Enrollment System (ES) 5.2

Deployment, Installation, Back-out,  
and Rollback Guide



March 2018

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 03/13/2018 | 5.2 | 5.2 update | SMS/Leidos TW |
| 02/12/2018 | 5.1 | For the 5.1 release removed VistA REE information and created a separate DIBRG for it | EHBD TW |
| 02/07/2018 | 5.1 | 5.1 update | SMS/Leidos TW |
| 01/24/2018 | 5.0.1 | 5.0.1 update | EHBD TW |
| 11/06/2017 | 5.0 | 5.0 update | SMS/Leidos TW |
| 09/26/2017 | 4.0 | 4.8 update | SMS/Leidos TW |
| 09/06/2017 | 3.2 | Updated schedules Added Section 4.12 Post-Deployment Tasks | SMS/Leidos TW |
| 08/11/2017 | 3.1 | Added Installation information to Section 4 per RA | SMS/Leidos TW |
| 07/17/2017 | 3.0 | 4.7 update | SMS/Leidos TW |
| 06/21/2017 | 2.3 | 4.6.3 update | SMS/Leidos TW |
| 06/02/2017 | 2.2 | 4.6.2 update | SMS/Leidos TW |
| 05/20/2017 | 2.1 | 4.6.1 update | SMS/Leidos TW |
| 04/15/2017 | 2.0 | 4.6 update | SMS/Leidos TW |
| 01/27/2017 | 1.1 | 4.5.1 update | SMS/Leidos TW |
| 12/15/2016 | 1.0 | Initial publication | SMS/Leidos TW |

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Guide 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 Guide 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

[1 Introduction 1](#_Toc508094656)

[1.1 Purpose 2](#_Toc508094657)

[1.2 Dependencies 2](#_Toc508094658)

[1.3 Constraints 2](#_Toc508094659)

[2 Roles and Responsibilities 3](#_Toc508094660)

[3 Deployment 3](#_Toc508094661)

[3.1 Deployment Timeline and Tasks 3](#_Toc508094662)

[3.1.1 Pre-Deployment Tasks 4](#_Toc508094663)

[3.1.2 Deployment Tasks 5](#_Toc508094664)

[3.2 Site Readiness Assessment 5](#_Toc508094665)

[3.2.1 Deployment Topology (Targeted Architecture) 5](#_Toc508094666)

[3.2.2 Site Information (Locations, Deployment Recipients) 5](#_Toc508094667)

[3.2.3 Site Preparation 5](#_Toc508094668)

[3.3 Resources 6](#_Toc508094669)

[3.3.1 Facility Specifics (optional) 6](#_Toc508094670)

[3.3.2 Hardware 6](#_Toc508094671)

[3.3.3 Software 6](#_Toc508094672)

[3.3.4 Communications 6](#_Toc508094673)

[3.3.5 Deployment/Installation/Back-out Checklist 7](#_Toc508094674)

[4 Installation 8](#_Toc508094675)

[4.1 Pre-Installation and System Requirements 8](#_Toc508094676)

[4.2 Platform Installation and Preparation 8](#_Toc508094677)

[4.2.1 Assumptions/Prerequisites 8](#_Toc508094678)

[4.2.2 Creating a Basic ES Domain 10](#_Toc508094679)

[4.3 Download and Extract Files 12](#_Toc508094680)

[4.4 Database Creation 12](#_Toc508094681)

[4.5 Installation Scripts 12](#_Toc508094682)

[4.6 Cron Scripts 12](#_Toc508094683)

[4.7 Access Requirements and Skills Needed for the Installation 12](#_Toc508094684)

[4.8 Installation Procedure 12](#_Toc508094685)

[4.9 Installation Verification Procedure 13](#_Toc508094686)

[4.9.1 Testing the Installation 14](#_Toc508094687)

[4.10 System Configuration 14](#_Toc508094688)

[4.10.1 Setting Up the ES Web Server 14](#_Toc508094689)

[4.10.1.1 Assumptions/Prerequisites 14](#_Toc508094690)

[4.10.1.2 Setting Up the ES Environment 14](#_Toc508094691)

[4.10.1.3 Installing WebHelp on the Web Servers 15](#_Toc508094692)

[4.10.1.4 Setting up the Enrollment and Eligibility Service (E&E) WebLogic Domain 15](#_Toc508094693)

[4.10.1.5 Setting up the Apache Web Server to Tunnel the Web Service Requests 17](#_Toc508094694)

[4.10.1.6 Setting Up TLS Authentication in E&E Servers 17](#_Toc508094695)

[4.10.1.7 Steps for VHAESRAPP45 Server 18](#_Toc508094696)

[4.10.1.8 Steps for VHAESRAPP46 Server 19](#_Toc508094697)

[4.10.1.9 Log On to WebLogic Administration Console for VHAEES\_PROD 20](#_Toc508094698)

[4.10.1.10 Setting up JMS Queues in E&E Servers 21](#_Toc508094699)

[4.11 Database Tuning 22](#_Toc508094700)

[5 Back-out Procedure 22](#_Toc508094701)

[5.1 Back-out Strategy 22](#_Toc508094702)

[5.2 Back-out Considerations 23](#_Toc508094703)

[5.2.1 Load Testing 23](#_Toc508094704)

[5.2.2 User Acceptance Testing 23](#_Toc508094705)

[5.3 Back-out Criteria 23](#_Toc508094706)

[5.4 Back-out Risks 24](#_Toc508094707)

[5.5 Authority for Back-out 24](#_Toc508094708)

[5.6 Back-out Procedure 24](#_Toc508094709)

[5.7 Back-out Verification Procedure 24](#_Toc508094710)

[6 Rollback Procedure 24](#_Toc508094711)

[6.1 Rollback Considerations 24](#_Toc508094712)

[6.2 Rollback Criteria 24](#_Toc508094713)

[6.3 Rollback Risks 25](#_Toc508094714)

[6.4 Authority for Rollback 25](#_Toc508094715)

[6.5 Rollback Verification Procedure 25](#_Toc508094716)

List of Tables

[Table 1: Key Roles and Responsibilities for Deployment, Installation, Back-out, and Rollback 3](#_Toc508094717)

[Table 2: ES 5.2 Deployment Timeline 4](#_Toc508094718)

[Table 3: ES 5.2 Pre-Deployment Tasks 4](#_Toc508094719)

[Table 4: ES 5.2 Deployment Tasks 5](#_Toc508094720)

[Table 5: ES 5.2 Deployment Communication Schedule 6](#_Toc508094721)

[Table 6: Contact List for ES 5.2 Deployment 7](#_Toc508094722)

[Table 7: Deployment/Installation/Back-out Checklist 7](#_Toc508094723)

[Table 8: Resources with the Authority to Authorize a Back-out 24](#_Toc508094724)

List of Figures

[Figure 1: Verifying Linux is installed and configured properly (CO40331FY07) 8](#_Toc508094725)

[Figure 2: Checking that Missing Linux 32-bit Shared Libraries are Installed (CO36416FY06) 9](#_Toc508094726)

[Figure 3: Setting up the WebLogic Linux Account with Environment Variables 10](#_Toc508094727)

[Figure 4: Checking the limits.conf File is Correct 10](#_Toc508094728)

[Figure 5: ES-VADIR Security Boundary 18](#_Toc508094729)

[Figure 6: JMS Configuration – EDEV and SQA 21](#_Toc508094730)

[Figure 7: JMS Configuration – Pre-Prod and Prod 22](#_Toc508094731)

# Introduction

The mission of the Department of Veterans Affairs (VA) Office of Information and Technology (OIT), Enterprise Program Management Office (EPMO) is to provide benefits to Veterans and their families. In order to meet this overarching goal, OIT is charged with providing high quality, effective, and efficient IT services and Operations and Maintenance (O&M) to persons and organizations that provide point-of-care services to our Veterans.

The VA’s goals for its Veterans and families include:

* Make it easier for Veterans and their families to receive the right benefits, and meeting their expectations for quality, timeliness, and responsiveness.
* Improve the quality and accessibility of health care, benefits, and memorial services while optimizing value.
* Provide world-class health care delivery, by partnering with each Veteran to create a personalized, proactive strategy to optimize health and well-being, while providing state of the art disease management.
* Ensure awareness and understanding of the personalized, proactive, and patient-driven health care model through education and monitoring.
* Provide convenient access to information regarding VA health benefits, medical records, health information, expert advice, and ongoing support needed to make informed health decisions and successfully implement the Veteran’s personal health plans.
* Receive timely, high quality, personalized, safe, effective, and equitable health care, not dependent upon geography, gender, age, culture, race, or sexual orientation.
* Strengthen collaborations with communities and organizations, such as the Department of Defense (DoD), Department of Health and Human Services (DHHS), academic affiliates, and other service organizations.

In order to assist in meeting these goals, the Enterprise Health Benefits Determination (EHBD) program will provide enterprise wide enhancements and sustainment for the following systems/applications:

* The Enrollment System (ES) assists Veterans to enroll for VA healthcare benefits and is the core application that feeds other VA systems with Enrollment and Eligibility (E&E) data.
* Income Verification Match (IVM) assists in determining priority grouping for healthcare eligibility.
* VistA Registration, Eligibility & Enrollment (REE) shares information with other VistA applications and enables registration and eligibility determinations and enrollment at VA Medical Centers (VAMC).
* Veteran’s On-Line Application (VOA) is re-purposed for the online Veterans Health Benefits Handbook (VHB). VHB provides each enrolled Veteran on-demand online access to a personalized and dynamic health benefits-related Handbook.

Enrollment System Modernization (ESM) defines health benefit plan(s) for which a client (Veteran, Service Member, or beneficiary) is eligible and ties them to the authority for care. Key enhancements to be completed include Pending Eligibility Determination, fixes to the Enrollment System, Date of Death, Internal Controls, Workflow, Veterans Financial Assessment, converting of Military Service Data Sharing (MSDS) to Enterprise Military Information Service (eMIS), Manage Relationships, Veteran Contact Service, and support for Enrollment System Community Care (ESCC).

The *ES 5.2 Deployment, Installation, Back-out, and Rollback Guide* defines the ordered, technical steps required to deploy and install the ES 5.2 release, as managed through the Enrollment Health Benefits Determination (EHBD) Program and ESM and ESCC projects and, if necessary, to back out the installation and to roll back to the previously installed version of the product.

## Purpose

The purpose of this guide is to provide a single, common document that describes how, when, where, and to whom the ES 5.2 software enhancements will be deployed and installed, as well as how they are 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.

## Dependencies

ES 5.2 depends on the Administrative Data Repository (ADR) to store the audit logs. High Availability (HA) for the ADR is 99.95% (excluding planned down time). Maintenance is scheduled in advance. The ADR Recovery Time Objective (RTO) is within 12 hours of a disaster declaration, and Recovery Point Objective (RPO) defines a loss of no more than 120 minutes of data.

ES 5.2 depends on the following systems and organizations, which are managed separately and their maintenance details are outside the scope of ES 5.2.

* Administrative Data Repository (ADR)
* Identity Management (IDM)
* Enterprise Military Information Service (eMIS)
* Enterprise Contact Information Service (eCIS)
* VistA Interface Engine (VIE)
* Veterans Benefits Administration (VBA)

## Constraints

There are no constraints for the ES 5.2 deployment.

# Roles and Responsibilities

Table 1 lists the key roles and responsibilities for the deployment, installation, back-out, and rollback of ES 5.2.

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

| Role | Description |
| --- | --- |
| Austin Information Technology Center (AITC) | The team at the AITC that supports ES |
| Development Team | Office of Information and Technology (OIT) Enterprise Program Management Office (EPMO) |
| Project Manager (PM) | Delwin C. Johnson |
| Health Eligibility Center (HEC) Representatives | Users of ES applications |

# Deployment

This section provides the schedule and milestones for the ES 5.2 deployment.

Deployment of ES 5.2 is planned as a one-time rollout to the Austin Information Technology Center (AITC). Deployment will be performed by team members from one or more of the operations organizations including Enterprise Operations (EO).

Deployment of the ES 5.2 release will be performed by Office of Information and Technology (OIT) team members with representatives from peer organizations as needed. Installation will be performed by AITC team members, along with representatives from peer organizations.

## Deployment Timeline and Tasks

A detailed step-by-step timeline, with estimated time of completion for all ES and related tasks, will be created by AITC Operations. AITC will also direct and manage all activities, including:

* Orderly shutdown
* Startup
* Configuration
* Deployment tasks

The ES development team will be under the direction of the task lead. A Microsoft LYNC meeting will be available if needed and decision makers may be given a time to call in for a status of the deployment.

* National Release of ES 5.2 is scheduled for April 07, 2018.
* Tentative time for ES 5.2 deployment start is 04/07/2018 at 2 PM CDT. Deployment is to be completed or rolled back by 04/07/2018 at 10 PM CDT.

Table 2 indicates the ES 5.2 deployment is scheduled to be completed in less than one day.

Table : ES 5.2 Deployment Timeline

| Details | Start Date | Completion Date | Responsible Party |
| --- | --- | --- | --- |
| Train the Trainer | 03/28/2018 | 03/28/2018 | SMS/Leidos and AITC |
| User Functionality Testing (UFT) | 03/14/2018 | 03/29/2018 | HEC, OCC/SEM, Test Team |
| Deploy to Production | 04/07/2018 | 04/07/2018 | ES Team and AITC |

### Pre-Deployment Tasks

Table 3 lists the Enrollment System pre-deployment tasks that need to be performed to successfully deploy ES 5.2.

Table : ES 5.2 Pre-Deployment Tasks

| Task Name | Description | Responsibility | Date Run |
| --- | --- | --- | --- |
| Validate checksums | Verify that the md5sum on each included WAR and EAR file is identical to those submitted in the Service Request or Change Order. | CM and Architect | Deployment Date minus one day |
| Verify configuration files | Two people must verify the data in the configuration files from the built WAR and EAR files against the master document to ensure that all the parameters are pointing to the respective production configurations. | Architect and Developer | Deployment Date minus one day |

### Deployment Tasks

Table 4 lists the Enrollment System deployment tasks that need to be performed to successfully deploy ES 5.2.

Table : ES 5.2 Deployment Tasks

| Description | Who? | Timing | Time to Complete |
| --- | --- | --- | --- |
| Shut down the servers, delete the previous deployment, and run the clean\_logs.sh to remove previous versions of the ui.war file by:  On admin server:  /u01/app/bea12/user\_projects/domains/ESRDomain/servers/ESRDomainAdmin/tmp rm –rf \_WL\_TEMP\_APP\_DOWNLOADS/  On admin and all the managed servers:  /u01/app/bea12/user\_projects/domains/ESRDomain/servers/MS\*/tmp rm –rf \_WL\_user/  /u01/app/bea12/user\_projects/domains/ESRDomain/servers/MS\*/cache rm –rf EJBCompilerCache | AITC | Prior to deploying the 5.2 EAR file | N/A |
| Deploy the ES 5.2 esr.ear, ccn-ws.war, msds-ws.war and ecis-ws.war files and all related packages per the instructions in the Change Order | AITC | Per deployment task list | 30 minutes |

## Site Readiness Assessment

ES 5.2 will be deployed at the Austin Information Technology Center (AITC) to application server virtual machines. AITC application managers will create a Deployment Checklist a week before the ES 5.2 deployment, and it will be reviewed by all participants.

### Deployment Topology (Targeted Architecture)

No changes to existing topology are introduced by ES 5.2.

### Site Information (Locations, Deployment Recipients)

ES 5.2 will be installed at the AITC.

### Site Preparation

A train-the-trainer session covering the changes included in the ES 5.2 release will be provided by the ES development team. The session includes a presentation and a demonstration of Online Help.

## Resources

This section describes the hardware, software, facilities, documentation, and any other resources, other than personnel, required for the deployment and installation of ES 5.2.

ES 5.2 represents a release to the production ES that is housed and maintained at the AITC. Deployment will be the shared responsibility of OIT and AITC.

### Facility Specifics (optional)

There are no special site preparation requirements for ES 5.2.

### Hardware

There are no hardware changes required for the implementation of ES 5.2.

### Software

There are no special software requirements for implementation of ES 5.2, outside of the application build.

### Communications

In preparation for the ES 5.2 deployment/installation, the ES 5.2 development team participates in planning meetings with AITC. As part of the ES 5.2 deployment, an Automated Notification Report (ANR) is created by AITC to notify all stakeholders of the planned outage. In addition, AITC sends follow up emails to include all Primary and Secondary stakeholders to announce the start and end of the deployment and any pertinent details of the current status of the System of Systems. This includes the deployed version of the ES software at the end of the outage.

Table 5 lists the communication schedule for the ES 5.2 deployment. The dates are correct, although the specific times might vary.

Table : ES 5.2 Deployment Communication Schedule

| Event | Date/Time | Method | Participants |
| --- | --- | --- | --- |
| Incident Management Automated Notification Reporting (ANR) | 04/07/2018, 2 PM CDT | Email notification and Enterprise Service Desk (ESD) Website | ESD and AITC |
| Deployment Commencement | 04/07/2018, 2 PM CDT | Email notification | Deployment Team, stakeholders |
| Status Update | 04/07/2018, 6 PM CDT | LYNC | Decision Owners, Deployment Team |
| Deployment Completion | 04/07/2018, 10 PM CDT | Email notification | Deployment Team, stakeholders |

Table 6 lists the contacts for deployment of ES 5.2.

Table : Contact List for ES 5.2 Deployment

| Name | Contact | Organization |
| --- | --- | --- |
| Ralph Weishaar | PII | Director for Internal Control |
| Delwin C. Johnson | PII | OIT Enterprise Health Benefits Determination (EHBD) PM |
| Joshua Faulkner | PII | Technical Lead, Enrollment System |
| Jim Steele | PII | AITC Operations, Division Chief |
| Patty Britten | PII | Senior IT Specialist, AITC |
| Asad Hafeez | PII | Linux System Administrator, AITC |
| Dinesh Punyala | PII | WebLogic Admin, AITC |
| Roger Dowling | PII | Senior System Analyst; VIE Admin, AITC |
| 005QD3 MGMT SYSTEMS HPS ADMIN1ES | PII | Secondary stakeholder (information only) |

### Deployment/Installation/Back-out Checklist

Table 7 captures the coordination effort and documents the day/time/individual when each activity (deploy, install, back-out) is completed for a project.

Table : Deployment/Installation/Back-out Checklist

| Activity | Day | Time | Individual Who Completed Task |
| --- | --- | --- | --- |
| Deploy | <day> | <time> | <name> |
| Install | <day> | <time> | <name> |
| Back-out | <day> | <time> | <name> |

# Installation

## Pre-Installation and System Requirements

This section assumes that the reader has knowledge of WebLogic administration tasks using the administration console. More detailed information is available from the official documentation via the following links:

* [Fusion Middleware Administering Oracle Fusion Middleware](https://docs.oracle.com/middleware/12212/lcm/ASADM/toc.htm)
* [Fusion Middleware Installing and Configuring Oracle WebLogic Server and Coherence](https://docs.oracle.com/middleware/12212/lcm/WLSIG/toc.htm)
* [Fusion Middleware Downloads for Oracle WebLogic Servers](http://www.oracle.com/technetwork/middleware/weblogic/downloads/wls-main-097127.html)

## Platform Installation and Preparation

### Assumptions/Prerequisites

The following assumptions and prerequisites apply to all WebLogic servers that will be part of the domain.

1. Verify Linux is installed and configured properly (CO40331FY07)

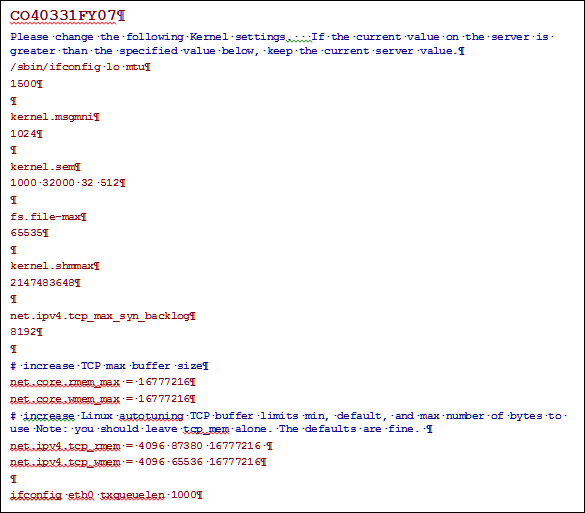


Figure : Verifying Linux is installed and configured properly (CO40331FY07)

1. Make sure the missing Linux 32-bit shared libraries are installed (CO36416FY06)



Figure : Checking that Missing Linux 32-bit Shared Libraries are Installed (CO36416FY06)

1. Set up the WebLogic Linux Account with the following environment variables set in either .profile or .bash\_profile (The BEA and Java version might change).

* The WebLogic account must have read and write access to the tmp directory.
* The WebLogic account must have read access to the JAVA\_HOME directory.



Figure : Setting up the WebLogic Linux Account with Environment Variables

1. Make sure the limits.conf file is correct (limits.conf@vaaacappl).

****

Figure : Checking the limits.conf File is Correct

1. Set up sudo to allow administrators to sudo su – WebLogic
2. BEA WebLogic 12.2.1 is installed to the location where the BEA\_HOME variable is set.
3. Install Java to the location where the JAVA\_HOME variable is set.
4. Create a node manager directory as set by a NODEMGR\_HOME variable.

### Creating a Basic ES Domain

ES will provide the domain creation scripts in a file named domain-scripts.tar.gz when it is time for initial domain configuration. The following steps apply to the server that will become the WebLogic administrative console.

1. sudo to the WebLogic12 account or login as the WebLogic12 user.
2. SCP the domain-scripts.tar.gz file to /tmp/domain-scripts on the server.
3. Unzip the domain-scripts.tar.gz file into the /tmp/domain-scripts directory.  
   cd /tmp/domain-scripts  
   tar –xzf domain-scripts.tar.gz
4. If the installDomain.sh or createBatchProcDirectory.sh file is not executable, make it executable.  
   chmod 744 \*.sh
5. Create the basic ES Domain by running the installDomain.sh script from the  
   /tmp/domain-scripts directory.  
   ./installDomain ESDomain.jar ESDomain
6. Create soft links to the ES Domain and node manager directories in the WebLogic home directory  
   cd ~  
   ln –s /u01/app/bea12/user\_projects/domains/ESDomain  
   ln –s /u01/app/bea12/nodemanager/
7. CD to ES Domain directory.  
   cd /u01/app/bea12/user\_projects/domains/ESDomain/
8. Rename the startWebLogic.sh script to startWeblogic.sh   
   mv startWebLogic.sh startWeblogic.sh

**Note:** Notice that there is a difference in uppercase “L” and lowercase “l”

1. Run ./startWeblogic.sh &

**Note:** Notice the background execution, to start the WLS Admin server the very first time.

* 1. Create new admin users by navigating to Security -> Realms -> myrealm -> Users.
  2. On the General tab, create a new administrator user account and password.
  3. Click Apply.
  4. On the Group tab, assign the user to the Administrators group.
  5. Click Apply.
  6. Delete the default WebLogic user.

1. Run ./stopWeblogic.sh <newUserName> <newPassword> to stop WLS Admin.
2. Delete boot.properties from your domain.  
   rm boot.properties
3. Set up the environment so that the boot.properties file gets recreated.  
   export JAVA\_OPTIONS=-DWebLogic.system.StoreBootIdentity=true
4. Run ./startWeblogic.sh

**Note:** (Foreground execution) to start the WLS Admin server. When asked to provide user name and password, use your new admin user name and password.

1. In another terminal, logged in as the WebLogic user, and in the ESDomain directory, run ./storeCredentials.sh t3://<servername>:7001 <newUserName> <newPassword> to store the admin user credentials so that you do not have to provide user IDs and passwords from the command line every time a script is run. Replace the tags in < > with the appropriate values.
2. Run ./stopWeblogic.sh to stop WLS Admin.
3. Remove the JAVA\_OPTIONS environment variable or logoff the session.  
   export JAVA\_OPTIONS=
4. One of the servers in the cluster will act as the file store for batch processes. The required directory tree can be created by running the ./createBatchProcDirectory.sh script in the ESDomain directory on the host server. All other servers in the cluster should mount a remote directory to /u02/batchProcess.

**STOP:** You are now ready to install ES, which will occur later.

## Download and Extract Files

Download and extract files do not apply to ES 5.2.

## Database Creation

No database creation is required for implementation of ES 5.2.

## Installation Scripts

No installation scripts are required for implementation of ES 5.2.

## Cron Scripts

No cron scripts are required for implementation of ES 5.2.

## Access Requirements and Skills Needed for the Installation

For installation, no access requirements or skills are required for ES 5.2.

## Installation Procedure

Specific installation procedures are managed and controlled by AITC and are under configuration control by the AITC application managers.

ES will provide the scripts.zip, config.xml, and esr.ear files when it is time for installation. The files in the scripts.zip file and the config.xml file will replace the scripts in the ESRDomain directory.

**Before** the scripts, config.xml, and esr.ear can be built, packaged and delivered, the development team needs to be notified with server names, server IP addresses, WebLogic admin user name, WebLogic admin user password, and CAIP server URL, so the nodemanager.host and config.xml files can be customized for the environment.

Steps 1 to 5 and 10 need to be done when ES is installed for the first time. For subsequent installations, ignore these steps.

1. Unzip the contents of the **scripts.zip** into ESRDomain directory on all application servers.
2. Set permissions:  **chmod 774 /u01/app/bea12/user\_projects/domains/ESRDomain/\*.sh**
3. Copy the new config.xml into ESRDomain directory on the admin server.
4. In the ESRDomain directory, open **config.xml** in vi. Navigate to the bottom of the file and find the **<EmbeddedLDAP** stanza and the **<SecurityConfiguration** stanza. In another window and still in the ESRDomain directory, run cat on **config.xml.booted**. Find the **<EmbeddedLDAP** stanza and the **<SecurityConfiguration** stanza. Replace the stanzas, similar to the strings below, with the like stanzas from the **config.xml.booted** file. **<EmbeddedLDAP CredentialEncrypted="{3DES}RHyup5TdHu/0p4Tb8Q3mFaI3v/1337YOyP//LJaiVY8=" Name="ESRDomain"/>  
   <SecurityConfiguration CredentialEncrypted="{3DES}sAMA66CtQIOvXiEHSqDrHM82+oyF3+5/paQ1oVzr1o/RQ5RgR0LBEqQQ1AKLvMxF1gCxTShpe52e+Mobv5XbYoiWhFs2lz7j"   
   Name="ESRDomain" RealmBootStrapVersion="1"/>**
5. Copy the new **nodemanager.hosts** under the **nodemanager** directory of all the servers.
6. Using the existing scripts on the servers, shut down ES cluster, node manager, and admin server processes by running: **.**/stopCluster.sh  
   ./stopNodemanager.sh   
   ./stopWebLogic.sh).
7. Run "**./cleanLogs.sh 2**" on all servers.
8. Copy the new **esr.ear, esr-ws.war,** and **ccn-ws.war**into **/u01/app/bea12/user\_projects/domains/ESRDomain/applications/** directory on the admin server.
9. Copy the new webhelp.zip to /u01/app/webhelp on each of the Web Servers.
10. Start admin server on the admin server (run ./**startWebLogic.sh &** from the ESRDomain directory in the background).
11. On another terminal, logged in as the WebLogic user, and in the ESRDomain directory, run **./storeCredentials.sh <newUserName> <newPassword> t3://<servername>:7001** to store the admin user credentials, so that you do not have to provide user IDs and passwords from the command line every time a script is run. Replace tags in < > with the appropriate values.

**Note:** This step is needed when ES is installed for the first time on a server. For subsequent installations, skip this step.

1. Start node manager processes on all the servers (run **./startNodeManager.sh &** in the background).
2. Start all ES clusters (**run ./startCluster.sh** from the ESRDomain directory on the admin). This command will start 3 clusters: ES Cluster1, ES Cluster2, and ES Cluster3.
3. After the previous step is complete, check if ES is installed successfully on all 6 servers. Log onto ES with the appropriate URL.

## Installation Verification Procedure

1. After ES and Person Service Identity Management (PSIM) are brought up, but before the VIE is started, verify that the ES-PSIM connection is functioning properly.
2. Verify that the VistA Interface Engine (VIE) can pull and push messages to ES.  
   Verify that ES can send and process the messages correctly.
3. Verify that Enrollment and Eligibility (E&E) can connect to ES and retrieve data.
4. Verify that the Enterprise Military Information Service (eMIS) queries are working and response can be received.
5. Verify the online applications are processing from vets.gov.
6. Verify that the Veterans Benefit Repository (VBR) URL is functional.
7. Verify that the User Interface (UI) navigation to all of the screens is working correctly.
8. Verify that the batch processes can read and write to the following folder:  
   /u02/batchProcess
9. Verify that batch processes are voided when the respective input files are missing in the following folder:  
   /u02/batchProcess
10. Verify that Income Verification Match (IVM) Polling Service has restarted and is reaching ES.

### Testing the Installation

To test the installation, try accessing the following URL:  
<https://DNS.URL:PORT/esr-ws/spring-ws/getEESummary/eeSummary.wsdl>

**Notes:**

* This varies according to the environment (Development, SQA, PreProd and Prod).
* The E&E Web Service is dependent on **ESR.ear** deployed on the WebLogic 12.2 server.

## System Configuration

### Setting Up the ES Web Server

#### Assumptions/Prerequisites

The Apache Web Server was installed on the Linux boxes.

#### Setting Up the ES Environment

Because ES can run on multiple Web Servers, depending on the environment (Prod, SQA, DR, EDEV), the steps below need to be repeated on each of the Web Servers for that specific environment.

1. Login to the Linux server that has the Apache Web Server installed.
2. SCP the **webserversetup.tar** file to **/tmp/setup**.
3. Untar the **webserversetup.tar** file under **/tmp/setup**.
4. If the **setupWebServerEnv.sh** is not executable, make it executable **chmod 744 setupWebServerEnv.sh**.
5. Run **dos2unix setupWebServerEnv.sh**.
6. Run **./setupWebServerEnv**.
7. Open **/etc/httpd/conf.d/WebLogic.conf** and uncomment and update the following attributes:
8. **ServerName** – Name and port that the server uses to identify itself.
9. Uncomment the section **<IfModule mod\_WebLogic.c>** and update the following attributes:
10. **WebLogicCluster** – The IP Addresses of the WebLogic clusters hosting the ES Web application. For ES, the servers under ES Cluster1 host the ES Web application. The ES Cluster1 IP addresses can be found in the WebLogic config.xml (search for the string “ES Cluster1”). The config.xml resides under the **/opt/bea/ESDomain** directory in the admin WebLogic server for the ES application.
11. **ErrorPage** – URL where the ES Unavailable error page is located. This will physically reside under **/var/www/html/status** directory of the Web Server. So the path will be something like **http://** DNS.URL **/status/ESR\_Unavailable.html**
12. Confirm that the WebHelp directory created under /**var/www/html** has read permissions for the Apache Server. In the EDEV environment, it will need additional read and write access for the development group.
13. Once the steps are completed, point the load balancer to these Web Servers.
14. Copy /**u01/app/bea12/wlserver12.2/server/lib/linux/i686/mod\_wl\_20.so** from the WebLogic admin server to the **/etc/httpd/modules** directory of Apache Server.
15. In the **WebLogic.conf** file, ensure that the line specifying the module to load is **mod\_wl\_20.so instead of mod\_wl\_20.so-x86\_64.so**.

**Note:** The **setupWebServerEnv.sh** performs the following tasks:

* Copies the file **WebLogic.conf** under the **/etc/httpd/conf.d** directory.
* Creates a directory **/var/www/html/status** and sets permissions **chmod 755** on the status directory.
* Copies the files related to the ES Unavailable error page into this directory.
* Creates a directory called "**webhelp**" under **/var/www/html** on vaaacwbd4.

#### Installing WebHelp on the Web Servers

1. Login to the Linux server that has the Apache Web Server installed.
2. SCP webhelp.zip and deployWebhelp.sh to /tmp/webhelpArchive from VAAACMUL1O: pscp D:\CM\IP5\20070329\CO43354FY07\webhelp\* user@vaaacweb1s:/tmp/webhelpArchive/.
3. Set permissions: chmod –R 755 /tmp/webhelpArchive/.
4. Run Dos2Unix on deployWebhelp.sh: dos2unix /tmp/webhelpArchive/deployWebhelp.sh.
5. Deploy Webhelp from /tmp/webhelpArchive directory: **./deployWebhelp.sh webhelp.zip** (As root (sudo)).
6. Repeat steps 1-4 for all Web Servers in that environment.

#### Setting up the Enrollment and Eligibility Service (E&E) WebLogic Domain

The COs for the E&E Web Service deployment tasks are as follows:

* Stage 1B: R350242FY10
* PreProd: CO53836FY10
* Prod: CO53841FY10

Enrollment and Eligibility Service requires WebLogic 12.2 version. Separate application servers were created with WebLogic 12.2 for E&E service.

**Notes:**

* All the scripts are in **EEService\_Scripts.tar.gz**
* Default WebLogic user password used in these scripts is "WebLogic123"
* Change it to a new password while creating the domain.

1. Unzip the contents of the **EEService\_Scripts.tar.gz** into a directory on all application servers.
2. Run **dos2unix** command on all the contents of this file.
3. Set the following environment variables. **export BEA\_HOME=/u01/app/bea  
   export WL\_HOME=/u01/app/bea/wlserver\_12.2  
   export EEDOMAIN\_HOME=/home/WebLogic/bea/<DOMAINNAME>  
   The domain name has the format EES-<Environmentname> e.g., EES-DEV, EES-SQA, EES-PreProd, EES-Prod.**
4. Change directory to the appropriate folder [dev , sqa etc.].
5. Use this command in the desired directory to remove ^M chars in the UNIX scripts. It will clean up all the files in the selected directory. **[WebLogic@DNS dev]find . -type f -name '\*' | xargs dos2unix**
6. Open **CreateDomain.py** in vi and change the WebLogic user password and the password for the dbconnection pool.
7. Run script **CreateDomain.sh** and it creates the EES domain. **bash$./CreateDomain.sh**
8. Change directory to **$EEDOMAIN\_HOME/bin** and run this command to start the admin server. For example, **[WebLogic@DNS dev]./startWebLogic.sh**
9. Logon to the admin console to make sure all the servers/machines/clusters/pools are created.
10. Run this command on all the managed servers to enroll those machines to the managed server in the domain.  **[WebLogic@DNS dev]$ ./SetNodeManager.sh**
11. Run this command to start the node manager on all the servers. **[WebLogicDNS dev]$ ./StartNodeManager.sh**
12. Change directory to **$EEDOMAIN\_HOME** and create a directory "application".
13. Copy the war file **esr-ws.war** to the applications folder.
14. Change directory to the appropriate folder under scripts to deploy the war file using this command. **[WebLogic@DNS dev]$ ./Deploy.sh**
15. Start the managed servers in one of the following ways.
16. From the admin console.
17. Using the WebLogic provided scripts **under $EEDOMAIN\_HOME/bin  
    WebLogic@DNS dev]$ ./StartManagedServers.sh**
18. If you need to re-install the domain, follow these steps.
19. Stop all the servers including the node manager and admin server.
20. Delete all the files and folders from the domain home.
21. Delete all the files and folders from the node manager home.
22. Start over from step 1 above.

#### Setting up the Apache Web Server to Tunnel the Web Service Requests

The Apache Web Server will be used as a front end to address load balancing and failover requirements. The instructions below are related to setting up the Web Server to tunnel the Web Service requests to the application server.

1. Login to the Linux server that has the Apache Web Server installed.
2. Open **/etc/httpd/conf.d/WebLogic.conf** and add a new virtual host that is similar to ESR.

WebLogicCluster should have the comma separated list of EEServiceServer:PORTNumber

<VirtualHost DNS.URL:PORT>

ErrorLog logs/ssl\_error\_log

TransferLog logs/ssl\_access\_log

LogLevel warn

SSLEngine on

SSLProtocol TLSv1

SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt

#SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt

#SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key

#SSLCertificateChainFile /etc/httpd/conf/ssl.crt/va.pem

<Files ~ "\.(cgi|shtml|phtml|php3?)$">

SSLOptions +StdEnvVars

</Files>

<Directory "/var/www/cgi-bin">

SSLOptions +StdEnvVars

</Directory>

SetEnvIf User-Agent ".\*MSIE.\*" \

nokeepalive ssl-unclean-shutdown \

downgrade-1.0 force-response-1.0

CustomLog logs/ssl\_request\_log \

"%t %h %{SSL\_PROTOCOL}x %{SSL\_CIPHER}x \"%r\" %b"

<IfModule mod\_WebLogic.c>

# WebLogicCluster 10.224.88.120:8101

WebLogicCluster DNS.URL:PORT

MatchExpression /esr-ws

</IfModule>

</VirtualHost>

1. Restart the Apache Server.

#### Setting Up TLS Authentication in E&E Servers

ES interface to VADIR Web Service, also called Enterprise Military Information Service-eMIS, uses Mutual Transport Layer Security (TLS) Authentication with VA issued certificates to identify and authorize server-to-server communications. TLS also provides the message’s confidentiality and integrity between the endpoints. For additional details, refer to ES eMIS interface control document. (Refer to Figure 5)

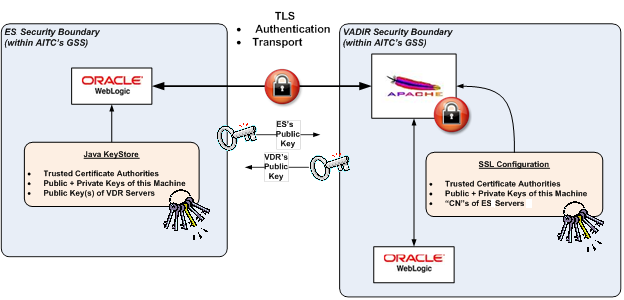


Figure : ES-VADIR Security Boundary

#### Steps for VHAESRAPP45 Server

Prerequisites: Need to have VA.pem, DNS.URL.pem, DNS.URL pem in /u01/cert/

STEP 1  
navigate to /u01/app/bea/wlserver\_12.2/server/lib/

STEP 2  
keytool -import -alias VA\_internal\_root\_CA -file /u01/cert/va.pem -keystore /u01/app/bea/wlserver\_12.2/server/lib/vacertstore.jks -storepass PASSWORD1

STEP 3  
keytool -import -alias DNS.URL -file /u01/cert/DNS.URL.pem -keystore /u01/app/bea/wlserver\_10.3/server/lib/vacertstore.jks -storepass PASSWORD1

STEP 4  
keytool -list -keystore vacertstore.jks -v (when prompted for password specify the PASSWORD1 from above)  
(Should come back with 2 entries - alias VA\_internal\_root\_CA and DNS.URL )

STEP 5  
java -classpath WebLogic.jar utils.ImportPrivateKey -keystore /u01/app/bea/wlserver\_12.2/server/lib/appcertstore.jks -storepass PASSWORD2 -storetype jks -keypass PASSWORD2 –DNS.URL -certfile /u01/cert/DNS.URLpem -keyfile /u01/cert/ DNS.URL.key -keyfilepass PASSWORD2

**Note**: The PASSWORD2 specified in STEP 5 should exactly match the password to open the certificate key file.

STEP 6  
keytool -list -keystore appcertstore.jks -v (when prompted for password use PASSWORD2)  
(Should come back with 1 entry – DNS.URL)

STEP 7

cd/u01/cert  
openssl verify -CAfile va.pem DNS.URL.pem  
(Check if the result is DNS.URL.pem: OK)

#### Steps for VHAESRAPP46 Server

Prerequisites: Need to have VA.pem, DNS.URL.pem, DNS.URL.pem in /u01/cert/

STEP 1  
navigate to /u01/app/bea/wlserver\_12.2/server/lib/

STEP 2  
keytool -import -alias VA\_internal\_root\_CA -file /u01/cert/va.pem -keystore /u01/app/bea/wlserver\_12.2/server/lib/vacertstore.jks -storepass PASSWORD1

STEP 3  
keytool -import - DNS.URL -file /u01/cert/ DNS.URL.pem -keystore /u01/app/bea/wlserver\_12.2/server/lib/vacertstore.jks -storepass PASSWORD1

STEP 4  
keytool -list -keystore vacertstore.jks -v (when prompted for password specify the PASSWORD1 from above)  
(Should come back with 2 entries - alias VA\_internal\_root\_CA and DNS.URL)

STEP 5  
java -classpath WebLogic.jar utils.ImportPrivateKey -keystore /u01/app/bea/wlserver\_12.2/server/lib/appcertstore.jks -storepass PASSWORD2 -storetype jks -keypass PASSWORD2 – DNS.URL -certfile /u01/cert/ DNS.URL.pem -keyfile /u01/cert/ DNS.URL.key -keyfilepass PASSWORD2

**Note**: The PASSWORD2 specified in STEP5 should exactly match the password to open the certificate key file.

STEP 6  
keytool -list -keystore appcertstore.jks -v (when prompted for password use PASSWORD2)  
(Should come back with 1 entry - DNS.URL)

STEP 7  
cd /u01/cert  
openssl verify -CAfile va.pem DNS.URL.pem  
(Check if the result is DNS.URL OK)

#### Log On to WebLogic Administration Console for VHAEES\_PROD

Repeat the steps below for EES-MS1 and EES-MS2.

1. Navigate to Environment->Servers-->[EES-MS1]-->Configuration-->Keystores.
2. Set Keystores to “Custom Identity and Custom Trust”.
3. In the Identity section set:
4. **Custom Identity Keystore** to the /u01/app/bea/wlserver\_12.2/server/lib/appcertstore.jks
5. **Custom Identity Keystore Type** to jks
6. **Custom Identity Keystore Passphrase** to PASSWORD 2
7. In the Trust section set:
8. **Custom Trust Keystore** to the file /u01/app/bea/wlserver\_12.2/server/lib/vacertstore.jks
9. **Customer Keystore Type** to jks
10. **Customer Trust Keystore Passphrase** to PASSOWORD1
11. Click Save.
12. Navigate to the SSL tab.
13. Set Identity and Trust Locations to “Keystores”.
14. In the Identity section set:
15. **Private Key Alias** to the alias DNS.URL
16. **Private Key Passphrase** to PASSWORD2
17. Click on Advanced and set:
18. **Hostname Verification** to “None”.
19. **Custom Hostname Verifier** to blank.
20. **Export Key Lifespan** unchanged.
21. **Use Server Certs** to checked.
22. **Two Way Client Cert Behavior** to “Client Certs Not Requested”.
23. **Cert Authenticator** to blank.
24. Click Save.
25. Under SERVER START, ARGUMENTS add the following.

* Djavax.net.ssl.trustStore=/u01/app/bea/wlserver\_12.2/server/lib/vacertstore.jks
* Djavax.net.ssl.trustStorePassword=PASSWORD1
* Djavax.net.ssl.keyStore=/u01/app/bea/wlserver\_12.2/server/lib/appcertstore.jks
* Djavax.net.ssl.keyStorePassword=PASSWORD2

**Note:** It is better to cut and paste the current content from ARGUMENTS field and add these two and paste the whole thing back.

#### Setting up JMS Queues in E&E Servers

Java Messaging Service (JMS) Queues are installed in E&E servers to facilitate communication between ES and MSDS Web Service delegate in E&E servers.

The JMS configuration is shown in Figure 6 and Figure 7.

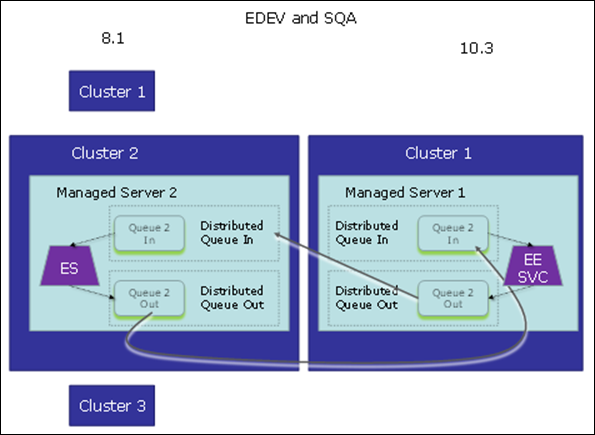


Figure : JMS Configuration – EDEV and SQA

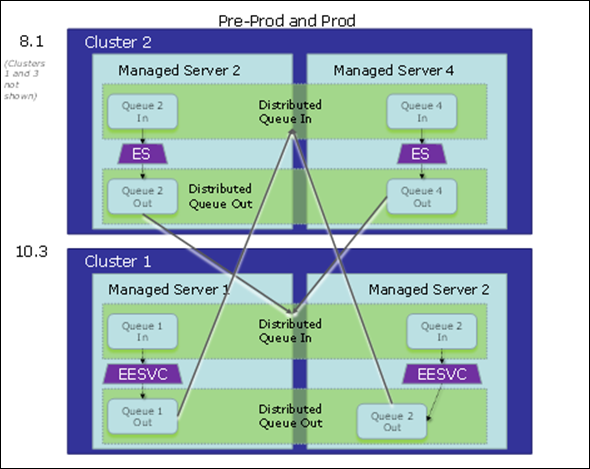


Figure : JMS Configuration – Pre-Prod and Prod

## Database Tuning

Database Tuning does not apply. ES is supported by the Administrative Data Repository (ADR).

# Back-out Procedure

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings.

## Back-out Strategy

Back-out to ES 5.1 will be required in the event ES 5.2 is determined to be unsuccessful. The following are examples of reasons that would warrant a back-out.

* An error was encountered during the implementation preventing the system from functioning as required.
* Messaging performance is not within tolerance.
* UI performance is below standard.
* Messaging errors encountered.

## Back-out Considerations

Certain milestones must be met in order to continue with the deployment. If any of the following conditions occur, the decision owners will be contacted, and a go or no-go decision to proceed will be made.

* Any step in the deployment timeline is exceeded by 50% or 60 minutes, whichever comes first.
* Accumulated delay in the deployment timeline of more than 2 hours requires approval to continue.
* Accumulated delay in the deployment timeline of more than 4 hours requires a conference call to evaluate cause; will only continue if cause is eliminated, and full operation can complete in an acceptable timeframe.
* A further delay of 60 minutes is cause for automatic roll back to previous version.
* Post deployment issues including, but not limited to, the following will require approval of decision owners to continue:

1. Smoke test fails.
2. Person Service Identity Management (PSIM)/Master Veteran Index (MVI) not available upon restart and cannot be engaged.
3. Message traffic yields an increase in errors of 1% or more.
4. Message throughput after 30 minutes is not commensurate with load.
5. At peak load, inbound Z07 processing should exceed 250 messages/minute on average. Outbound Z11s should exceed 750 messages/minute, and should be greater than the average number of Z07s processed.
6. Veterans Benefit Administration (VBA) messages/connectivity is not available.
7. Introscope monitors indicate unresolvable failures in any cluster.

* Income Verification Match (IVM) is unable to connect to and retrieve data from ES through the Bi-directional Interface.

### Load Testing

No load testing is included in the ES 5.2 deployment.

### User Acceptance Testing

When the results of the User Acceptance Testing are complete, it is documented by the Chief Business Office (CBO) in the ES 5.2 Testing Analysis Report (TAR); the report is located in Rational Team Concert.

This testing includes:

* Verification and validation of the ES changes
* User Functional Testing (UFT)

## Back-out Criteria

Refer to Section 5.2 Back-out Considerations.

## Back-out Risks

* If ES 5.1 is *not* cleanly restored, then messaging and/or functional operations may be impacted.
* If ES 5.2 is *not* the root cause of the conditions requiring back-out, then those conditions may persist upon restoration of ES 5.1.
* If ES 5.2 is fully backed out, then needed functionality will be delayed to Production.

## Authority for Back-out

Table 8 lists the resources with the authority to authorize a back-out.

Table : Resources with the Authority to Authorize a Back-out

| First Name | Last Name | Organization |
| --- | --- | --- |
| Ralph | Weishaar | Director for Internal Control |
| Delwin C. | Johnson | OIT Enterprise Health Benefits Determination (EHBD) PM |
| Jim | Steele | Austin Information Technology Center (AITC) Operations, Division Chief |

## Back-out Procedure

If a decision to back-out is made, the following step is required:   
Roll back to the previous version, ES 5.1.

## Back-out Verification Procedure

No back-out verification procedure is required for ES 5.2.

# Rollback Procedure

The Rollback procedure for 5.2 is to redeploy the previous 5.1 ear file.

## Rollback Considerations

Because all database actions in ES are transaction based, any error during a data persistence operation will be automatically rolled back by the system and an error logged in the application error log. The state of the database is returned to the last commit point using the Oracle ROLLBACK transaction statement, and no further database maintenance is required.

## Rollback Criteria

There are no rollback criteria for ES 5.2.

## Rollback Risks

There are no rollback risks for ES 5.2.

## Authority for Rollback

Refer to Table 8: Resources with the Authority to Authorize a Back-out.

## Rollback Verification Procedure

The verification steps are identical as above to verify redeployment of the previous version after back-out of ES 5.2 and roll back and redeployment of ES 5.1.