Advanced Medication Platform (AMPL) Graphical User Interface (GUI)

Production Operations Manual (POM)

Version 1.5

November 2024

Department of Veterans Affairs

Revision History

Date	Version	Description	Author
11/2024	1.4	• Content Update	AMPL GUI Team
06/2024	1.3	• No Update	AMPL GUI Team
02/2024	1.2	• Content Update	AMPL GUI Team
08/2023	1.0	• Document Baseline	AMPL GUI Team

Artifact Rationale

The POM provides the information needed by the production operations team to maintain and troubleshoot the product. The POM must be provided prior to release of the product.

Table of Contents

Table of Tables

Table of Figures

1.   Introduction

This document describes how to maintain the components of the Advanced Medication Platform (AMPL) Graphical User Interface (GUI) 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 will be finalized prior to production release and includes many updated elements specific to the hosting environment.

2.   Routine Operations

This section describes procedures and tasks required for normal operations of the system.

2.1.   Administrative Procedures

System administrators complete routine operations to maintain the configuration, upkeep, and reliable operation of computer systems. Additionally, system administrators ensure that the performance, uptime, resources, and security of the systems meet the needs of the end users.

2.1.1.   System Start-up

To verify if the AMPL GUI application is functioning, login to the AMPL GUI server, and run the following commands:

1. Verify that the production EC2 instances are active, if not start them.
2. Navigate to the AWS ECS Cluster page (for AMPL-GUI)
3. Navigate to the production cluster.
4. Verify that the services (API, Web & Preference) are active, and the desired task is not set to 0.
5. If service(s) is down
   a. Change the desired task for the API task to a number greater than 0 and update the service.
   b. Ensure that the API service is active, then change the desired task for the Web task to a number greater than 0 and update the service.
   c. Verify that the API and Web tasks are running.
6. Verify the application is available by connecting to the application with a browser.

2.1.1.1.   System Start-Up from Emergency Shut-Down

In the event of a power outage or other abrupt termination of the server operating systems, please start-up the servers as detailed in the **System Start-up** and allow the operating system to check the disks for corruption.

2.1.2. System Shut-down

To stop the ECS cluster running on EC2 instances there are 2 steps:

1. Stop the ECS Cluster services and tasks.

2. Stop the EC2 instances supporting the ECS Cluster.

2.1.2.1. Emergency System Shut-down

The emergency system shutdown procedure is to shut down all AMPL GUI servers in AWS. These servers may be shut down in any order so the instructions as seen in System Shut-down can be used.
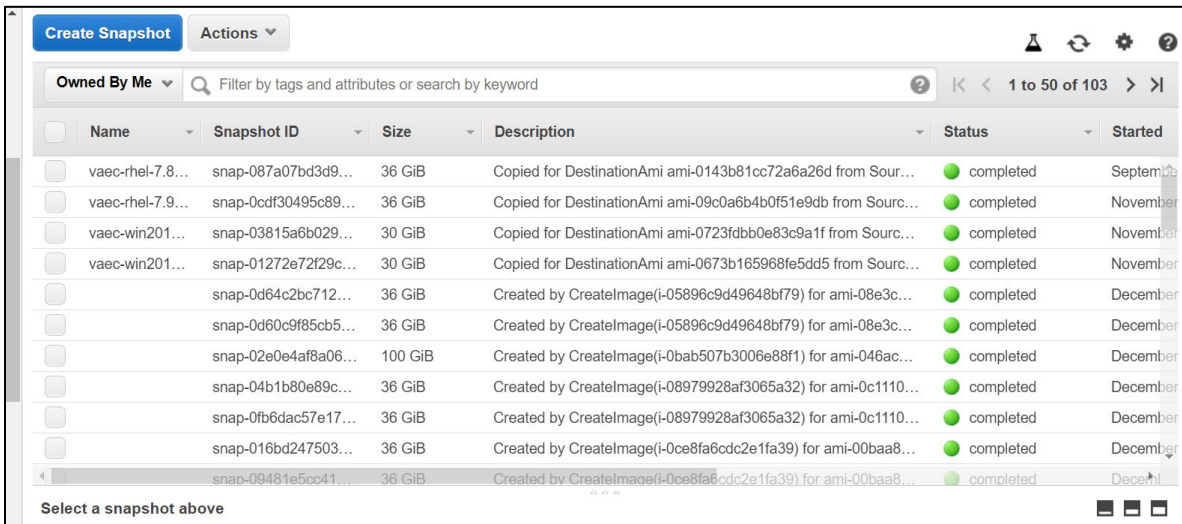
2.1.3. Back-up & Restore

AMPL GUI is created using an infrastructure as code methodology, therefore it is not necessary to create application server-level backups. The underlying infrastructure supporting the Container platform is created using archived scripts that are configuration managed within Veteran (VA) controlled source control.

2.1.3.1. Back-Up Procedures

Auto scheduled snapshots using Lifecycle Manager are utilized to create backup of instances once a week and are retained for three weeks.

Figure 1: Lifecycle Manager

2.1.3.2. Restore Procedures

Please refer to Section 2.1.3.3 Back-up Testing.

2.1.3.3. Back-Up Testing

1. From the Snapshots list, choose the snapshot to create the volume.

2. Click the Actions button and select **Create Volume**.

Figure 2: Actions Button
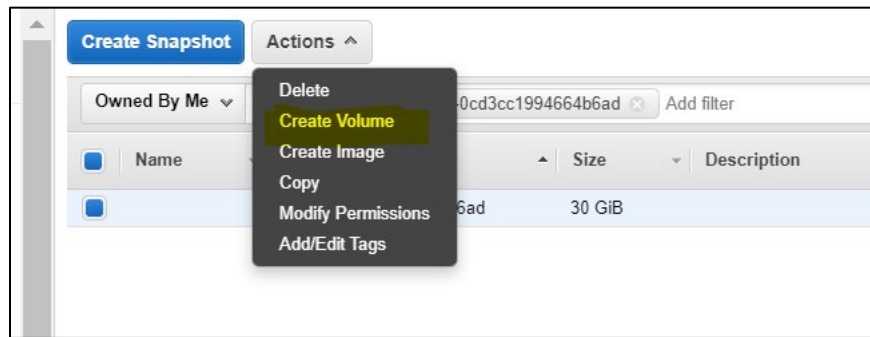
3. Remember, for **Availability Zone**, choose the Availability Zone in which to create the volume.

> **NOTE:** EBS volumes can only be attached to EC2 instances in the same Availability Zone.

4. Choose **Create additional tags** to add the approved VAEC tags to the volume. For each tag, provide a tag Key and a tag Value.

Figure 3: Create Volume

5. Choose **Create Volume**.

6. After you've restored a volume from a snapshot, you can attach it to an instance to begin using it. To do so,

- **Stop** the instance.
- **Detach** the volume and attach the new volume.
- **Start** the instance.

Figure 4: Create Volume Request Succeeded
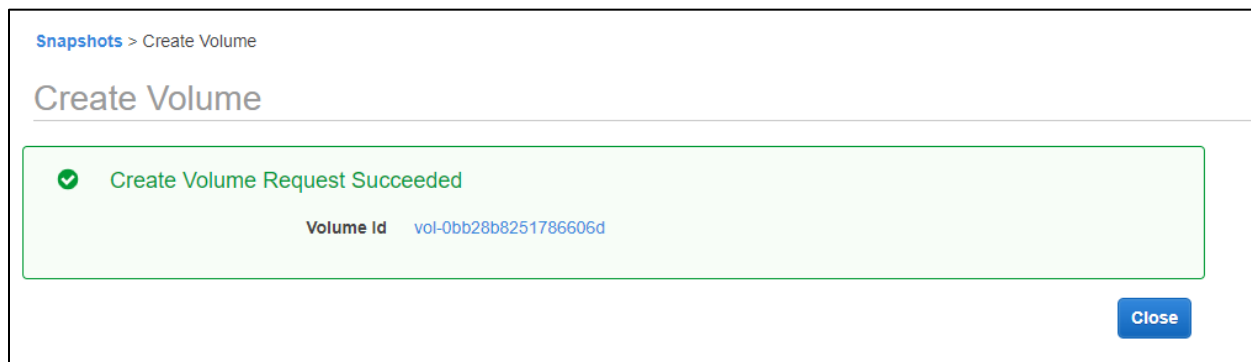
7. **Connect** to instance.

Figure 5: Remote Desktop Connection
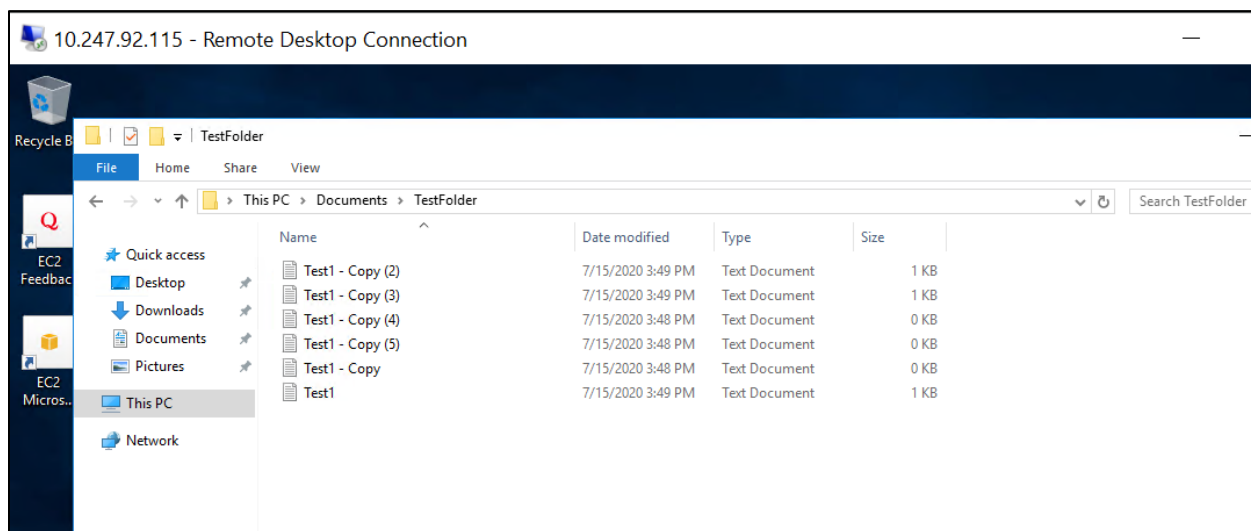
2.1.3.4.   Storage and Rotation

Storage and rotation information is not applicable.

2.2.   Security / Identity Management

AMPL GUI is a read-only viewer of existing enterprise patient data. All data presented in AMPL GUI is obtained from an external source, Veterans Data Integration & Federation (VDIF).

VDIF is outside the ATO boundary of AMPL and implements its own security mechanisms. AMPL uses designated interfaces and security mechanisms to access data via VDIF. Additional information can be found in the *AMPL GUI System Design Document*.

Table 1: AMPL Security Configuration by Environment

AMPL Environment	AD Group	IAM Endpoint
Development	AAC VDIF AMPL	https://int.fed.eauth.va.gov/oauthi/sps/oauth/oauth20/authorize

AMPL Environment	AD Group	IAM Endpoint
	ReadOnly NPD	
SQA	AAC VDIF AMPL ReadOnly NPD	https://sqa.fed.eauth.va.gov/oauthi/sps/oauth/oauth20/authorize
Pre-Prod	AAC VDIF AMPL ReadOnly PPD	https://preprod.fed.eauth.va.gov/oauthi/sps/oauth/oauth20/authorize
Production	AAC VDIF AMPL ReadOnly PRD	https://fed.eauth.va.gov/oauthi/sps/oauth/oauth20/authorize

2.2.1. Identity Management

AMPL GUI only has one user role defined that allows read-only access to Pharmacy specific patient and medication data. There are no administrative roles defined in AMPL GUI.

User authentication is accomplished through Identity and Access Management (IAM) OAuth2 services and users are required to validate their identity with VA issued Personal Identity Verification (PIV) cards.

User authorization is controlled through membership in VA Active Directory (AD) groups. If the user is a member of the appropriate AD group, then they are permitted to retrieve patient data from the VDIF services. Currently there are three AD groups defined for AMPL GUI.

Each AD group permits access to individual AMPL GUI environments and are defined in the table below.

Table 2: AMPL GUI AD Security Groups

AD Group	AMPL Environment	User Group
AAC VDIF AMPL ReadOnly PRD	Production	Production Clinical and Support users
AAC VDIF AMPL ReadOnly PPD	Pre-Production	Test-Site, PBM and SQA test and support users
AAC VDIF AMPL ReadOnly NPD	Development and SQA	Test-Site, PBM and SQA test and support users

2.2.2. Access control

Access to AMPL GUI is granted by membership in an AD group. After initial implementation, a site may request access or removal of an individual by submitting a SNOW ticket by contacting

the Enterprise Service Desk or by using the YourIT portal. The SNow ticket must be assigned to the 'SPM.Health.PCS.Sub_1.AMPL Engineering'" group.

User Notifications

The system administrators will plan maintenance outages on the infrastructure level in AWS Cloud. The planned maintenance calendar will be shared to members of the AMPL team (architects, testers, developers, etc.). Planned outages will be completed on off days (i.e., Friday night or Saturday night). Unplanned outages are addressed when the architect and systems engineer get notified via email.

2.2.3. User Notification Points of Contact

The following table lists the personnel who will be notified in the event of scheduled or unscheduled changes in system state.

Table 3: User Notification Points of Contact

Title	Name	Phone	Email
Business Stakeholder	Amy K. Norris	561-543-8876	Amy.Colon@va.gov
Business Stakeholder	Dionne L. Roney	843-789-6566	Dionne.Roney@va.gov
Technical POC	Asli Goncer	407-359-0506	Asli.Goncer@va.gov
System Owner	Tony Sines	316-249-8510	Tony.Sines@va.gov
Program Manager	James Goldsmith	(903) 267-0663	James.Goldsmith@va.gov
Information System Security Officer	Nathan Mailloux	352-248-0949	Nathan.Mailloux@va.gov

2.3. System Monitoring, Reporting & Tools

This section describes a high-level overview of the monitoring for the AMPL production environment.

2.3.1. Dataflow Diagram

The following figure depicts the AMPL GUI HealthShare Data Flow. Additional information can be found in the *AMPL GUI System Design Document.*

Figure 6: Logical High Level AMPL GUI HealthShare Data Flow
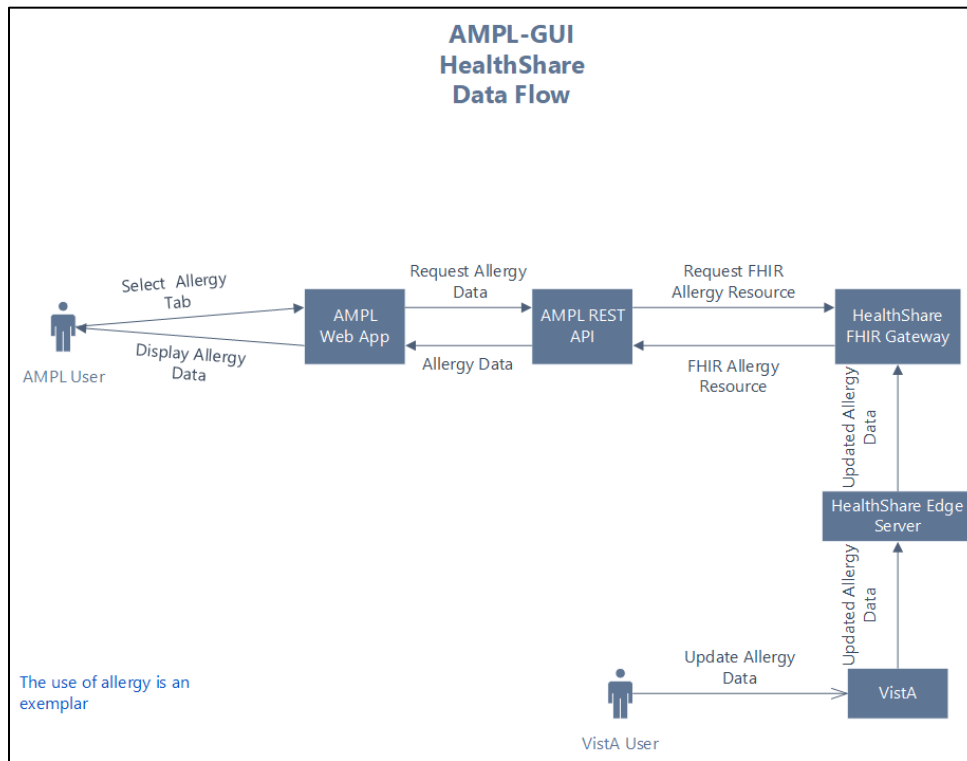
2.3.2. Availability Monitoring

The VA Enterprise Cloud (VAEC) AWS GovCloud High is a General Support System that provides a secure application and hosting environment for VA applications, content, and utilities. These applications and services are used to deliver content to an audience made up of employees, Veterans, contractors, partners across all VA medical centers and component facilities, Federal government, and the general public. Content and applications are provided by Veterans Benefits Administration (VBA), Veterans Health Administration (VHA), National Cemetery Administration (NCA), and Support Offices. VAEC provides the following services: Content delivery, Application Hosting and Management Services.

The VAEC infrastructure is hosted by AWS GovCloud, a cloud service provider. The AWS GovCloud platform is used to provide a variety of hosting environments to suit a variety of needs. AWS GovCloud can support applications categorized up to High as rated in accordance with Federal Information Processing Standard (FIPS) 199. VA applications available to the public are hosted in AWS GovCloud.

A dedicated private data link (AWS Direct Connect) provides all connectivity for VA resources communicating to the environment. Virtual Private Clouds (VPC) wrap the applications within VAEC AWS GovCloud to encapsulate network access. Access from the applications to VA internal resources such as Identity, Credential, and Access Management (ICAM) and AD Services are conducted over the encrypted private data link to the VA network.

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and

actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications, and services that run on AWS and on-premises servers. CloudWatch can be used to detect anomalous behavior in environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep applications running smoothly.

Amazon Simple Notification services are in place to send alerts generated from CloudWatch. The figure below displays the notifications sent. The email notifications are sent to the topics subscribed.

Figure 7: Amazon Simple Notification
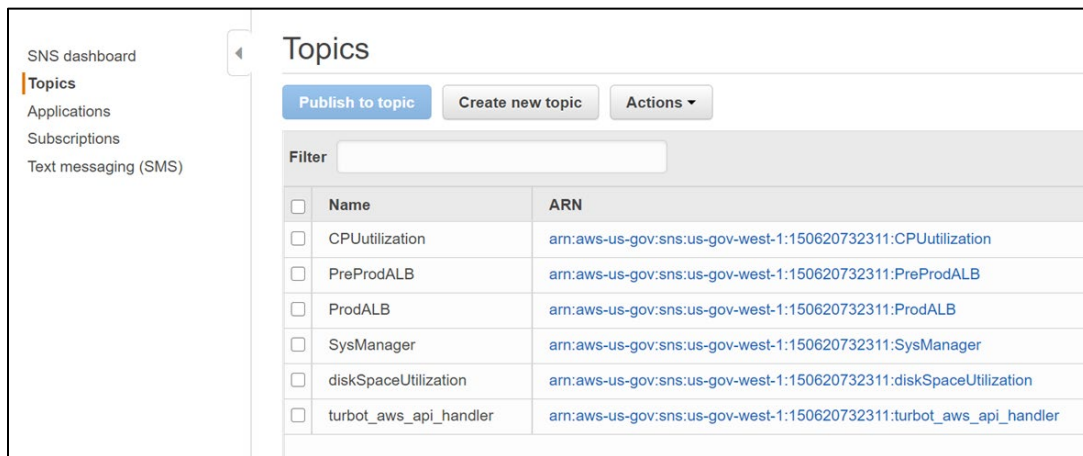
2.3.3. Performance/Capacity Monitoring

Performance monitoring is completed by reaching out to the Monitoring Service Registry (MSR) team and onboarded Dynatrace tool. Elastic Search is the mandatory tool for applications on the cloud.

DynaTrace, ScienceLogic and OpenSearch are in place to address various monitoring requirements. These dashboards provide information about AWS service including the service and application health, uptime, and capacity planning. AWS Cloud Watch and Amazon Simple Notification Service (SNS) notification services are also in place for monitoring and alerting. Reports can be obtained by contacting the POC in Table 4.

Table 4: DynaTrace and Elastic Search Reports POC

Tool	POC	Email Address
DynaTrace	Jennifer Jeffress	Jennifer.Jeffress@va.gov
ScienceLogic	Iran Reynolds	Iran.Reynolds@va.gov
OpenSearch	Nicholas Owusu-Sampah	Nicholas.Owusu-Sampah@va.gov

2.3.4. Critical Metrics

The critical metrics captured for AMPL GUI are covered in <u>Section 2.4.3: Performance/Capacity Monitoring.</u>

2.4. Routine Updates, Extracts and Purges

AMPL GUI does not maintain or store any data. The AMPL GUI application solely uses VDIF services for patient and pharmacy data retrieval. Therefore, the system does not implement or require any data updates, extracts, or purges.

2.5. Scheduled Maintenance

This section includes information on maintenance scheduled for AMPL GUI. The system administrators will plan maintenance outages on the infrastructure level in AWS Cloud. The planned maintenance calendar will be shared to members of the AMPL team (architects, testers, developers, etc). Planned outages will be completed on off days (i.e., Friday night or Saturday night).

2.6. Capacity Planning

The AMPL GUI system has a planned capacity of approximately 14,000 individual users with a maximum of about 4,000 individuals accessing the system simultaneously.

The number of individual users has no impact on AMPL GUI as they are maintained external to AMPL GUI in both the IAM System and the AD system.

The maximum number of simultaneous users is attributable to two factors, the capacity of the AMPL GUI and the capacity of the VDIF systems. To a reasonable extent, the capacity of the AMPL system can be measured in isolation. All testing done to date indicates that production infrastructure exceeds the maximum anticipated load. There is no lower VDIF environment that accurately reflects the production environment and there is no ability to extrapolate performance in production. To date, all tests of the VDIF platform show a deficit in performance.

Both the AMPL and VDIF systems include performance monitoring systems. System capacity is a function of performance, so capacity can be determined in the production environment. This data is periodically reviewed. If a deficit is detected or predicted, then an action plan will be created to resolve the deficit.

2.6.1. Initial Capacity Plan

The initial capacity plan has two phases, and they are outlined in the table below. The AMPL GUI system will be monitored by Dynatrace and other tools. These tools will be used to measure the key metrics.

Table 5: Initial Capacity Plan

Phase	Users	Simultaneous Users	CPU Utilization	Memory Utilization	Response Time
Initial Operational Capability (IOC)	~400	<100	<5%	<50%	Stable
Initial National Deployment	~8000	<1000	<50%	<60%	<20% increase

3. Exception Handling

Similar to other systems, AMPL GUI may generate a small set of errors that may be considered routine, in the sense that they have minimal impact on the user and do not compromise the operational state of the system. Most of the errors are temporary in nature and only require the user to retry an operation. The following subsections describe these errors, their causes, and what response an operator needs to take.

3.1. Routine Errors

While the occasional occurrence of these errors may be routine, getting many individual errors over a short period of time is an indication of a more serious problem. In that case, the error needs to be treated as an exceptional condition. Refer to Significant Errors for more information.

3.1.1. Security Errors

Security is addressed by IAM Single Sign-On Internal (SSOi). User authentication is handled by the IAM SSOi system. The AMPL subsystem does not provide or enforce a security model. However, the system does access other system interfaces which may encounter security violations when accessed.

3.1.2. Time-outs

Time out may occur when accessing the VDIF system. Occasionally queries are dependent upon the availability of VDIF or run out of time if a large results query is requested.

3.1.3. Concurrency

AMPL GUI is a read-only application. As a read-only application maintaining data concurrency on writes is not applicable.

The VDIF services provides a federated view of all the VistA systems maintained by the VHA. There are inherent latencies in this system, so updates from source VistA systems may be delayed. Additionally, data caching is employed at various system layers for performance and may incur additional update latency.

3.2. 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.

3.2.1. Application Error Logs

AMPL GUI uses the AWS CloudWatch for logging of the applications. AMPL uses the Apache Log4j framework for logging.

Logs location – AWS CloudWatch - /ecs/Production-Web and /ecs/Production-Api

Maxfilesize= *To be determined*

Max. backed up files are *To be determined*

Growth rate is capped at *To be determined*

3.2.2. Application Error Codes and Descriptions

An AMPL user may encounter Application System Errors. System Errors are unplanned errors encountered during normal system operation.

These unplanned errors include Java errors (e.g. null pointer exceptions), connection exceptions, and any other unexpected error the system might encounter. The Java errors will be logged in the Application Error Logs.

3.2.3. Infrastructure Errors

VHA IT systems rely on various infrastructure components. These components are defined in the Logical and Physical Descriptions section of this document. Majority of these infrastructure components generate their own set of errors. Each Component has its own sub-section and describes how errors are reported. The sub-sections are typical list of components and are meant to be modified for each individual system.

3.2.3.1. Database

AMPL does not employ a DBMS. The only persistence employed by AMPL is AWS S3 Buckets to store User preference data. This solely configuration data and there is not clinical, PII or PHI data retained.

3.2.3.2. Web Server

There are no expected errors that may come through the web server. Any unexpected errors need analysis of appropriate tools. Additional information can be found on [The Apache HTTP](#).

3.2.3.3. Application Server

AMPL uses Spring Framework and the Spring Framework Exception Handling to capture and log errors. AMPL logs are in AWS CloudWatch. Assistance from AMPL Java Developers may be required to analyze log file entries to diagnose issues.

Network

The physical and virtual network in which AMPL GUI resides is controlled and managed by VAEC COMMS Team and AWS.

3.2.3.4. Authentication & Authorization (A&A)

Users will use VA SSOi and PIV authentication.

A&A error messages include:

- Smart Card Required: The user has not inserted their PIV card into the card reader
- ActivClient: The user's PIV PIN was entered incorrectly

A detailed overview of the login process from the user's perspective is provided in the *AMPL GUI User Guide*. All project documentation is available on the AMPL GUI Product Repository on GitHub.

3.2.3.5. Logical and Physical Descriptions

The VAEC AWS is in one AWS GovCloud region with two Availability Zones. AMPL GUI does not disclose the physical address of its data centers.

Figure 8: AWS GOV Cloud
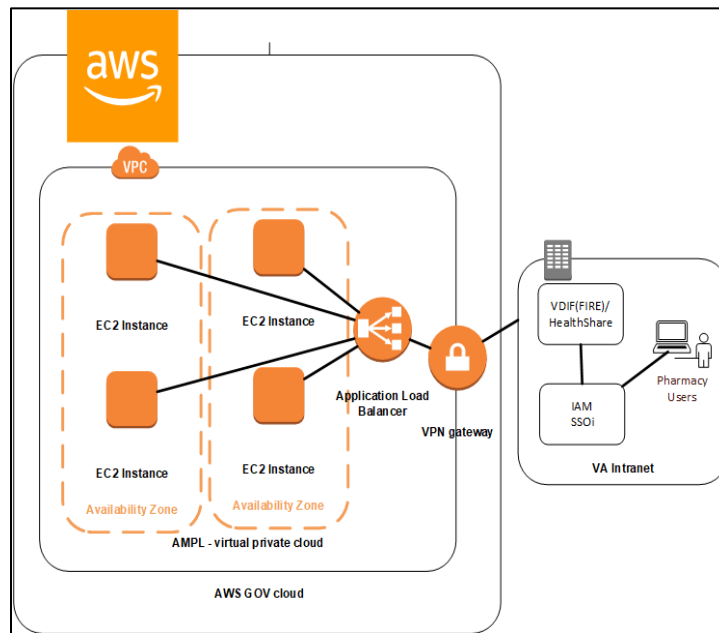
3.3.   Dependent System(s)

The table below lists the other VA systems upon which AMPL GUI depends.

Dependency	Type	Dependency Type	Purpose
Fast Healthcare Interoperability Resources (FHIR)	Service	HL7/FHIR	Mapped data will be provided via VDIF Enterprise Platform (EP) with the use of FHIR messages. Screens display the appropriate fields and map to the appropriate underlining source element
VDIF VCRS	Service	REST	Provides data directly from VistA Instance
Clinical Context Objective Workgroup (CCOW)	Service		Synchronizes AMPL GUI patient context with other clinical applications
IAM SSOi	Service		Authentication and Authorization Security provider

3.4.   Troubleshooting

Tier 1 troubleshooting for internal VA users is handled through the Enterprise Service Desk (ESD). Tier 2 issues are handled by the Clinical Ancillary Products (CAP) Team 1 and troubleshooting is handled directly with the application developers.

3.5.   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.

All hardware, network, and physical infrastructure are the responsibility of AWS and are outside the scope of this document. Recovery priorities are determined based on the criticality to the solution, as well as the number of users impacted and risk for interruption to normal business processes. Detailed processes are provided in the *VAEC System High Availability and Recovery Plan.*

Table 6: System Recovery

IS Services (Application/IS Support Services)	Recovery Priority
JumpBox Service	1

Authentication Services	2
Server Configuration Management Service	3
Vulnerability Scanning Service	4
Monitoring Service	5
Auditing Service	6
Code Configuration and Release Management Services	7

3.5.1. Restart after Non-Scheduled System Interruption

In the event of a power outage or other abrupt termination of the server operating systems, please refer to System Startup from Emergency Shutdown and System Start-up for guidance.

3.5.2. Restart after Database Restore

Refer to System Start-up for the system startup procedures.

3.5.3. Back-out Procedures

For Back-out procedures, refer to the *Deployment, Installation, Backout and Rollback Guide* (DIBR).

3.5.4. Rollback Procedures

For Rollback procedures, refer to the *Deployment, Installation, Backout and Rollback Guide*.

4. Operations and Maintenance Responsibilities

The Operations and Maintenance (O&M) Plan defines the operational support tasks and activities that each of the Office of Information & Technology (OI&T) functional areas are required to provide in the delivery and support of a production enterprise system. The O&M Plan defines specific roles and responsibilities of OI&T functional support teams to avoid confusion over which party is responsible for specific areas of process, tasks, or actions. The O&M plan supports the specific service levels for each activity as defined in the Service Level Agreement (SLA), describes how performance is measured, and identifies the responsible entities for each activity.

All key functions are assigned to one or more responsible parties and activities are clearly defined in order to maintain and support the applications and system components throughout its life cycle. These roles and responsibilities are displayed in a tabular RACI format at the end of each section of the plan to further define **R**esponsibility, **A**ccountability, **C**onsultation, and **I**nformation roles.

Table 7: Operations and Maintenance Responsibilities

Role and Brief Description	Assigned Organization (Pillar and Sub-office)	Contact Information
Enterprise Service Desk (ESD) Tier 1: Provide first contact resolution via the Knowledge section retained in ServiceNow (IT Service Management) ITSM.	ITOPs (ESD)	855-NSD-HELP (855-673-4357)
Tier 2: Provides second level service provider functions, which include problem screening, definition, and resolution. Service requests that cannot be resolved at this level within a set period are elevated to appropriate service providers at the Tier 3 level.	CAP Team 1	Will be routed via ESD Tickets from NSD Tier 1 team.
Tier 3: Provides third level service provider functions, which primarily consist of problem identification, diagnosis, and resolution. Service requests that cannot be resolved at the Tier 2 level are typically referred to the Tier 3 for resolution.	AMPL GUI Development Team	Will be routed via ESD Tickets from AMPL GUI Development Team.

AMPL_GUI RACI.xlsx

5.   Acronyms and Abbreviations

The following table lists acronyms found in this document and provides definitions.

Table 8: Acronyms and Abbreviations

Acronym	Definition
AD	Active Directory
AMPL GUI	Advanced Medication Platform Graphical User Interface
AWS	Amazon Web Services
CAP	Clinical Ancillary Products
CCOW	Clinical Context Objective Workgroup
DIBR	Deployment, Installation, Back-out, and Rollback Guide
EC2	Elastic Compute Cloud
EUO	End-User Operations
FHIR	Fast Healthcare Interoperability Resource

Acronym	Definition
IAM	Identity and Access Management
ICAM	Identity, Credential, and Access Management
IOC	Initial Operating Capability
ITOPS	IT Operations and Services
MSR	Monitoring Service Registry
MPI	Master Person Index
NARS	Network Access Requests
NCA	National Cemetery Administration
O&M	Operation and Maintenance
OI&T	Office of Information and Technology
RACI	Responsibility, Accountability, Consultation, and Information
SLA	Service Level Agreement
SNow	Service Now
SNS	Amazon Simple Notification Service
SRE	Site Reliability Engineers
SSOi	Single Sign-On Integration
VA	Department of Veterans Affairs
VAEC	VA Enterprise Cloud
VBA	Veterans Benefits Administration
VDIF	Veterans Data Integration & Federation
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VPC	Virtual Private Clouds