VistA Adaptive Maintenance VAEC Security (VAM)

Monthly Progress Report



July 2019

Version 1.4

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 07-03-2019 | 1.4 | Updates for June 2019 | AbleVets |
| 06/03/2019 | 1.3 | Updates for May 2019 | AbleVets |
| 05/03/2019 | 1.2 | Updates for April 2019 | AbleVets |
| 04/03/2019 | 1.1 | Updates for March 2019 | AbleVets |
| 03/04/2019 | 1.0 | Initial version of the document | AbleVets |

Table of Contents

[1. Introduction 1](#_Toc10190239)

[2. Work Completed 1](#_Toc10190240)

[3. Work Planned 1](#_Toc10190241)

[4. Risks and Issues 2](#_Toc10190242)

[A. Appendix: Project Deliverables 3](#_Toc10190243)

[B. Appendix: Acronyms and Abbreviations 4](#_Toc10190244)

Table of Tables

[Table 1: Risks and Issues 2](#_Toc10190245)

[Table 2: PWS Project Deliverables 3](#_Toc10190246)

[Table 3: ATO Artifacts 3](#_Toc10190247)

[Table 4: Acronyms and Abbreviations 4](#_Toc10190248)

# Introduction

VistA Adaptive Maintenance (VAM) is a Cloud-Native Platform-as-a-Service (Paas) deployed entirely and exclusively within the U.S. GovCloud FedRAMP-HIGH, HIPAA-compliant VA Enterprise Cloud (VAEC), which leverages Amazon Web Services (AWS) commercial cloud infrastructure, security, 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 leveraging FedRAMP-high VAEC-approved AWS Kinesis and AWS CloudWatch Logs.  VAM provides comprehensive commercial cloud-based VistA RPC Interface monitoring and security for all VISTA systems migrated to the VAEC.

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

 VAM is a 100% Cloud-native, Legacy-free, 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 (i.e. ‘safe’ and ‘non-invasive’). Should VAM ( RPC Mirror or Monitor) be disabled or deactivated, all RPC traffic flows between VISTA and all its Clients as usual, only without any monitoring.

VAM and all its functionality is contained exclusively and entirely as a PaaS within the VAEC, thus inheriting all the security and compliance controls of the FISMA-high VAEC. VAM has no connection with, nor does it share any information with any organization, application, or system outside this VAEC.  VAM is hosted within the FedRAMP-high, HIPAA-certified VA Enterprise Cloud (VAEC) leveraging U.S. GovCloud  Amazon Web Services (AWS).

VAM provides a quadruple aim of (1) reducing the cost and complexity of maintenance for VistA systems; (2) resolving the severe security vulnerabilities within all VistA systems; (3)  taking full advantage of the features, security, and scaling of VA’s commercial cloud capabilities, and (4) ensures the safe, secure, and seamless continuity of veteran care and services as VistA systems are migrated to the VAEC.

This Project VAM Monthly Progress Report covers the Period of Performance (PoP) from June 1 through June 30, 2019.

# Work Completed

The work detailed below was completed during the June 1 through June 30, 2019 PoP.

* Facilitated multiple, weekly status meetings to discuss Team AbleVets’ progress. Meeting minutes can be found on the [VAM workspace](https://github.com/vistadataproject/VAM2ProjectManagement/tree/master/Documents/weekly_meeting_minutes) of GitHub.
* Analyzed the system logs from version D4 of the RPC Definition and Toolkit that capture logins and usage, currently in VistA, to enhance definitions. The logs provided the basis for the Security Vulnerability Report and was deployed on June 7, 2019. (<https://github.com/vistadataproject/RPCDefinitionToolkit/issues/38>)
* Delivered the test framework with the D4 system logs on June 28, 2019. (<https://github.com/vistadataproject/RPCDefinitionToolkit/tree/master/Test>)
* Updated and delivered the PWS artifacts detailed in Table 2 on June 3, 2019
* Delivered CLIN0001AF VAM VAEC Security Weekly Onboarding Status Report on 06-05, 06-12, 06-19 and 06-26.
* Created the Logical and Physical System Boundary and Data Flow document and updated the VAM architecture diagram to include the logical and physical system boundaries.
* Updated VAM’s RiskVision profile by adding the Logical and Physical System Boundary and Data Flow diagrams as evidence for multiple RiskVision controls.
* Updated VAM’s RiskVision profile by adding the details for the new project description provided by the Business Owner.
* Reviewed and updated all controls in RiskVision.
* Updated the documentation in support of the Authority to Operate (ATO) process. Submitted documents in batches and received final signatures, as applicable, for these documents from the PM, Privacy Officer, System Owner, ISO, PIA Support Group, and Business Owner.
* Submitted a request for and received the access to the VAM Pre-Production and Production Environment in the VAEC AWS.
* Deployed the VAM Pre-Production and Production instances in the VAEC AWS.
* Requested the Nessus Scan. It is scheduled to run on 07-15, 2019 as per CSOC
* Requested the Secure Code, and Quality Code Scans. They are delayed due to high current volume of work at the VA level.
* VAM does not require the Database Scan, ISA-MOU, WASA Scan, and Threat Model & Secure Design Review. POAMs for these items were created and submitted to ISO for her signatures.

# Work Planned

The work detailed below is planned for the July 1, 2019 to June 31, 2019 PoP.

* Facilitate weekly status meetings
* Continue updating RiskVision for ISO review
* Submit all relevant information and documentation for the processing of the ATO
* Update project documentation and prepare same for delivery
* Continue analysis of the version D5 logs and enhancement of definitions
* Continue updates to the test framework
* Obtain appropriate Scans for the VAM environments in AWS.

# Risks and Issues

Table 1 lists the currently known risks and issues. Each item will be resolved prior to the delivery of the Build 4 in January, 2020.

Table 1: Risks and Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Issue Number and Category | Due Date | Issue Description | Risk | Mitigation Plan |
| VAM-R18 (PWS Dashboard)  Release Process | 07/31/2019 | Identify a Release Manager and release process. | Without a VA Release Manager there is no point of approval so that the deployment can move forward.  Without a release process the release workflow and acceptance criteria cannot be defined. | Identify the VA Release Manager; formulate and formalize the release process in GitHub. |
| VAM-R10 (ATO Dashboard)  Technical | 8/30/2019 | Receive an ATO | We cannot move to IOC Production without the ATO. | Team AbleVets will continue to refine the RiskVision profile and ATO documentation with guidance from the PM and ISO. |
| VAM-R17 (IOC Dashboard)  Technical | 10/31/2019 | Configure the VAEC IOC environments at Valley Coastal, TX and Omaha, NE | We cannot deliver Dev-Int Build 4 unless there are IOC environments configured. | Migrate the two identified IOC VistA environments to VAEC and establish connectivity. |

1. Appendix: Project Deliverables

Table 2 list the project deliverables required by the PWS, and Table 3 list the artifacts and evidence necessary for the processing of the ATO.

Table 2: PWS Project Deliverables

|  |  |
| --- | --- |
| CLIN | Artifact |
| [0001AA](https://github.com/vistadataproject/VAM2ProjectManagement/blob/master/Documents/source/CLIN%200001AA%20VAM%20Contractor%20Project%20Management%20Plan%20v%201%203.docx) | Contractor Project Management Plan (CPMP) v1.3 |
| [0001AB](https://github.com/vistadataproject/VAM2ProjectManagement/blob/master/Documents/source/CLIN%200001AB%20VAM%20Monthly%20Progress%20Report%20v1%203.docx) | Monthly Progress Report v1.3 |
| 0001AF | Weekly Onboarding Status Report |
| [0003AA](https://github.com/vistadataproject/VAM2ProjectManagement/blob/master/Documents/source/CLIN%200003AA%20VAM%20Master%20Test%20Plan%20v1%203.docx) | Master Test Plan v1.3 |

Table 3: ATO Artifacts

|  |  |
| --- | --- |
| Business Impact Analysis (BIA) | Security Impact Analysis (SIA) |
| Configuration Management Plan (CM Plan) | Signatory Authority |
| Disaster Recovery Plan (DRP) | System Design Document (SDD) |
| Incident Response Plan (IRP) | System Owner Attestation |
| Information Security Contingency Plan (ISCP) | System Owner Responsibilities |
| Privacy Impact Assessment (PIA) | System Security Categorization Report (SSC) |
| Privacy Threshold Analysis (PTA) | System Security Plan (SSP) |
| Risk Assessment |  |

1. Appendix: Acronyms and Abbreviations

Table 4 lists the acronyms and abbreviations used in this document with their descriptions.

Table 4: Acronyms and Abbreviations

|  |  |
| --- | --- |
| Acronym | Description |
| **ATO** | Authority to Operate |
| **AWS** | Amazon Web Services |
| **BIA** | Business Impact Analysis |
| **CM** | Configuration Management |
| **CPMP** | Contractor Project Management Plan |
| **DRP** | Disaster Recovery Plan |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **HIPAA** | Health Insurance Portability and Accountability Act of 1996 |
| **IOC** | Initial Operating Capability |
| **IRP** | Incident Response Plan |
| **ISCP** | Information Security Contingency Plan |
| **ISO** | Information Security Officer |
| **JSON** | JavaScript Object Notation |
| **MUMPS** | Massachusetts General Hospital Utility Multi-Programming System |
| **PIA** | Privacy Impact Assessment |
| **PM** | Project Manager |
| **POM** | Production Operations Manual |
| **PoP** | Period of Performance |
| **PTA** | Privacy Threshold Analysis |
| **PWS** | Project Work Statement |
| **RPC** | Remote Procedure Call |
| **SIA** | Security Impact Analysis |
| **SDD** | System Design Document |
| **SSC** | System Security Categorization Report |
| **SSP** | System Security Plan |
| **VA** | Department of Veterans Affairs |
| **VAEC** | VA Enterprise Cloud |
| **VAM** | VistA Adaptive Maintenance |
| **VDD** | Version Description Document |
| **VistA** | Veterans Health Information Systems and Technology Architecture |