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

Production Operations Manual



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 | Submitted to the client | AbleVets |
| 08/02/2019 | 1.1 | Submitted to the client | AbleVets |
| 05/02/2019 | 1.0 | Submitted to the client | AbleVets |
| 02/01/2019 | 0.1 | Initial draft of the document | 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](#_Toc31284501)

[2. Routine Operations 1](#_Toc31284502)

[2.1. Administrative Procedures 2](#_Toc31284503)

[2.1.1. System Startup 2](#_Toc31284504)

[2.1.1.1. System Startup from Emergency Shutdown 2](#_Toc31284505)

[2.1.2. System Shutdown 2](#_Toc31284506)

[2.1.2.1. Emergency System Shutdown 2](#_Toc31284507)

[2.1.3. Backup and Restore 2](#_Toc31284508)

[2.1.3.1. Backup Procedures 2](#_Toc31284509)

[2.1.3.2. Restore Procedures 2](#_Toc31284510)

[2.1.3.3. Backup Testing 2](#_Toc31284511)

[2.1.3.4. Storage and Rotation 3](#_Toc31284512)

[2.2. Security/Identity Management 3](#_Toc31284513)

[2.2.1. Identity Management 3](#_Toc31284514)

[2.2.2. Access control 3](#_Toc31284515)

[2.3. User Notifications 3](#_Toc31284516)

[2.3.1. User Notification Points of Contact 3](#_Toc31284517)

[2.4. System Monitoring, Reporting and Tools 3](#_Toc31284518)

[2.4.1. Dataflow Diagram 4](#_Toc31284519)

[2.4.2. Availability Monitoring 5](#_Toc31284520)

[2.4.3. Performance/Capacity Monitoring 5](#_Toc31284521)

[2.4.4. Critical Metrics 5](#_Toc31284522)

[2.5. Routine Updates, Extracts and Purges 5](#_Toc31284523)

[2.6. Scheduled Maintenance 5](#_Toc31284524)

[2.7. Capacity Planning 5](#_Toc31284525)

[2.7.1. Initial Capacity Plan 5](#_Toc31284526)

[3. Exception Handling 6](#_Toc31284527)

[3.1. Routine Errors 6](#_Toc31284528)

[3.1.1. Security Errors 6](#_Toc31284529)

[3.1.2. Timeouts 6](#_Toc31284530)

[3.1.3. Concurrency 6](#_Toc31284531)

[3.2. Significant Errors 6](#_Toc31284532)

[3.2.1. Application Error Logs 6](#_Toc31284533)

[3.2.2. Application Error Codes and Descriptions 6](#_Toc31284534)

[3.2.3. Infrastructure Errors 6](#_Toc31284535)

[3.2.3.1. Database 6](#_Toc31284536)

[3.2.3.2. Web Server 7](#_Toc31284537)

[3.2.3.3. Application Server 7](#_Toc31284538)

[3.2.3.4. Network 7](#_Toc31284539)

[3.2.3.5. Authentication and Authorization 7](#_Toc31284540)

[3.2.3.6. Logical and Physical Descriptions 7](#_Toc31284541)

[3.3. Dependent System(s) 7](#_Toc31284542)

[3.4. Troubleshooting 7](#_Toc31284543)

[3.5. System Recovery 7](#_Toc31284544)

[3.5.1. Restart after Non-Scheduled System Interruption 7](#_Toc31284545)

[3.5.2. Restart after Database Restore 7](#_Toc31284546)

[3.5.3. Backout Procedures 7](#_Toc31284547)

[3.5.4. Rollback Procedures 8](#_Toc31284548)

[4. Operations and Maintenance Responsibilities 8](#_Toc31284549)

[5. RACI Matrix 8](#_Toc31284550)

[6. Approval Signatures 9](#_Toc31284551)

[A. Appendix: Acronyms and Abbreviations 1](#_Toc31284552)

# 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.

The primary objective of Project VAM is to assist VA in strengthening its cybersecurity profile by enhancing the protection of Veteran data. The successful execution and completion of the project resolves the following aims:

* Reduce the cost and complexity of VistA systems maintenance.
* Resolve severe security vulnerabilities within all VistA systems.
* Full utilization of the features, security, and scaling of VA’s commercial cloud capabilities.
* Ensure the safe, secure, and seamless continuity of Veteran care and services as VistA systems are migrated to the VAEC.

# 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

### System Startup

VAM leverages AWS CloudFormation for start-up. The VAM CloudFormation stack includes an Auto Scaling Group, which is responsible spinning up EC2 instances that are configured to run the Traffic Mirroring software.

To start the VAM system, create the VAM CloudFormation stack via the AWS Management Console. A detailed procedure can be found via the following URL: <https://github.com/vistadataproject/VAM2ProjectManagement/wiki/Traffic-Mirror---AWS-Deployment-Procedure>.

Information on CloudFormation stack creation can also be found via the following Amazon AWS URL:<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html>.

#### System Startup from Emergency Shutdown

The process to recover and startup from emergency shutdown is the same as a normal system startup.

### System Shutdown

To shut down the VAM system, delete the VAM CloudFormation stack. Information on CloudFormation stack deletion can be found at this Amazon AWS URL: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-delete-stack.html>.

#### Emergency System Shutdown

The process to shut the system down in an emergency is the same as a normal system shutdown.

### Backup and Restore

The VAM system relies on AWS resource management and backup facilities. No additional configuration or services are required.

#### Backup Procedures

The VAM system relies on AWS resource management and backup facilities. No additional configuration or services are required.

#### Restore Procedures

The VAM system relies on AWS resource management and backup facilities. No additional configuration or services are required.

#### Backup Testing

The VAM system relies on AWS resource management and backup facilities. No additional configuration or services are required.

#### Storage and Rotation

The VAM system relies on AWS S3 storage and backup facilities. No additional configuration or services are required.

## Security/Identity Management

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

### Identity Management

Users with valid VistA Access and Verify codes can access VAM.

### Access control

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

## User Notifications

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

### User Notification Points of Contact

VAM has not yet been released to Production. The administrative procedures are in discussion and development.

## System Monitoring, Reporting and Tools

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

* **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
* **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 (SNS) topic or Amazon Elastic Compute Cloud (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 three (3) major architectural components.

The RPC Monitor segment represents the software pipeline that facilitates RPC parsing, classification and alert notification functions of the VAM application.

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.

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.

1. *All the VAM components will be managed within a single security boundary in VAEC.*

The two system and security boundaries are:

**Client Boundary VA Network:** The client application, for example CPRS/VSE in the case of the Initial Operating Capabilities (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.

**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.

Please see the *System Boundary Document* and the *VAM VAEC Security System Design Document* for detailed information.

### Availability Monitoring

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

### Performance/Capacity Monitoring

VAM Traffic Mirroring software is managed on each EC2 instance by PM2, which monitors software resource usage.

All other performance and resource usage metrics are made available by AWS.

### Critical Metrics

VAM Traffic Mirror Monitor:

* CPU Usage: Under 75% total usage for any sampled period.
* RAM Usage: Under 75% provisioned heap size (4GB) for any sampled period.

## Routine Updates, Extracts and Purges

VAM stores mirrored traffic data to an S3 bucket configured to purge data older than five days. This process is wholly managed by AWS.

## Scheduled Maintenance

No scheduled maintenance is required for the VAM system

## Capacity Planning

The VAM capacity planning, performance and scalability assessment can be found via the following URL: <https://github.com/vistadataproject/VAM2ProjectManagement/wiki/Capacity,-Performance-and-Scalability-Assessment-for-National-Deployment>.

### Initial Capacity Plan

See the document referred to in section **Error! Reference source not found.**.

# Exception Handling

## Routine Errors

VAM provides no user access, therefore, no routine errors are generated.

### Security Errors

VAM provides no user access, therefore, no security errors are generated.

### Timeouts

VAM provides no user access, therefore, no timeout errors are generated.

### Concurrency

VAM provides no user access, therefore, no concurrency errors are generated.

## 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 the resolution of significant errors, conditions, or other issues.

### Application Error Logs

The VAM Traffic Mirror software is managed by PM2, which is configured to maintain console log output via a rolling log file scheme. The log rotation scheme uses the following configuration options:

* Max file size: 10MB
* Rotation interval: Daily, at 12:00 am
* Retention: 30 files

The log files can be viewed via console or via the PM2 ‘logs’ utility via the console from an SSH session to the EC2 instance hosting the traffic mirroring software.

### Application Error Codes and Descriptions

The application error logs described above will either report application crash errors, or I/O output errors. Each error will be accompanied by a software stack listing. This can be used to determine the types of errors generated.

### Infrastructure Errors

VAM infrastructure is managed by AWS, so no special errors are generated

#### Database

Not applicable, since VAM does not utilize a managed database

#### Web Server

Not applicable, since VAM does not utilize a web server

#### Application Server

Not applicable, since VAM does not utilize an application server

#### Network

The VAM system resides on the production VISTA VPC, which is managed by AWS and the VISTA deployment team.

#### Authentication and Authorization

VAM uses the same authentication RPCs that CPRS uses. Authentication-related errors will be limited to *incorrect login* and *number of tries exceeded* errors.

#### Logical and Physical Descriptions

Please see the *System Boundary Document* and the *System Design Document* for details.

## Dependent System(s)

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

## Troubleshooting

This section is not applicable.

## 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.

### Restart after Non-Scheduled System Interruption

VAM software is managed by PM2 which provides auto-restart capability, and the EC2 instances are managed by AWS Auto Scaling auto-restart capability, so no manual intervention is required for non-scheduled interruption.

### Restart after Database Restore

This section is not applicable. VAM does not utilize a managed database.

### Backout Procedures

Back-out is defined as returning to the best last known operational state of the software and appropriate platform settings.

Please see the V*istA Adaptive Maintenance (VAM) VA Enterprise Cloud (VAEC) Security Deployment, Installation, Backout, and Rollback Guide* for detailed information.

### Rollback Procedures

Please see the V*istA Adaptive Maintenance (VAM) VA Enterprise Cloud (VAEC) Security Deployment, Installation, Backout, and Rollback Guide* for detailed information.

# Operations and Maintenance Responsibilities

There are no operations and maintenance responsibilities in the scope of the VAM project.

# RACI Matrix

Not applicable to VAM VAEC Security.

****

# Approval Signatures

The signatures below indicate approval of the Production Operations Manual.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. Rafael M. Richards Date

*Product Owner*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dave Catanoso Date

*Receiving Organization*

1. Appendix: Acronyms and Abbreviations

Table 1 lists the acronyms and abbreviations used throughout this document, with their descriptions.

Table 1: Acronyms and Abbreviations

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| AWS | Amazon Web Services |
| BPE | Business Partner Extranet |
| EC2 | Amazon Elastic Compute Cloud |
| FedRAMP | Federal Risk and Authorization Management Program |
| FISMA | Federal Information Security Management Act of 2002 |
| GSS | General Support System |
| HIPAA | Health Insurance Portability and Accountability Act |
| IOC | Initial Operating Capabilities |
| PaaS | Platform as a Service |
| RPC | Remote Procedure Call |
| SNS | Simple Notification Service |
| SSP | System Security Plan |
| VA | Department of Veterans Affairs |
| VAEC | VA Enterprise Cloud |
| VAM | VistA Adaptive Maintenance |
| VistA | Veterans Health Information Systems and Technology Architecture |