptive Maintenance VAEC Security (VAM), as well as how to troubleshoot problems that might occur with this product in production. The intended audience for this document is the Information Technology (IT) teams responsible for hosting and maintaining the system after production release. This document is normally finalized just prior to production release and includes many updated elements specific to the hosting environment.

VAM resides in VAEC Amazon Infrastructure and is monitored using Amazon CloudWatch. Amazon CloudWatch is the component of Amazon Web Services that provides real-time monitoring of AWS resources and customer applications running on Amazon infrastructure.

This manual provides Department of Veterans Affairs (VA) site managers with a technical description of the Veterans Health Information System and Technology Architecture (VistA) Adaptive Maintenance VAEC Security (VAM) Graphical User Interface () routines, files, menus, cross references, globals, and other necessary information required to effectively manage the system.

# 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.

## Administrative Procedures

First build is not going to get installed in VAEC so this section is not completed.

### System Start-up

#### System Start-Up from Emergency Shut-Down

### System Shut-down

#### Emergency System Shut-down

### Back-up & Restore

#### Back-Up Procedures

#### Restore Procedures

#### Back-Up Testing

#### Storage and Rotation

## Security / Identity Management

Access to the VAM is restricted to authorized users within the VAEC.

Access control and authentication takes place before VAM displays any data.

### Identity Management

Users with a valid VistA access can access VAM.

### Access control

## User Notifications

The VAM has no notification system and does not use a secondary database and should always be available when VistA is available. Any notification regarding system availability will be identical to VistA availability.

### User Notification Points of Contact

## System Monitoring, Reporting & Tools

The following automated monitoring tools are used to watch VAM in the VAEC Amazon Infrastructure :

* **System Status Checks** - monitor the VAEC AWS systems required to use VAM instance to ensure they are working properly. These checks detect problems with VAM instance that require VAEC AWS involvement to repair. When a system status check fails, you can choose to wait for AWS to fix the issue or you can resolve it yourself (for example, by stopping and restarting or terminating and replacing an instance). Examples of problems that cause system status checks to fail include:
  + Loss of network connectivity
  + Loss of system power
  + Software issues on the physical host
  + Hardware issues on the physical host that impact network reachability

For more information, see [Status Checks for Your Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html).

* **Instance Status Checks** - monitor the software and network configuration of VAM individual instance. These checks detect problems that require your involvement to repair. When an instance status check fails, typically you will need to address the problem yourself (for example, by rebooting the instance or by making modifications in your operating system). Examples of problems that may cause instance status checks to fail include:
  + Failed system status checks
  + Misconfigured networking or startup configuration
  + Exhausted memory
  + Corrupted file system
  + Incompatible kernel

For more information, see [Status Checks for Your Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html).

* **Amazon CloudWatch Alarms** - watch a single metric over a time period you specify, and perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon Simple Notification Service (Amazon SNS) topic or Amazon EC2 Auto Scaling policy. Alarms invoke actions for sustained state changes only. CloudWatch alarms will not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see [Monitoring Your Instances Using CloudWatch](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html).
* **Amazon CloudWatch Events** - automate VAEC AWS services for VAM and respond automatically to system events. Events from AWS services are delivered to CloudWatch Events in near real time, and you can specify automated actions to take when an event matches a rule you write. For more information, see [What is Amazon CloudWatch Events?](https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html).
* **Amazon CloudWatch Logs** - monitor, store, and access your log files from Amazon EC2 instances, AWS CloudTrail, or other sources. For more information, see the [Amazon CloudWatch Logs User Guide](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/).
* **Amazon EC2 Monitoring Scripts** - Perl scripts that can monitor memory, disk, and swap file usage in your instances. For more information, see [Monitoring Memory and Disk Metrics for Amazon EC2 Linux Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html).

### Dataflow Diagram

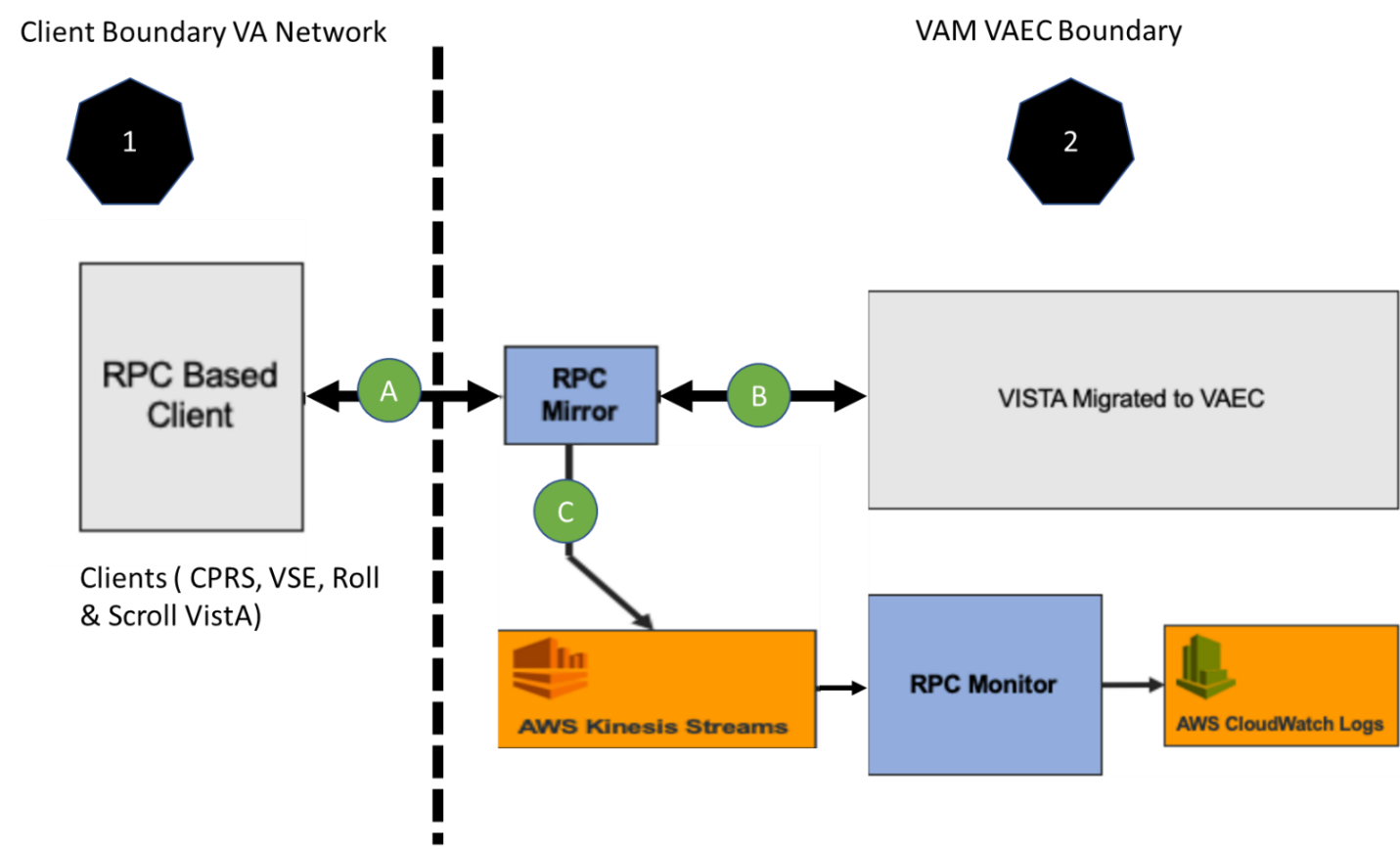
VAM is comprised of 3 major architectural components:

1. **RPC Monitor** – The RPC Monitor segment represents the software pipeline that facilitates RPC parsing, classification and alert notification functions of the VAM application.
2. **RPC Mirror** – The RPC Mirror segment represents the small piece of software that mirrors client-to-VISTA RPC traffic to an alternate, data streaming service (Kinesis). This software needs to make as small an impact as possible, since it does sit on the critical network traffic path between VISTA clients and VISTA.
3. **RPC Definition Models** – The RPC Definition Models segment represents the static RPC definition model files generated by the RPC Definition Toolkit, as well as the Classifier pipeline, resident in the RPC Monitor, that applies said models against RPC traffic to generate classifications and alerts.

Note, all the above VAM components will be managed within a single security boundary, within VAEC. For illustrative purposes, Figure 1 (next page) depicts a typical usage scenario for VAM and the associated security boundaries. This Figure also represents the planned configuration for the IOC deployment. The two system and security boundaries are:

1. **Client Boundary VA Network:** The client application, for example CPRS/VSE in the case of the IOC, will be installed on a machine within end-user’s segment of the VA network. It will directly connect to the VAM Boundary through the VAECs Business Partner Extranet (BPE) ExpressRoute connection.
2. **VAM VAEC Boundary:** VAM and its associated components are all contained within a single security boundary within the VAEC using the AWS VA GSS. AWS VA General Support System (GSS) that is already documented within Risk Vision. All Security controls that are already documented in Risk Vision for AWA GSS cloud will be inherit within our System Security Plan (SSP). VAM will connect directly to the Client Boundary and the VistA which are migrated in VAEC AWS.

#### Figure 1: VAM Architecture diagram with Security Boundaries and Data Flow Diagram



#### Table 1: Data Flow

|  |  |  |
| --- | --- | --- |
| **ID** | **Data Flow Link** | **Description** |
| A | Client to and from RPC Mirror | Data flows between Client and RPC Mirror bi-directionally. This link carries RPC Calls, Meta Data and de-identified PII/PHI data. This is the only link which will cross between VA Network to VAEC AWS Boundary. |
| B | RPC Mirror to and from VistA | Data flows between RPC Mirror and VistA bi-directionally. This link directs all traffic from RPC Mirror to VistA and responses from VistA back to RPC Mirror. |
| C | RPC Mirror to VAM Application | Data flows from RPC Mirror to VAM Application unidirectionally. This data parsed using VAM (AWS Kinesis Streams, RPC Monitor and AWS CloudWatch Logs) to provide audit results in CloudWatch. |

### Availability Monitoring

The VAM application has no availability separate from the VistA system.

### Performance/Capacity Monitoring

### Critical Metrics

## Routine Updates, Extracts and Purges

## Scheduled Maintenance

## Capacity Planning

### Initial Capacity Plan

# Exception Handling

First build is not going to get installed in VAEC so this section is not completed.

## Routine Errors

### Security Errors

### Time-outs

### Concurrency

## Significant Errors

### Application Error Logs

### Application Error Codes and Descriptions

### Infrastructure Errors

#### Database

#### Web Server

#### Application Server

#### Network

#### Authentication & Authorization

The VAM uses the exact same authentication RPC’s that the CPRS uses. Its authentication related errors will be identical and limited to incorrect login and number of tries exceeded errors.

#### Logical and Physical Descriptions

## Dependent System(s)

First build is not going to get installed in VAEC so this section is not completed.

## Troubleshooting

First build is not going to get installed in VAEC so this section is not completed.

## System Recovery

First build is not going to get installed in VAEC so this section is not completed.

### Restart after Non-Scheduled System Interruption

### Restart after Database Restore

### Back-out Procedures

### Rollback Procedures

# 4. Operations and Maintenance Responsibilities

**There is NO Operation Maintenance in the SCOPE of VAM.**

# RACI Matrix Template

**N/A**

# Approval Signatures

Indicate the approval of the Production Operations Manual and accompanying RACI, below.

REVIEW DATE: <date>

SCRIBE: <name>

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Portfolio Director Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Product Owner Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Receiving Organization Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Operations Support Date

Template Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| May 2019 | 1.0 | Initial Document | AbleVets |