Enterprise Precision Scanning and Indexing (EPSI)

Software Version 1.2.5

Deployment, Installation, Back-Out, and Rollback Guide (DIBRG)

January 2023

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
1/27/2023	1.1	Added table to section 3.3.2. Updated section 3.2.2.	VetsEZ
8/10/2022	1.0	Initial release	VetsEZ

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan 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 Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan 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

List of Figures

List of Tables

1. Introduction

This document describes how to deploy and install the Enterprise Precision Scanning and Indexing (EPSI) product, as well as how to back-out the product and roll back to a previous version or data set. This document is a companion to the project charter and management plan for this effort. In cases where a non-developed Commercial off the Shelf (COTS) product is being installed, the vendor provided user and installation guides may be used, but the back-out recovery strategy still needs to be included in this document.

1.1. Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the EPSI product will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2. Dependencies

Table 1: System Dependencies

Dependency	Type	Dependency Type	EPSI Use
Centralized VistA Imaging Exchange (CVIX)	Service	Data/Information	Internal service that provides centralized access to VistA Imaging Exchange (VIX) instances via a Representational State Transfer (REST) API interface.
VistA Imaging Exchange (VIX)	Service	Data/Information	Internal service that provides access to VistA Imaging services at each VistA site using a RESTful API interface.
Identity and Access Management (IAM) Single Sign-On (SSOi)	Service	Authentication	Internal service that authenticates EPSI users using various methods, including Personal Identity Verification (PIV) card and username/ password via a WebAgent plugin that is installed on the EPSI proxy server.
Identity and Access Management (IAM) Secure Token Service (STS)	Service	Authentication	Internal service that is used to obtain security tokens required to log in to various other systems like VistA using a Simple Object Access Protocol (SOAP) interface.

Dependency	Type	Dependency Type	EPSI Use
Corporate Data Warehouse (CDW)	Service	Data/Information	Internal data service to interact and query CDW cached data. Data will be a scheduled task to load CDW into the EPSI environment. CDW data will reside within EPSI for lookup and reference within the EPSI decision logic. The data will have its own designated datastore due to it being relational data.

1.3. Constraints

The EPSI project team, software, and test servers will adhere to the following directives, policies, procedures, standards, and guidelines:

- Department of Veterans Affairs (VA) DevOps Process.
- Section 508 Information Technology (IT) accessibility standards governed under 29 U.S.C 794d.
- Health Insurance Portability and Accountability Act (HIPAA).
- VA Directive 6508 – Privacy Impact Assessments.
- VA Directive 6500 – Information Security Program.
- One-VA Technical Reference Model (TRM).
- VA Standards and Conventions Committee (SACC) Codes Standards and Conventions.
- The EPSI app will pass any Web Application Security Assessment (WASA) scans.
- The EPSI app will not have any Critical or High issues identified by a Fortify scan.
- Nessus scans will be performed monthly by VA Cyber Security Operations Center (CSOC).
    - Critical findings will be remediated within 30 days.
    - High findings will be remediated within 60 days.
    - Medium findings will be remediated within 90 days.
    - Low findings will be remediated at the discretion of the System Owner.
- Open security findings are tracked within eMASS as POA&M items.

2. Roles and Responsibilities

Table 2: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase/Role	Tasks
1	Vendor Development	Review/Update DIBRG/POM	Review and update the Deployment, Installation, Back-Out, and Rollback Guide (DIBRG) and Product Operations Manual (POM) documents as required in preparation for deployment.
1	Vendor Development	Deployment in Local Dev	Plan and schedule deployment in local environment.
2	Vendor Development	Deployment in Software Quality Assurance (SQA)/ User Acceptance Testing (UAT) in VA	Determine and document the roles and responsibilities of those involved in the deployment.
3	Vendor Development	Deployment in Production	Test for operational readiness.
4	Vendor Development	Installation	Plan and schedule installation.
6	VA	Installation	Validate through facility point of contact (POC) to ensure that IT equipment has been accepted using asset inventory processes.
8	Vendor Development	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out).
9	Vendor Development	Post Deployment	Hardware, software, and system support.

3. Deployment

This section provides the schedule and milestones for the deployment. The deployment is planned as an iterative rollout.

3.1. Timeline

This section providers the project schedule and milestones for this version.

Table 3: EPSI Task Names and Start Dates

Task Name	Start Date	End Date
Hand-off to SQA	8/1/2022	8/2/2022
SQA Testing	8/3/2022	8/5/2022
Promote Code to Pre-Prod	N/A	N/A

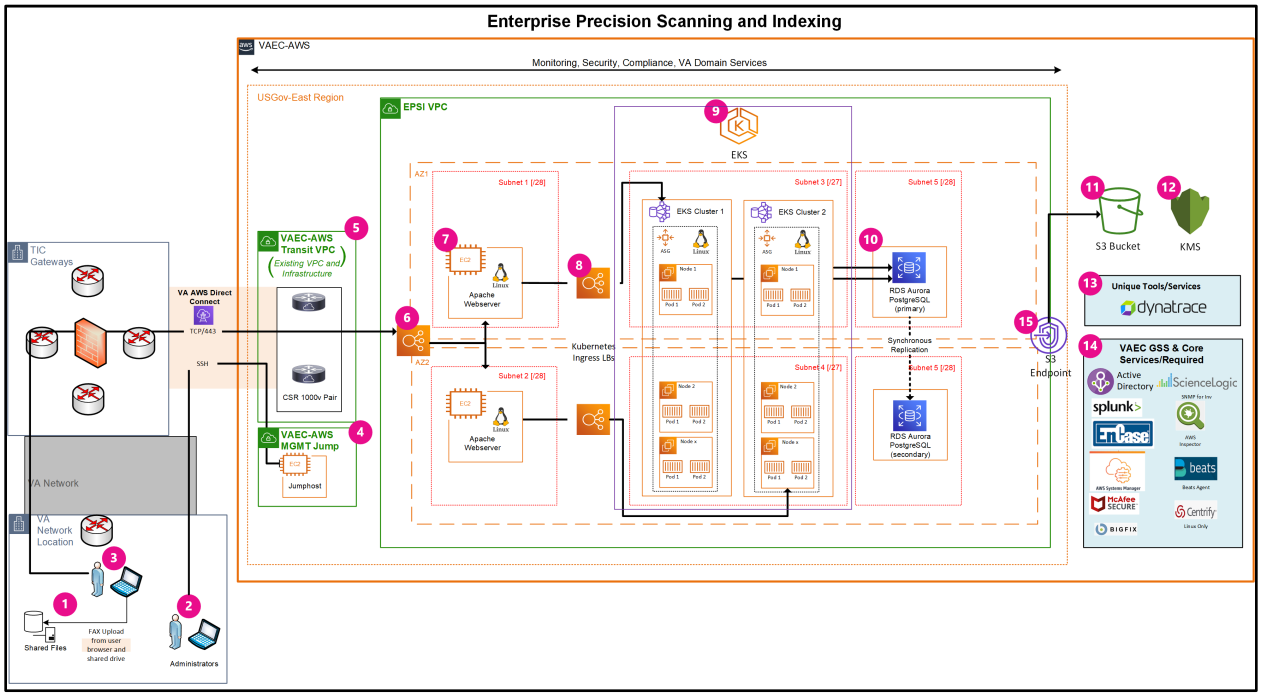
Task Name	Start Date	End Date
Initial Operating Capability (IOC) Testing (Selected Users)	6/13/2022	6/17/2022
IOC Testing (All Sites)	6/21/2022	7/5/2022
IOC Re-Test with Limited Sites	7/11/2022	7/14/2022
Release to Prod	8/15/2022	9/12/2022

3.2. Site Readiness Assessment

3.2.1. Deployment Topology (Targeted Architecture)

The figure below shows the deployment topology (targeted architecture) of the EPSI application.

Figure 1: EPSI Deployment Topology



3.2.2. Site Information (Locations, Deployment Recipients)

EPSI has been deployed nationally to all sites.

3.2.3. Site Preparation

The following table describes preparation required by the site prior to deployment.

Table 4: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
Site	Assign EPSI Site Administrators.	Approve access requests for Indexers, Nurses, and Quality Assurance.	Training	Vendor staff

3.3. Resources

This section describes hardware, software, facilities, documentation, and any other resources—other than personnel—required for deployment and installation.

3.3.1. Hardware

EPSI is in the VA Enterprise Cloud (VAEC) enclave. There are four VAEC cloud environments maintained (see Figure 2). All environments have a common hardware parity with the hardware specifications listed below. All application software and microservice configuration (Kubernetes) are executed on the hardware.

Please refer to Section 2, Roles and Responsibilities, for details about who is responsible for preparing the site to meet these hardware specifications.

Figure 2: Hardware Resources

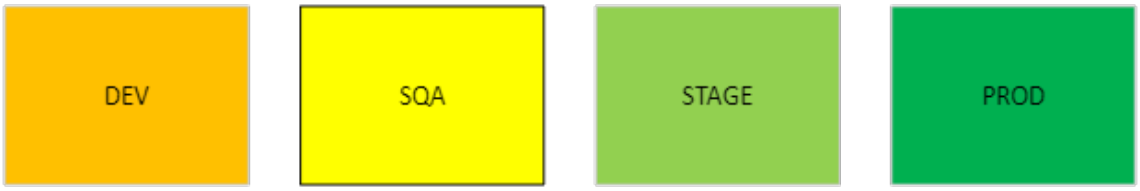


Table 5: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Amazon Web Services (AWS)	M4-M5	Large-XLarge	Virtual	Virtual	All servers

Table 6: Technology Components

Technology Component	Location	Usage
EPSI Production (Production 1) – VA Cloud	VA Cloud environment	To serve the EPSI application within the VA Production environment.

Technology Component	Location	Usage
EPSI Stage (Verification/Test) – VA Cloud	VA Cloud environment	To test the EPSI application within a VA preprod and/or verification environment.
EPSI DEV/SQA/DEMO (Verification/Test) – VA Cloud	VA Cloud environment	To test the EPSI application within a VA test and/or verification environment.
EPSI Development (Development) – Local Development Environments	Developer workstations	To develop and test the EPSI application before transition to the VA cloud environment.

3.3.2. Software

The following tables describe software specifications required at each site prior to deployment.

Table 7: EPSI Technology

Technology	Approval Status	Reference
AWS CloudWatch	Under 3PAO Assessment	https://aws.amazon.com/compliance/services-in-scope/
AWS Elastic Compute (EC2)	FedRAMP Approved	https://aws.amazon.com/compliance/services-in-scope/
AWS Elastic LoadBalancer	FedRAMP Approved	https://aws.amazon.com/compliance/services-in-scope/
AWS RDS Postgres	FedRAMP Approved	https://aws.amazon.com/compliance/services-in-scope/
AWS Simple Storage Service (S3)	FedRAMP Approved	https://aws.amazon.com/compliance/services-in-scope/
Datadog	FedRAMP Approved	https://www.datadoghq.com/blog/datadog-fedramp-moderate-impact-authorization/
Helm 3.8.x	TRM Approved – CY 2023 Q1	https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=14767#
Java 11+	TRM Approved – CY 2023 Q1	https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=14884
Kubernetes 1.21.x	TRM Unapproved – CY 2023 Q1	https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=11815#
ReactJS 17.x	TRM Divest – CY 2023 Q1	https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=10254

Technology	Approval Status	Reference
Red Hat Enterprise Linux (RHEL) 8.x	TRM Approved – CY 2023 Q1	https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=6367
SpringBoot 2.7.x	TRM Approved – CY 2022 Q1	https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=8508
VistA	TRM Approved	N/A

Table 8: Software Specifications

Required Software	Make	Version
Apache	Apache Software	2.4.X
Kubernetes	Red Hat	1.21.X
Elastic Kubernetes Service (EKS)	AWS	eks.4
Docker	Docker, Inc	19.3.X
Red Hat	Enterprise Linux Server	7.X

Please see Section 2, Roles and Responsibilities, for details about who is responsible for preparing the site to meet these software specifications.

3.3.3. Communications

Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance will be disseminated to the business user community a minimum of 48 hours prior to the scheduled event. The Product Owner and Product Manager will be notified via email.

Notification will be distributed to VA users within 30 minutes of occurrence for unscheduled system outages or other events that impact the response time.

Notification will be distributed to VA users as soon as possible for unexpected system outages or other events that impact the response time.

Notification will be distributed to VA users regarding technical help desk support for obtaining assistance with receiving and processing.

3.3.3.1. Deployment/Installation/Back-Out Checklist

The table below outlines the coordination effort and documents for the day/time/individual when each activity (deploy, install, back-out) is completed for EPSI.

Table 9: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual Who Completed Task
Deploy	Dependent on current build timeline.	When approved by VA stakeholders.	Community Care DevSecOps (CCDSO) staff

Activity	Day	Time	Individual Who Completed Task
Install	Dependent on current build timeline.	When approved by VA stakeholders.	CCDSO staff
Back-Out	Dependent on current build timeline.	When approved by VA stakeholders.	CCDSO staff

4. Installation

4.1. Pre-installation and System Requirements

EPSI is a containerized application that runs on Kubernetes. Components are deployed using Helm. The Kubernetes platform used for EPSI is Elastic Kubernetes Service (EKS) which is a cloud managed Kubernetes implementation that greatly simplifies the amount of work needed to maintain the system. Kubernetes deployments are broken into two parts: the Control Plane and the Worker Nodes. EKS manages the Control Plane and provides redundancy and fault tolerance by running it in multiple Availability Zones (AZ). The Worker Nodes are run on AWS Elastic Compute Cloud (EC2) instances built using an Amazon Machine Image (AMI) provided by VAEC.

4.2. Platform Installation and Preparation

The EPSI platform is installed using a set of CloudFormation templates. The templates are broken into the following categories:

- EKS Control Plane
- EKS Nodes
- WebServer Load Balancer
- WebServer Nodes
- SQS Queue
- Database

The templates, scripts and instructions for setting up the EPSI Platform can be found on GitHub at https://github.com/department-of-veterans-affairs/epsi-devops. The repository contains various WIKIs to guide you through the process of setting up the platform on AWS.

4.3. Download and Extract Files

This section not applicable to EPSI project.

4.4. Database Creation

Instructions for installing the EPSI database are covered in Section 4.2, Platform Installation and Preparation.

4.5. Installation Scripts

This section not applicable to EPSI project.

4.6. Cron Scripts

This section not applicable to EPSI project.

4.7. Access Requirements and Skills Needed for the Installation

To install the EPSI Platform and Application, you will need the following:

- Access to the VAEC-epsi account in the VAEC WebGovCloud—your user account should have privileges to run CloudFormation scripts, read from S3 buckets, and provision various compute services (e.g., EKS, EC2, RDS). The Active Directory Federation Services (ADFS)-project-administrator role is typically assigned to users and will have these privileges.
- Access to the EPSI GitHub code repositories with permissions to run GitHub Actions.

4.8. Installation Procedure

Install and upgrade the EPSI application with the following steps. These instructions assume that a GitHub Release exists for the version of the EPSI Application to be installed. The release should document the changes that were made to the application.

1. Navigate your web browser to https://github.com/department-of-veterans-affairs/epsi. Log in if necessary.
2. Select the **Actions** tab.
3. Select **Deploy EPSI** from the left of workflows on the left of the page.
4. Select the **Run Workflow** button, which will open a popup window where you can select the branch from which to run the workflow and the environment to which you wish to deploy EPSI.
    a. For the **Use workflow from** field, always select a tag. GitHub environments are set up to only allow tagged releases to be deployed.
    b. Select the environment to which you which to deploy using the **Environment** input field.
    c. Select the **Run Workflow** button.
5. Deployments to production require approval from a user with Admin permissions in the EPSI repository to proceed with the deployment.

4.9. Installation Verification Procedure

1. Open your web browser.
2. Navigate to https://epsi.va.gov.
3. Log in with your PIV card.

4. Based on user role, validate the application information is correct.
5. Select the person icon on the top right portion of the screen.
6. Verify the provisioned sites are visible as expected.

4.10. System Configuration

This section not applicable to EPSI project.

4.11. Database Tuning

This section not applicable to EPSI project.

5. Back-Out Procedure

This section describes the back-out procedure for EPSI. Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings.

The EPSI system will provide data protection measures, such as back-up intervals and redundancy that is consistent with systems categorized as mission critical (12-hour restoration, 2-hour recovery point objective).

5.1. Authority for Back-Out

Based on authority provided by our Business Sponsor and VA Office of Information and Technology (OIT) IT Program Manager, EPSI can be backed out with their approval.

EPSI can back-out any service within the Kubernetes cluster, which are all application components.

6. Rollback Procedure

Database (DB) snapshots are taken every evening. To restore the EPSI DB instance from a DB snapshot:

1. Sign into the **Amazon Web Services (AWS) Management Console** and open the **(Relational Database Service) RDS** console.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to restore from.
4. For Actions, choose **Restore Snapshot**. The **Restore DB Instance** page displays.
5. For DB Instance Identifier under **Settings**, enter the name that you want to use for the restored Database instance. If you are restoring from a DB instance that you deleted after you made the Database snapshot, you can use the name of that DB instance.
6. Choose **Restore DB Instance**.

6.1. Rollback Considerations

EPSI can roll back the EPSI AWS RDS SQL Server instance.

6.2. Rollback Criteria

Rollback criteria are not applicable.

6.3. Rollback Risks

There is minimal risk associated to these rollback procedures. It is common practice to roll back Kubernetes microservices and is part of the design of the technology. All EPSI application code and infrastructure are maintained as code saved in source control in VA GitHub, so there is minimal potential loss of functionality when an issue arises. Finally, AWS provides highly resilient backup processes for all the EPSI AWS RDS databases.

6.4. Authority for Rollback

Based on authority provided by our Business Sponsor and VA OIT IT Program Manager, EPSI can be backed out with their approval.

6.5. Rollback Procedure

The EPSI system will provide data protection measures, such as back-up intervals and redundancy that is consistent with systems categorized as mission critical (12-hour restoration, 2-hour recovery point objective) for the application and infrastructure. The rollback instructions are the same as back-out for the application.

7. Risk and Mitigation Plan

The EPSI project team maintains a Program Risk Registry. Refer to the Program Risk Registry for all risks and mitigation plans for the entire EPSI project.