Pharmacy Reengineering (PRE) Inbound ePrescribing (eRx) 3.1

Deployment, Installation, Rollback, and Back-Out Guide

May 2019
Department of Veterans Affairs
Office of Information and Technology (OI&T)
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/07/2019</td>
<td>2.5</td>
<td>Updates for changes with 3.1.0.004 reference: pg 127, 132, 145, 146, and 150</td>
<td>Technatomy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Title page to month of March</td>
<td></td>
</tr>
<tr>
<td>03/11/2019</td>
<td>2.4</td>
<td>Updates for changes with 3.1.0.003 reference: pg 127, 132, 145, 146, and 150</td>
<td>Technatomy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Title page to month of February</td>
<td></td>
</tr>
<tr>
<td>10/29/2018</td>
<td>2.3</td>
<td>Update Title page to month of November</td>
<td>Technatomy</td>
</tr>
<tr>
<td>10/24/2018</td>
<td>2.2</td>
<td>Updates for changes with 3.0.5.008 reference: pg 132</td>
<td>Technatomy</td>
</tr>
<tr>
<td>09/21/2018</td>
<td>2.1</td>
<td>Updated to address VIP RA Comments Sections: 5.6.1, 5.7.1, 6.5.2, 6.5.2.1</td>
<td>Technatomy</td>
</tr>
<tr>
<td>09/19/2018</td>
<td>2.0</td>
<td>Updates for changes with 3.0.5.005.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>07/26/2017</td>
<td>0.93</td>
<td>Updates for changes with 2.0.4.057.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>07/20/2017</td>
<td>0.92</td>
<td>Updates for changes with 2.0.4.057.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>06/27/2017</td>
<td>0.91</td>
<td>Updates for changes with 2.0.4.054.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>05/22/2017</td>
<td>0.8</td>
<td>Updates for changes with 2.0.4.048.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>05/10/2017</td>
<td>0.7</td>
<td>Updates for changes with 2.0.3.047.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>04/25/2017</td>
<td>0.6</td>
<td>Updates with corrected information for Staging, PreProd and Production.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>04/12/2017</td>
<td>0.5</td>
<td>Updates with corrected information for Staging, PreProd and Production.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>02/15/2017</td>
<td>0.4</td>
<td>Updates with corrected information for Staging, PreProd and Production. New sections for SSOi.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>02/07/2017</td>
<td>0.3</td>
<td>Multiple updates with new steps introduced throughout Build 1, cleanup for Staging, PreProd and Production.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>11/10/2016</td>
<td>0.2</td>
<td>Sprint Update – Added draft steps for rolling back Weblogic; added the VistA Patch #; added a placeholder for backing out the database.</td>
<td>Technatomy</td>
</tr>
<tr>
<td>10/27/2016</td>
<td>0.1</td>
<td>Initial Draft (Template Version 2.2 March 2016)</td>
<td>Technatomy</td>
</tr>
</tbody>
</table>
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

1.1 Purpose .................................................................................................................. 1
1.2 Dependencies .......................................................................................................... 1
1.3 Constraints ............................................................................................................. 2

2. Roles and Responsibilities ......................................................................................... 3

3. Deployment .............................................................................................................. 4

3.1 Timeline .................................................................................................................. 4

3.2 Site Readiness Assessment ...................................................................................... 4

3.2.2 Deployment Topology (Targeted Architecture) .................................................... 7
3.2.3 Site Information (Locations, Deployment Recipients) ........................................ 7
3.2.4 Site Preparation .................................................................................................. 7

3.3 Resources ............................................................................................................... 7

3.3.1 Facility Specifics ................................................................................................ 7
3.3.2 Hardware ........................................................................................................... 8
3.3.3 Software ............................................................................................................ 8
3.3.4 Communications ............................................................................................... 8

3.3.4.1 Deployment/Installation/Back-Out Checklist .................................................... 9

4. Installation ............................................................................................................... 9

4.1 Pre-installation and System Requirements ............................................................ 9

4.1.1 Pre-requisites .................................................................................................... 9
4.1.2 Environment Configurations ............................................................................ 11

4.2 Platform Installation and Preparation ................................................................... 18

4.2.1 Modify /etc/hosts entry .................................................................................... 18
4.2.2 X Windows ........................................................................................................ 18
4.2.3 Setup Administration Accounts ....................................................................... 18
4.2.4 Install Java ......................................................................................................... 20
4.2.5 Apache Installation on VM1 and VM2 ............................................................... 20
4.2.6 Apache Configuration on VM1 and VM2 ......................................................... 21
4.2.7 Certificate Configuration ................................................................................... 23
4.2.8 Create NSS certificate database on VM1 ......................................................... 28
4.2.9 Create NSS certificate database on VM2 ......................................................... 29
4.2.10 NSS Configuration on VM1 .......................................................................... 30
4.2.11 NSS Configuration on VM2 ........................................................................... 31
4.2.12 Configure Apache Plug-in for WebLogic on VM1 ......................................... 33
4.2.13 Configure Apache Plug-in for WebLogic on VM2 ......................................... 34
4.2.14 Create IEP CPanel on VM1 and VM2 ............................................................ 34
4.2.15 Install Apache SSOi Web Agent on VM1 ....................................................... 35
4.2.16 Configure Apache SSOi Web Agent on VM1 .................................................. 36
4.2.17 Post Configure Edits for Apache SSOi Web Agent on VM1 ........................................... 39
4.3 Download and Extract Files ................................................................................................. 41
4.4 Database Creation ................................................................................................................ 41
4.5 Installation Scripts .............................................................................................................. 41
4.6 Cron Scripts ......................................................................................................................... 41
4.7 Access Requirements and Skills Needed for the Installation ............................................. 42
4.8 Installation Procedure ......................................................................................................... 42

4.8.1 WebLogic Installation ...................................................................................................... 42
    4.8.1.1 Install WebLogic ........................................................................................................ 42
    4.8.1.2 Set Temporary Environment on VM1 ................................................................... 62
    4.8.1.3 Create a Domain Boot Identity File on VM1 .......................................................... 62
    4.8.1.4 Copy Identity/Trust Store Files on VM1 ................................................................ 62
    4.8.1.5 Configure nodemanager Identity/Trust Store on VM1 ........................................... 62
    4.8.1.6 Configure TLS on VM1 ............................................................................................. 62
    4.8.1.7 Copy Identity/Trust Store Files on VM2 ................................................................ 62
    4.8.1.8 Configure nodemanager Identity/Trust Store on VM2 ........................................... 63
    4.8.1.9 Disable basic authentication ...................................................................................... 63
    4.8.1.10 Configure JPA for Domain on VM1 .................................................................... 63
    4.8.1.11 Create Inbound eRx Datasource ......................................................................... 64
    4.8.1.12 Configure Identity/Trust Store File on Managed Servers .................................... 72
    4.8.1.13 Pack Domain on VM1 ............................................................................................. 79
    4.8.1.14 Unpack Domain on VM2 ......................................................................................... 79
    4.8.1.15 Copy Identity/Trust Store Files on VM2 ................................................................ 79
    4.8.1.16 Enroll VM2 ............................................................................................................. 79
    4.8.1.17 Check Node Manager on Each WebLogic Machine ............................................... 80
    4.8.1.18 Create a Boot Identity File for Managed Servers .................................................... 80
    4.8.1.19 Deploy Test Application ........................................................................................... 80
    4.8.1.20 Configure JPA for Domain on VM2 .................................................................... 89
    4.8.1.21 Install VistAlink on VM1 ......................................................................................... 89
    4.8.1.22 Configure VistAlink on VM1 ................................................................................... 90
    4.8.1.23 Install VistAlink on VM2 ......................................................................................... 90
    4.8.1.24 Configure VistAlink on VM2 ................................................................................... 91
    4.8.1.25 Stop and start Node Manager and Domain on VM1, VM2 .................................... 91
    4.8.1.26 Deploy VistAlink Libraries ..................................................................................... 92
    4.8.1.27 Deploy VistAlink Adapters ..................................................................................... 117

4.8.2 Inbound eRx Application Installation ............................................................................... 123
    4.8.2.1 Install Inbound eRx Application ............................................................................... 123
    4.8.2.2 Create Startup/Shutdown Scripts ............................................................................. 138
    4.8.2.3 Shut Down Domain .................................................................................................. 139
    4.8.2.4 Shut Down Nodemanagers ...................................................................................... 139

4.8.3 Pentaho Installation ......................................................................................................... 140
    4.8.3.1 Pentaho Software Installation .................................................................................. 140
    4.8.3.2 Pentaho Repository Definition Import ...................................................................... 142

4.8.4 Nexus Repository Installation (DEV2 VM1 Only) .......................................................... 143
    4.8.4.1 SonaType Nexus Software Installation .................................................................... 143

4.8.5 VistA Patch Installation .................................................................................................. 144

4.9 Installation Verification Procedure ....................................................................................... 144
5. Back-Out Procedure ........................................................................ 144
   5.1 Back-Out Strategy .................................................................... 144
   5.2 Back-Out Considerations ......................................................... 144
      5.2.1 Load Testing ...................................................................... 145
      5.2.2 User Acceptance Testing ................................................... 145
   5.3 Back-Out Criteria ..................................................................... 145
   5.4 Back-Out Risks ........................................................................ 145
   5.5 Authority for Back-Out .............................................................. 145
   5.6 Back-Out Procedure ................................................................. 145
      5.6.1 Back-Out of VistA Patch ...................................................... 145
      5.6.2 Back-Out of Inbound eRx Application Installation ............. 146
      5.6.3 Back-Out of WebLogic Application Installation ................. 146
      5.6.4 Back-out of Pentaho Installation .................. Error! Bookmark not defined.
      5.6.5 Back-out Database ............................................................. Error! Bookmark not defined.
   5.7 Back-out Verification Procedure ............................................... 149
      5.7.1 Verify VistA Patch Back-Out .............................................. Error! Bookmark not defined.
      5.7.2 Verify VistA Link Back-Out .............................................. Error! Bookmark not defined.
      5.7.3 Verify WebLogic Back-Out .............................................. Error! Bookmark not defined.
      5.7.4 Verify Pentaho Back-Out ............................................... Error! Bookmark not defined.

6. Rollback Procedure ...................................................................... 149
   6.1 Rollback Considerations .......................................................... 149
   6.2 Rollback Criteria ..................................................................... 149
   6.3 Rollback Risks ......................................................................... 149
   6.4 Authority for Rollback ............................................................... 149
   6.5 Rollback Procedure ................................................................. 150
      6.5.1 Rollback WebLogic ............................................................ 150
         6.5.1.1 Remove Old Release .................................................... 150
         6.5.1.2 Deploy Rolled-Back Release ........................................ 151
      6.5.2 Rollback VistA Patch ........................................................ 153
         6.5.2.1 Validation of Roll Back Procedure .............................. 153
   6.6 Rollback Verification Procedure ............................................... 153

7. Operational Procedures ................................................................ 153
   7.1 Startup Procedures .................................................................... 153
      7.1.1 Start Weblogic Node Managers and Admin Console ........ 153
      7.1.2 Managed Servers ................................................................ 154
      7.1.3 Pentaho Services Startup .................................................. 154
   7.2 Shut Down Procedures .............................................................. 155
7.2.1 Pentaho Services Shutdown................................................................. 155
7.2.2 WebLogic Application Server Shutdown............................................ 155

8. Appendices ............................................................................................. 156

8.1 Certificate Contents ............................................................................ 156
8.1.1 va_root_ca_cert.txt............................................................................ 156
8.1.2 va_internal_subordinate_ca_cert.txt.................................................. 157
8.1.3 va_root_ca_s2_cert.pem...................................................................... 157
8.1.4 va_internal_ca1_s2_cert.pem............................................................... 158
8.1.5 va_internal_ca2_s2_cert.pem............................................................... 158
8.1.6 betrusted_production_ssp_ca_a1_cert.txt............................................ 159
8.1.7 federal_common_policy_ca_cert.txt.................................................... 159
8.1.8 veterans_affairs_device_ca_b2_cert.txt............................................. 160
8.1.9 vaww.esrdev.aac.va.gov_cert.txt......................................................... 161
8.1.10 vaww.esrstage1a.aac.va.gov.pem...................................................... 162
8.1.11 vaww.esrstage1b.aac.va.gov.pem...................................................... 162
8.1.12 vaww.esrpre-prod.aac.va.gov.pem.................................................... 163
8.1.13 das-test.va.gov.pem........................................................................... 164
8.1.14 das-sqa.va.gov.pem.......................................................................... 165
8.1.15 das.va.gov.pem............................................................................... 166
## Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Inbound eRx Application Context Diagram</td>
</tr>
<tr>
<td>Figure 2</td>
<td>High-Level eRx Architecture</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Install WebLogic – Oracle Fusion Middleware Installation Inventory Setup</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Install WebLogic – Oracle Universal Installer Dialog Box</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Install WebLogic – Oracle Fusion Middleware WebLogic Server and Coherence Installer Screen</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Install WebLogic – Installation Location</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Install WebLogic – Installation Type</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Install WebLogic – Prerequisite Checks</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Install WebLogic – Security Updates Screen</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Install WebLogic – My Oracle Support Username/Email Address Not Specified Dialog Box</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Install WebLogic – Installation Summary Screen</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Install WebLogic – Installation Progress Screen</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Install WebLogic – Installation Complete</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Install WebLogic – Oracle Configuration Wizard Splash Screen</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Install WebLogic – Create New Domain</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Install WebLogic – Templates Screen</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Install WebLogic – Administrator Account Screen</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Install WebLogic - Domain Mode and JDK</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Install WebLogic – Advanced Configuration</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Install WebLogic – Administration Server Screen</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Install WebLogic – Node Manager</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Install WebLogic – Managed Servers</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Install WebLogic – Clusters</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Install WebLogic – Assign Servers to Clusters</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Install WebLogic – Machines</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Install WebLogic – Assign Servers to Machines</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Install WebLogic – Configuration Summary Screen</td>
</tr>
<tr>
<td>Figure 28</td>
<td>Install WebLogic - Configuration Success</td>
</tr>
<tr>
<td>Figure 29</td>
<td>Create Inbound eRx Datasource – Datasources</td>
</tr>
<tr>
<td>Figure 30</td>
<td>Create Inbound eRx Datasource – Datasource Properties</td>
</tr>
<tr>
<td>Figure 31</td>
<td>Create Inbound eRx Datasource – Database Driver</td>
</tr>
<tr>
<td>Figure 32</td>
<td>Create Inbound eRx Datasource – Transaction Properties</td>
</tr>
<tr>
<td>Figure 33</td>
<td>Create Inbound eRx Datasource – Connection Properties</td>
</tr>
<tr>
<td>Figure 34</td>
<td>Create Inbound eRx Datasource – Test Connection</td>
</tr>
<tr>
<td>Figure 35</td>
<td>Create Inbound eRx Datasource – Select Targets/Finish</td>
</tr>
<tr>
<td>Figure 36</td>
<td>Create Inbound eRx Datasource – Modify New Datasource</td>
</tr>
<tr>
<td>Figure 37</td>
<td>Inbound eRx Datasource –Connection Pool Properties</td>
</tr>
<tr>
<td>Figure 38</td>
<td>Inbound eRx Datasource –Connection Pool Advanced Properties</td>
</tr>
<tr>
<td>Figure 39</td>
<td>Inbound eRx Datasource – Wrap Data Type Property</td>
</tr>
<tr>
<td>Figure 40</td>
<td>Inbound eRx Datasource – Save Properties</td>
</tr>
<tr>
<td>Figure 41</td>
<td>Configure Identity/Trust Store File – Access Server Configuration Page</td>
</tr>
<tr>
<td>Figure 42</td>
<td>Configure Identity/Trust Store File – Change Keystores</td>
</tr>
<tr>
<td>Figure 43</td>
<td>Configure Identity/Trust Store File – Keystores – Select Custom Identity and Custom Trust</td>
</tr>
<tr>
<td>Figure 44</td>
<td>Configure Identity/Trust Store File – Modify Keystore Settings</td>
</tr>
<tr>
<td>Figure 45</td>
<td>Configure Identity/Trust Store File – Modify SSL Settings</td>
</tr>
</tbody>
</table>
Figure 94: Install Inbound eRx Application – Verify Server Settings ........................................ 124
Figure 95: Install Inbound eRx Application – Verify General & Keystore Settings ...................... 125
Figure 96: Install Inbound eRx Application – Verify SSL Settings ........................................ 126
Figure 97: Install Inbound eRx Application – Summary of Deployments .................................. 127
Figure 98: Install Inbound eRx Application – Install New Deployment of INB_ERX .................... 127
Figure 99: Install Inbound eRx Application – Select INB_ERX Deployment Targets ...................... 128
Figure 100: Install Inbound eRx Application – Verify INB_ERX Deployment Settings .................. 129
Figure 101: Install Inbound eRx Application – Verify INB_ERX Deployment Settings (Finish) ........ 130
Figure 102: Install Inbound eRx Application – Verify INB_ERX Deployment Configuration Settings ... 131
Figure 103: Install Inbound eRx Application – Install New Deployment of INB_ERX_UI .................. 132
Figure 104: Install Inbound eRx Application – Select INB_ERX_UI Deployment Targets .............. 133
Figure 105: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings ............... 134
Figure 106: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings (Finish) ..... 135
Figure 107: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Configuration Settings 136
Figure 108: Install Inbound eRx Application – Start erx Servers ........................................... 137
Figure 109: Install Inbound eRx Application – erx Servers Running ......................................... 138

List of Tables

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities 3
Table 2: Deployment Timeline 4
Table 3: Site Preparation 7
Table 4: Software Specifications 8
Table 5: Deployment/Installation/Back-Out Checklist 9
Table 6: Development/SQA Detailed VM Requirements 9
Table 7: Staging Detailed VM Requirements 10
Table 8: Pre-Production Detailed VM Requirements 10
Table 9: Production Detailed VM Requirements 10
Table 10: Environment Variables 11
Table 11: Symbolic Names by Environment 12
Table 12: Symbolic Names by Environment (cont) 12
Table 13: Symbolic Names by Environment (cont) 13
Table 14: Symbolic Names by Environment (cont) 14
Table 15: Symbolic Names by Environment (cont) 15
Table 16: Symbolic Names by Environment (cont) 16
Table 17: Symbolic Names for sensitive items 17
1. Introduction

This document describes how to deploy and install the various components of the software for the Pharmacy Reengineering (PRE) Inbound ePrescribing (eRx) project, as well as how to back-out the product and rollback 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 Guide may be used, but the Back-Out Recovery strategy still needs to be included in this document. Veterans Health Administration (VHA), Patient Care Services (PCS) and Pharmacy Benefits Management (PBM) has requested a new capability as part of the PRE program to receive inbound electronic prescriptions (e-prescriptions or eRxs) from an external provider (e.g., a doctor not associated with the Department of Veterans Affairs [VA], medical staff at a Department of Defense [DoD] military treatment facility, etc.). They also seek to have the ability to transfer prescriptions electronically between pharmacies, both VA to VA, as well as VA to non-VA (ideally). Once received, these prescriptions will then be fed into the existing Veterans Health Information Systems and Technology Architecture (VistA) Outpatient Pharmacy (OP) for processing and dispensing.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the PRE Inbound eRx application 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

Figure 2 depicts the Inbound eRx application and the external systems that it interacts with, including the following: Change Healthcare, Master Veteran Index (MVI), Eligibility & Enrollment (E&E), Health Data Repository (HDR), and VistA OP.

Figure 1: Inbound eRx Application Context Diagram
1.3 Constraints

Design constraints that pertain to the PRE Inbound eRx implementation include the following:

- Existing interfaces will be implemented with the least possible change in order to support existing client system implementations. However, it is recognized that in some circumstances, a change to the interface may be necessary in order to support PRE Inbound eRx requirements or to accommodate technology or frameworks used for PRE Inbound eRx development. One key change is the need for service consumers to maintain the session state and provide this to PRE Inbound eRx on each call. This change is necessary to provide stateless services, as required by the VA Service-Oriented Architecture (SOA).
- The Java language and Java Enterprise Edition (JEE) platform will be used to develop the PRE Inbound eRx.
- Security policies and mechanisms for SOA middleware are currently being developed and updated. The timeframes for the production ready versions may not coincide with the PRE Inbound eRx effort. This includes solutions to the VistA anonymous login and authorization/authentication for the middleware running on non-VistA platforms as part of the enterprise SOA architecture.
- The application user interfaces (UI) must follow enterprise common UI templates and style guidelines.
- Application user interfaces must comply with Section 508.
- The application must comply with VA Enterprise Architecture published data standards (HL7, National Council for Prescription Drug Programs [NCPDP]).
- Inbound eRx must identify and leverage authoritative information sources for data retrieval and manipulation.
- The application must operate optimally using information from the authoritative source or receive permission for caching data locally.
- The team must configure system and server platforms used by the application using standard system images published in the current VA Release Architecture.
- The team must publish relational and object oriented databases utilized by the solution in the current VA Release Architecture.
- The team must base application production capacity requirements on workload analysis, simulated workload benchmark tests, or application performance models.
- The team must base application storage capacity requirements on detailed capacity analysis and/or models.
- The team must design the solution to operate within the current VA Local Area Network (LAN) and Wide Area Network (WAN) network configurations.
- The deployment environment must meet the performance and downtime monitoring requirements of the solution.
- The team and data center must develop and provision a disaster recovery plan.
- All critical infrastructure components (including data) must be located at multiple physical locations.
• The application backup and restore solution must meet data recovery requirements [Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO)].
• The application UIs must exist as browser based UIs and roll and scroll in VistA.
• The application must establish secure access paths for accessing the application and application data.
• The solution must document specific reasons for all limited, external access to data, including the need to know along with security, privacy and other legal restrictions.
• The solution must implement appropriate controls that prevent unwarranted disclosure of sensitive, Personally Identifiable Information (PII), or Protected Health Information (PHI).
• The team must base all system interfaces (both external and internal) implemented by the solution on open standards such as SOAP, REST, JMS, MQ, HTTPS and standard message formats such as HL7 and NCPDP.
• The solution must access available enterprise information through services.
• The VA TRM must identify all products and standards used by this solution as permissible for usage.

2. Roles and Responsibilities
This section outlines the roles and responsibilities for managing the deployment of the PRE Inbound eRx system.

| ID | Team                        | Phase / Role | Tasks                                                                                          | Project Phase (See Schedule) |
|----|-----------------------------|--------------|------------------------------------------------------------------------------------------------|
| 1  | FO, EO, NDCP or Product Development (depending upon project ownership) | Deployment   | Plan and schedule deployment (including orchestration with vendors).                           | Deployment                   |
| 2  | FO, EO, NDCP or Product Development (depending upon project ownership) | Deployment   | Determine and document the roles and responsibilities of those involved in the deployment.    | Design/Build                 |
| 3  | FO, EO, or NDCP             | Deployment   | Test for operational readiness.                                                                | Design/Build                 |
| 4  | FO, EO, or NDCP             | Deployment   | Execute deployment.                                                                            | Design/Build                 |
| 5  | FO, EO, or NDCP             | Installation | Plan and schedule installation.                                                                | Deployment                   |
| 6  | Regional PM/ Field Implementation Services (FIS)/ Office of Policy and Planning (OPP) PM | Installation | Ensure authority to operate and that certificate authority security documentation is in place. | Design/Build                 |
3. **Deployment**

The deployment is planned as a phased rollout. This type of rollout is best suited for the rapid turnaround time and repeat nature of the installations required for this project.

### 3.1 Timeline

The deployment and installation is scheduled to run for 18 months as depicted in the master deployment schedule. The timelines are depicted in the Deployment Timeline table below.

<table>
<thead>
<tr>
<th>VIP Build</th>
<th>Delivery Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP Build 1 Transaction Hub Version 1.0 Foundation</td>
<td>07/28/2016-10/31/2016</td>
</tr>
<tr>
<td>VIP Build 2 Transaction Hub Version 1.0 Complete eRx Transaction Hub</td>
<td>10/31/2016-01/27/2017</td>
</tr>
<tr>
<td>VIP Builds 3 &amp; 4 Inbound Electronic Prescriptions Version 2.0 Complete Inbound eRx Transaction Processing, UAT, IOC, CD-2</td>
<td>01/28/2017-07/27/2017</td>
</tr>
<tr>
<td>VIP Build 5 National Deployment Version 2.0 (includes 1.0 and 2.0)</td>
<td>07/28/2017-11/27/2017</td>
</tr>
<tr>
<td>VIP Build 1 &amp; 2 (New CD1) Transfer to/from VA Pharmacy Development Increment for Version 3 eRx Transfers plus other features development, UAT, IOC, CD-2</td>
<td>07/28/2017-01/27/2018</td>
</tr>
<tr>
<td>VIP Build 3 National Deployment Version 3 NationalDeployment of Version 3.0 (4 months total)</td>
<td>03/04/2018-06/01/2018</td>
</tr>
</tbody>
</table>

### 3.2 Site Readiness Assessment

This section discusses the locations that will receive the PRE Inbound eRx application deployment. Topology determinations are made by Enterprise Systems Engineering (ESE) and vetted by Field Operations (FO), National Data Center Program (NDCP), and AITC during the
design phase as appropriate. Field site coordination is done by FO unless otherwise stipulated by FO.

The product will be released by the PRE Inbound eRx Configuration Manager to the AITC Build Manager via a Change Order. The AITC Build Manager will follow the installation steps in Section 4 to complete the product’s activation at AITC and for the Disaster Recovery server. The Implementation Manager has assured site readiness by assessing the readiness of the receiving site to deploy the product. AITC, under contract, will provide the product dependencies, power, equipment, space, manpower, etc., to ensure the successful activation of this product.

### 3.2.1 Application Architecture

The following diagram represents the high-level architecture for the eRx application.
Figure 2: High-Level eRx Architecture

Inbound eRx Topology

Protocols
- HTTP
- HTTPS
- SQL Net
- VistA Link
- Undefined
- JMS
- VPN

Boundaries
- Process
- SW Product
- Enclave
- Server

Inbound eRx Deployment, Installation, Back-Out & Roll Back Guide

May 2019
3.2.2 **Deployment Topology (Targeted Architecture)**

This product will be released to AITC. The AITC, under contract, will house and secure this product on its Pre-Production and then Production servers. A few field located super users will be given access upon National Release. The PRE Inbound eRx system will be available to VA users on a continuous basis (excluding scheduled maintenance activities). Clustering at the application and web services servers will provide high availability and failover capabilities at the application tier and presentation tier. The servers will be load-balanced to distribute uniform processing across all servers.

Additionally, a VistA patch will be released to all VistA sites.

3.2.3 **Site Information (Locations, Deployment Recipients)**

AITC will host the web and application servers for the PRE Inbound eRx system. Initial Operating Capability (IOC) will occur in September of 2018. IOC sites are:

- Brooklyn, NY VA Medical Center (VAMC)
- Fayetteville VAMC Veterans Health Care System of the Ozarks
- Health Administration Center (Meds by Mail)
- Indianapolis, IN VA Medical Center

3.2.4 **Site Preparation**

No preparation is required for the individual VistA sites installing the VistA patch or using the Inbound eRx application.

The following table describes preparation required by AITC prior to deployment.

<table>
<thead>
<tr>
<th>Site/Other</th>
<th>Problem/Change Needed</th>
<th>Features to Adapt/Modify to New Product</th>
<th>Actions/Steps</th>
<th>Owner</th>
</tr>
</thead>
</table>
| AITC       | Creation of VMs for application hosting | N/A | • Software Installation  
• Network configuration | ESE |

3.3 **Resources**

This section describes the hardware, software, and communications for the deployment of Inbound eRx, where applicable.

3.3.1 **Facility Specifics**

No facility-specific features are required for this deployment.
3.3.2 Hardware
As middleware, PRE Inbound eRx requires no hardware to install.

3.3.3 Software
The following table describes the software specifications required prior to deployment.

<table>
<thead>
<tr>
<th>Required Software</th>
<th>Make</th>
<th>Version</th>
<th>Configuration</th>
<th>Manufacturer</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebLogic Application Server</td>
<td>Application Server</td>
<td>12.1.3c</td>
<td>Clustered</td>
<td>Oracle</td>
<td></td>
</tr>
<tr>
<td>Oracle Database</td>
<td>Database</td>
<td>11.2.0g</td>
<td>Standalone (not synchronized across data centers)</td>
<td>Oracle</td>
<td></td>
</tr>
<tr>
<td>Pentaho Data Integration</td>
<td>Data Integration Tool</td>
<td>6.1</td>
<td>Standalone</td>
<td>Pentaho (a Hitachi Group Company)</td>
<td></td>
</tr>
</tbody>
</table>

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

The software components will be staged at the following location:
\vaauspecdbs801.aac.dva.va.gov\AITC\IEP-eRx\downloads

Application deployment packages will be staged at the following location:
\vaauspecdbs801.aac.dva.va.gov\AITC\IEP-eRx\v.30\deployments

3.3.4 Communications
This section outlines the communications to be distributed to the business user community:

- Communication between the development team and AITC will occur via email and conference calls scheduled through Microsoft Lync.
- 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.
- Notification to VA users for unscheduled system outages or other events that impact the response time will be distributed within 30 minutes of the occurrence.
- Notification will be distributed to VA users regarding technical help desk support for obtaining assistance with receiving and processing inbound eRxs, and sending and receiving eRx transfers.
3.3.4.1 Deployment/Installation/Back-Out Checklist

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Day</th>
<th>Time</th>
<th>Individual who completed task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy</td>
<td>TBD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>TBD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back-Out</td>
<td>TBD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Deployment/Installation/Back-Out Checklist

4. Installation

This section outlines the installation steps for the various Inbound eRx components.

NOTE: The highlighted sections throughout this document indicate that that the text will be modified in future versions of this document.

4.1 Pre-installation and System Requirements

This section outlines the minimum requirements for the product to be installed, as well as the recommended hardware and software system requirements.

4.1.1 Pre-requisites

The following table outlines the specifications for VM.

<table>
<thead>
<tr>
<th>VM</th>
<th>RAM (GB)</th>
<th>Space (GB)</th>
<th>CPUs</th>
<th>OS</th>
<th>VM Description/Use/DNS Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>DEV 1 DB Server running Oracle</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>DEV 2 DB Server running Oracle</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>SQA 1 DB Server running Oracle</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>SQA 2 DB Server running Oracle</td>
</tr>
<tr>
<td>5</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>DEV1 AP Server running Apache/WebLogic</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>DEV 2 AP Server running Apache/WebLogic</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>SQA 1 AP Server running Apache/WebLogic</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>SQA 2 AP Server running Apache/WebLogic</td>
</tr>
<tr>
<td>Total</td>
<td>128</td>
<td>2400</td>
<td>32</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>
### Table 7: Staging Detailed VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>RAM (GB)</th>
<th>Space (GB)</th>
<th>CPUs</th>
<th>OS</th>
<th>VM Description/Use/DNS Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16</td>
<td>800</td>
<td>4</td>
<td>RHEL 7</td>
<td>STAGING DB Server running Oracle</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 7</td>
<td>STAGING Application Server running Apache/WebLogic</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 7</td>
<td>STAGING Application Server running Apache/WebLogic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>16</td>
<td>3</td>
<td><strong>48</strong></td>
</tr>
</tbody>
</table>

### Table 8: Pre-Production Detailed VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>RAM (GB)</th>
<th>Space (GB)</th>
<th>CPUs</th>
<th>OS</th>
<th>VM Description/Use/DNS Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16</td>
<td>1300</td>
<td>4</td>
<td>RHEL 6</td>
<td>PRE-PRODUCTION DB Server running Oracle</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>PRE-PRODUCTION Application Server running Apache/WebLogic</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>PRE-PRODUCTION Application Server running Apache/WebLogic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12</td>
<td>3</td>
<td><strong>48</strong></td>
</tr>
</tbody>
</table>

### Table 9: Production Detailed VM Requirements

<table>
<thead>
<tr>
<th>VM</th>
<th>RAM (GB)</th>
<th>Space (GB)</th>
<th>CPUs</th>
<th>OS</th>
<th>VM Description/Use/DNS Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16</td>
<td>1300</td>
<td>4</td>
<td>RHEL 6</td>
<td>PRODUCTION DB Server running Oracle</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>PRODUCTION Application Server running Apache/WebLogic</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>300</td>
<td>4</td>
<td>RHEL 6</td>
<td>PRODUCTION Application Server running Apache/WebLogic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12</td>
<td>3</td>
<td><strong>48</strong></td>
</tr>
</tbody>
</table>
4.1.2 Environment Configurations

Table 10 lists Environment Variables values that should be substituted throughout this document as system administrators are completing the installation steps.

<table>
<thead>
<tr>
<th>ENV</th>
<th>ORACLE_BASE</th>
<th>WLS_HOME</th>
<th>DOMAIN_HOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV1</td>
<td>/u01/app/Oracle_Home</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/erxdomain1</td>
</tr>
<tr>
<td>DEV2</td>
<td>/u01/app/Oracle_Home</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/erxdomain2</td>
</tr>
<tr>
<td>SQA1</td>
<td>/u01/app/Oracle_Home</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/erxdomain1</td>
</tr>
<tr>
<td>STAG</td>
<td>/u01/oracle</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/iep-stage</td>
</tr>
<tr>
<td>STAG2</td>
<td>/u01/oracle</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/iep-stage2</td>
</tr>
<tr>
<td>PREP</td>
<td>/u01/oracle</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/iep-preprod</td>
</tr>
<tr>
<td>PREP2</td>
<td>/u01/oracle</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/iep-preprod2</td>
</tr>
<tr>
<td>PROD</td>
<td>/u01/oracle</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/iep-prod</td>
</tr>
<tr>
<td>PROD2</td>
<td>/u01/oracle</td>
<td>$ORACLE_BASE/wlserver</td>
<td>$ORACLE_BASE/user_projects/domains/iep-prod2</td>
</tr>
</tbody>
</table>
Table 11 lists the symbolic names that should be substituted throughout this document as system administrators are completing the installation steps.

**Table 11: Symbolic Names by Environment**

<table>
<thead>
<tr>
<th>ENV</th>
<th>vm1_fqdn</th>
<th>vm1_name</th>
<th>vm2_fqdn</th>
<th>vm2_name</th>
<th>domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV1</td>
<td>vauserxappdev1.aac.va.gov</td>
<td>vauserxappdev1</td>
<td>vauserxappdev2.aac.va.gov</td>
<td>vauserxappdev2</td>
<td>erxdomain1</td>
</tr>
<tr>
<td>DEV2</td>
<td>vauserxappdev2.aac.va.gov</td>
<td>vauserxappdev2</td>
<td>vauserxappdev1.aac.va.gov</td>
<td>vauserxappdev1</td>
<td>erxdomain2</td>
</tr>
<tr>
<td>SQA1</td>
<td>vauserxappsqa1.aac.va.gov</td>
<td>vauserxappdev1</td>
<td>vauserxappdev2.aac.va.gov</td>
<td>vauserxappdev2</td>
<td>erxdomain1</td>
</tr>
<tr>
<td>STAG</td>
<td>vausappiep402.aac.va.gov</td>
<td>vausappiep402</td>
<td>vausappiep403.aac.va.gov</td>
<td>vausappiep403</td>
<td>iep-stage</td>
</tr>
<tr>
<td>STAG2</td>
<td>vausappiep621.aac.va.gov</td>
<td>vausappiep621</td>
<td>vausappiep622.aac.va.gov</td>
<td>Vausappiep622</td>
<td>iep-stage2</td>
</tr>
<tr>
<td>PREP</td>
<td>vausappiep404.aac.va.gov</td>
<td>vausappiep404</td>
<td>vausappiep405.aac.va.gov</td>
<td>vausappiep405</td>
<td>iep-preprod</td>
</tr>
<tr>
<td>PREP2</td>
<td>vausappiep421.aac.va.gov</td>
<td>vausappiep421</td>
<td>vausappiep422.aac.va.gov</td>
<td>vausappiep422</td>
<td>iep-preprod2</td>
</tr>
<tr>
<td>PROD</td>
<td>vausappiep201.aac.va.gov</td>
<td>vausappiep201</td>
<td>vausappiep202.aac.va.gov</td>
<td>vausappiep202</td>
<td>iep-prod</td>
</tr>
<tr>
<td>PROD2</td>
<td>vausappiep221.aac.va.gov</td>
<td>vausappiep221</td>
<td>vausappiep222.aac.va.gov</td>
<td>vausappiep222</td>
<td>iep-prod2</td>
</tr>
</tbody>
</table>

**Table 12: Symbolic Names by Environment (cont)**

<table>
<thead>
<tr>
<th>ENV</th>
<th>env</th>
<th>Env</th>
<th>erx_port</th>
<th>proxy_fqdn</th>
<th>proxy_name</th>
<th>db_fqdn</th>
<th>db_name</th>
<th>db_port</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV1</td>
<td>dev1</td>
<td>Dev1</td>
<td>8001</td>
<td>vauserxappdev1.aac.va.gov</td>
<td>vauserxappdev1</td>
<td>vauserxdevsdev1.aac.va.gov</td>
<td>ERXD1</td>
<td>1549</td>
</tr>
<tr>
<td>DEV2</td>
<td>dev2</td>
<td>Dev2</td>
<td>8003</td>
<td>vauserxappdev2.aac.va.gov</td>
<td>vauserxappdev2</td>
<td>vauserxdevsdev2.aac.va.gov</td>
<td>ERXD2</td>
<td>1550</td>
</tr>
<tr>
<td>SQA1</td>
<td>sqa1</td>
<td>Sqa1</td>
<td>8001</td>
<td>vauserxappsqa2.aac.va.gov</td>
<td>vauserxappsqa2</td>
<td>vauserxdbssqa1.aac.va.gov</td>
<td>ERXS1</td>
<td>1549</td>
</tr>
<tr>
<td>STAG</td>
<td>stag</td>
<td>Stag</td>
<td>8001</td>
<td>vausappiep402.aac.va.gov</td>
<td>vausappiep402</td>
<td>vausdbiep400.aac.va.gov</td>
<td>IEPOA</td>
<td>1647</td>
</tr>
<tr>
<td>STAG2</td>
<td>stag2</td>
<td>Stag2</td>
<td>8001</td>
<td>vausappiep622.aac.va.gov</td>
<td>vausappiep622</td>
<td>vausdbiep400.aac.va.gov</td>
<td>IEPOA2</td>
<td>1648</td>
</tr>
<tr>
<td>PREP</td>
<td>prep</td>
<td>Prep</td>
<td>8001</td>
<td>vausappiep404.aac.va.gov</td>
<td>vausappiep404</td>
<td>vausdbiep401.aac.va.gov</td>
<td>IEPY</td>
<td>1647</td>
</tr>
<tr>
<td>PREP2</td>
<td>prep2</td>
<td>Prep2</td>
<td>8001</td>
<td>vausappiep422.aac.va.gov</td>
<td>vausappiep422</td>
<td>vausdbiep420.aac.va.gov</td>
<td>IEPY2</td>
<td>1647</td>
</tr>
<tr>
<td>PROD</td>
<td>prod</td>
<td>Prod2</td>
<td>8001</td>
<td>vausappiep201.aac.va.gov</td>
<td>vausappiep201</td>
<td>vausdbiep200.aac.va.gov</td>
<td>IEPP</td>
<td>1647</td>
</tr>
<tr>
<td>PROD2</td>
<td>prod2</td>
<td>Prod2</td>
<td>8001</td>
<td>vausappiep221.aac.va.gov</td>
<td>vausappiep221</td>
<td>vausdbiep220.aac.va.gov</td>
<td>IEPP2</td>
<td>1647</td>
</tr>
</tbody>
</table>
Table 13: Symbolic Names by Environment (cont)

<table>
<thead>
<tr>
<th>ENV</th>
<th>mserver1</th>
<th>mserver2</th>
<th>cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV1</td>
<td>erx1</td>
<td>erx2</td>
<td>dev1</td>
</tr>
<tr>
<td>DEV2</td>
<td>erx1</td>
<td>erx2</td>
<td>dev1</td>
</tr>
<tr>
<td>SQA1</td>
<td>erx1</td>
<td>erx2</td>
<td>dev1</td>
</tr>
<tr>
<td>STAG2</td>
<td>ManagedServer001</td>
<td>ManagedServer002</td>
<td>Cluster001</td>
</tr>
<tr>
<td>STAG</td>
<td>ManagedServer001</td>
<td>ManagedServer002</td>
<td>Cluster001</td>
</tr>
<tr>
<td>PREP2</td>
<td>ManagedServer001</td>
<td>ManagedServer002</td>
<td>Cluster001</td>
</tr>
<tr>
<td>PREP</td>
<td>ManagedServer001</td>
<td>ManagedServer002</td>
<td>Cluster001</td>
</tr>
<tr>
<td>PROD2</td>
<td>ManagedServer001</td>
<td>ManagedServer002</td>
<td>Cluster001</td>
</tr>
<tr>
<td>PROD</td>
<td>ManagedServer001</td>
<td>ManagedServer002</td>
<td>Cluster001</td>
</tr>
<tr>
<td>ENV</td>
<td>iam_hco</td>
<td>iam_policy_entries</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>--------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>DEV1</td>
<td>INTHCO</td>
<td>policyserver=&quot;smp1.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td>DEV2</td>
<td>INTHCO</td>
<td>policyserver=&quot;smp1.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.int.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td>SQA1</td>
<td>SQAHO</td>
<td>policyserver=&quot;smp1.sqa.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.sqa.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.sqa.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.sqa.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td>STAG</td>
<td>PREPRODHCO</td>
<td>policyserver=&quot;smp1.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp5.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp6.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp7.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp8.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td>STAG2</td>
<td>PREPRODHCO</td>
<td>policyserver=&quot;smp1.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp5.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp6.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp7.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp8.preprod.iam.va.gov,44441,44442,44443&quot;</td>
<td></td>
</tr>
</tbody>
</table>
### Table 15: Symbolic Names by Environment (cont)

<table>
<thead>
<tr>
<th>ENV</th>
<th>iam_hco</th>
<th>iam_policy_entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREP</td>
<td>PREPRODHCO</td>
<td>policyserver=&quot;smp1.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp5.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp6.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp7.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp8.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td>PREP2</td>
<td>PREPRODHCO</td>
<td>policyserver=&quot;smp1.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp5.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp6.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp7.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp8.preprod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
</tbody>
</table>
Table 16: Symbolic Names by Environment (cont)

<table>
<thead>
<tr>
<th>ENV</th>
<th>iam_hco</th>
<th>iam_policy_entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROD</td>
<td>PRODHCO</td>
<td>policyserver=&quot;smp1.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp5.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp6.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp7.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp8.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td>PROD2</td>
<td>PRODHCO</td>
<td>policyserver=&quot;smp1.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp2.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp3.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp4.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp5.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp6.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp7.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policyserver=&quot;smp8.prod.iam.va.gov,44441,44442,44443&quot;</td>
</tr>
</tbody>
</table>
In addition to the above Environment Variables and Symbolic Names, there are several passwords or secret phrases which are required throughout the installation. The table below identifies Symbolic Names that will be used in this document, and provide a brief description of each. The values of these sensitive items will be will be defined by the appropriate administrator during the installation process, and should be properly recorded and shared with others on a need to know basis.

<table>
<thead>
<tr>
<th>Symbolic Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore_passphrase</td>
<td>[proxy_fqdn]</td>
</tr>
<tr>
<td>privatekey_passphrase</td>
<td>[keystore_passphrase]</td>
</tr>
<tr>
<td>weblogic_password</td>
<td>[privatekey_passphrase]</td>
</tr>
</tbody>
</table>

KeyStores=CustomIdentityAndCustomTrust
CustomIdentityAlias= [proxy_fqdn]
CustomIdentityKeyStoreFileName= [DOMAIN_HOME]/security/[proxy_fqdn]
CustomIdentityKeyStorePassPhrase= [keystore_passphrase]
CustomIdentityKeyStoreType=JKS
CustomIdentityPrivateKeyPassPhrase= [privatekey_passphrase]

Need to think about setting up environment scripts for the following:
$ export ORACLE_BASE=/u01/app/Oracle_Home
$ export WLS_HOME=$ORACLE_BASE/wlserver
$ export DOMAIN_HOME=$ORACLE_BASE/user_projects/domains/erxdomain1
4.2 Platform Installation and Preparation

The following sections describe the steps to prepare the operating system for the installation of the application. Most activities are to be performed by the RHEL System Administrator.

4.2.1 Modify /etc/hosts entry

1. Modify /etc/hosts to add fully qualified domain name for the local server (the following must be performed by a system administrator):
   
   ```
   $ sudo vi /etc/hosts
   ```

2. Add entries similar to the following:
   
   ```
   ????.???.??? [vm1_fqdn][vm1_name].domain.local [vm1_name]  
   ????.???.??? [vm2_fqdn][vm2_name].domain.local [vm2_name]  
   ????.???.??? [db_fqdn][db_name].domain.local [db_name]  
   ```

3. Save the file and exit. Note the following explanations of the hosts entry fields:
   
   ```
   ????.???.??? <- IP address of the server
   ```

4.2.2 X Windows

1. Install the Linux X Window libraries (the following must be performed by a system administrator):
   
   ```
   $ sudo yum install xorg-x11-xauth.x86_64
   ```

2. Start Attachmate Reflection X (Click Start > All Programs > Attachmate Reflection > Reflection X).

3. Modify the SSH session:
   
   a. Connection > SSH > X11 > Enable X11 forwarding
   
   b. Connection > SSH > X11 > X display location > :0.0

4. Connect to the Linux server with the new SSH session settings. The DISPLAY environment variable should be automatically set.

5. In order to run X applications after doing a sudo su to another account, first modify the .Xauthority file

6. As your normal Linux login account:
   
   ```
   $ cp ~/.Xauthority /tmp
   ```

7. After you sudo su to another user, copy the .Xauthority file:
   
   ```
   $ cp /tmp/.Xauthority ~
   ```

4.2.3 Setup Administration Accounts

1. Create the Linux weblogic user and group (the following must be performed by a system administrator):
   
   ```
   $ sudo groupadd -g 7400 weblogic (this group already exists in LDAP)  
   $ sudo useradd -g weblogic weblogic
   ```

2. Create the Linux weblogic sudoer file (the following must be performed by a system administrator):
   
   ```
   $ cat > /etc/sudoers.d/weblogic
   weblogic ALL=NOPASSWD:/sbin/service wls start,/sbin/service wls stop,/sbin/service wls stop_all,/sbin/service wls status,/sbin/service wlnm start,/sbin/service wlnm stop,/sbin/service wlnm status
   ```

PRE Inbound eRx  
3. Modify the Linux weblogic account to add umask command near the beginning of the file
   `~weblogic/.bash_profile`:
   ```
   umask 0022
   ```

4. Create the app software directory if it doesn’t exist (the following must be performed by a
   system administrator):
   ```
   $ sudo chmod 777 /u01
   $ sudo mkdir -p /u01/app
   $ sudo chown weblogic:weblogic /u01/app
   $ sudo chmod 777 /u01/app
   ```

5. Create the Linux kettle user and group (the following must be performed by a system
   administrator):
   ```
   $ sudo groupadd -g 7600 kettle
   $ sudo useradd -g kettle kettle
   $ sudo usermod -a -G weblogic kettle (weblogic group already exists in LDAP)
   ```

6. Create the Linux kettle sudoer file (the following must be performed by a system
   administrator):
   ```
   $ sudo cat > /etc/sudoers.d/kettle
   kettle ALL=NOPASSWD:/sbin/service kettle start,/sbin/service kettle stop,/sbin/service
   kettle stop all,/sbin/service kettle status
   Cmd_Alias KETTLE_SU=/bin/su
   Cmd_Alias KETTLE_SU=/bin/su
   %kettle        ALL=(ALL)       KETTLE_SU
   %kettle
   ```

7. Create the pentaho software directory if it doesn’t exist (the following must be performed
   by a system administrator):
   ```
   $ sudo mkdir -p /u01/app/pentaho
   $ sudo chown kettle:kettle /u01/app/pentaho
   $ sudo chmod 755 /u01/app/pentaho
   ```

8. Modify the Linux kettle account to add umask command near the beginning of the file
   `~kettle/.bash_profile`:
   ```
   umask 0022
   ```

9. Modify the Linux kettle account to replace the PATH= and export PATH near the end of
   the file `~kettle/.bash_profile`:
   ```
   export JAVA_HOME=/u01/app/java/latest/bin/java
   export PATH=$JAVA_HOME/bin:$PATH:$HOME/bin
   ```

10. Create the Linux apache sudoer file (the following must be performed by a system
    administrator):
    ```
    $ sudo vi /etc/sudoers.d/apache
    apache ALL=(kettle:kettle) NOPASSWD:/u01/app/cpanel/bin/carte_slave_util.sh
    ```
4.2.4 Install Java

1. As your normal Linux login account, sudo su to the weblogic account:
   $ sudo su - weblogic
2. Create downloads directory if it doesn’t exist:
   $ mkdir -p /u01/downloads
3. Download Oracle JDK 1.8 for Linux x86-64 to the downloads directory:
   Download from ATIC IEP eRx Downloads directory
4. Create Java directory if it doesn’t exist:
   $ mkdir -p /u01/app/java
5. Unpack the Oracle JDK 1.8 archive to in the downloads directory:
   $ cd /u01/app/java
   $ gzip -cd < /u01/downloads/jdk-8uXXX-linux-x64.tar.gz | tar xvf -
6. Create symbolic link for latest Java installation:
   $ ln -s cd /u01/app/java/jdk1.8.0_xxx /u01/app/java/latest
7. Add instructions to open permissions to permit access to all users, and to create link for /u01/app/java if located in a different location.
   $ exit
8. Return back in your normal Linux login account.
   $ exit

4.2.5 Apache Installation on VM1 and VM2

Perform the following steps on VM1 and VM2:

1. EO SA installs standard Apache 2.2 RHEL6 RPM, as your normal Linux login account verify as follows:
   $ sudo rpm -q -a | grep httpd
   httpd-2.2.15-39.el6.x86_64
   httpd-tools-2.2.15-39.el6.x86_64
2. Install the Linux NSS package (the following must be performed by a system administrator):
   $ sudo yum install mod_nss.x86_64
3. Modify the httpd startup configuration (the following must be performed by a system administrator):
   $ sudo chkconfig --level 2345 httpd on
   $ sudo systemctl enable httpd # for RHEL 7 systems
4.2.6 Apache Configuration on VM1 and VM2

servers are RHEL 7 and they have Apache version 2.4. Want to confirm if these instructions are for Apache 2.2 or 2.4?

Here are the differences between document and Apache conf file on server.

6. No <IfModule prefork.c>

9. No <Directory "/var/www/icons"> section

Instead <Directory "/var/www/html"> section exist and it has the Option parameter

Options Indexes FollowSymLinks

The following step need to be performed on VM1 and VM2:

1. Modify HTTPD configuration:

   $ sudo vi /etc/httpd/conf/httpd.conf

2. Modify Timeout parameter:

   Timeout 120

3. Modify <IfModule prefork.c>parameters:

   StartServers 8
   ServerLimit 300
   MaxClients 300

4. Modify Listen parameter:

   Listen 80

5. Modify <Directory /> section:

   <Directory />
      Options FollowSymLinks
      AllowOverride None
      <Limit PUT>
          Order deny,allow
          Deny from all
      </Limit>
   </Directory>

6. Modify <Directory "/var/www/icons"> Options parameter:

   #Options Indexes MultiViews FollowSymLinks
   Options Indexes

7. Modify <Directory "/var/www/html"> section:

   <Directory "/var/www/html">
      Options Indexes FollowSymLinks
      AllowOverride None
      Order allow,deny
      Allow from all
   </Directory>

8. Add <Directory "/var/www/html/cpanel"> section:

   <Directory "/var/www/html">
      Options Indexes FollowSymLinks
      AllowOverride None
      Order allow,deny
      Allow from all
   </Directory>

9. Enable ScriptAlias:

   ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"

10. Modify <Directory "/var/www/cgi-bin"> section:

    <Directory "/var/www/cgi-bin">
        AllowOverride None
        Options None
        Order allow,deny
        Allow from all
    </Directory>
11. Modify HTTPD configuration:
   $ sudo vi /etc/httpd/conf/httpd.conf

12. Add Header Edit entries to bottom of /etc/http/conf/httpd.conf
   Header edit Set-Cookie "(?i)\^\{?!:(?!;\s?HttpOnly).\}+$" "$1; HttpOnly"
   Header edit Set-Cookie "(?i)\^\{?!:(?!;\s?secure).\}+$" "$1; Secure"
   Header always append X-Frame-Options DENY

13. Reverse Proxy to Pentaho Slaves in /etc/http/conf.d/pentaho.conf:
   $ sudo vi /etc/http/conf.d/pentaho.conf
   # Reverse proxy to Pentaho slaves
   <Location /master1/>
     ProxyPass http://[vm1_fqdn]:8080/
     ProxyPassReverse http://[vm1_fqdn]:8080/
     AddOutputFilterByType SUBSTITUTE text/html
     Substitute "s|/kettle/|/master1/kettle/|i"
   </Location>
   <Location /slave1/>
     ProxyPass http://[vm1_fqdn]:8081/
     ProxyPassReverse http://[vm1_fqdn]:8081/
     AddOutputFilterByType SUBSTITUTE text/html
     Substitute "s|/kettle/|/slave1/kettle/|i"
   </Location>
   <Location /slave2/>
     ProxyPass http://[vm1_fqdn]:8082/
     ProxyPassReverse http://[vm1_fqdn]:8082/
     AddOutputFilterByType SUBSTITUTE text/html
     Substitute "s|/kettle/|/slave2/kettle/|i"
   </Location>
   <Location /slave3/>
     ProxyPass http://[vm2_fqdn]:8083/
     ProxyPassReverse http://[vm2_fqdn]:8083/
     AddOutputFilterByType SUBSTITUTE text/html
     Substitute "s|/kettle/|/slave3/kettle/|i"
   </Location>
   <Location /slave4/>
     ProxyPass http://[vm2_fqdn]:8084/
     ProxyPassReverse http://[vm2_fqdn]:8084/
     AddOutputFilterByType SUBSTITUTE text/html
     Substitute "s|/kettle/|/slave4/kettle/|i"
   </Location>

14. Restart Apache:
   $ sudo service httpd stop
   $ sudo service httpd start
4.2.7 Certificate Configuration

3 thru 14. Saving these certificates with .pem file extension instead of .txt, this does not make any difference in functionality, it’s only a better representation of the file format, since they are actually PEM format.

15, 16. Replacing these steps with the AITC standards that we follow to generate and request certificates. Steps are as follows:

1) Create a configuration file with name: [proxy_fqdn].cnf, content:

```plaintext
[req]
req_extensions = v3_req
prompt = no
[v3_req]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
# Some CAs do not yet support subjectAltName in CSRs.
# Instead the additional names are form entries on web
# pages where one requests the certificate...
subjectAltName = @alt_names
[alt_names]
DNS.1 = [proxy_fqdn1]
DNS.2 = [proxy_fqdn2]
[req_distinguished_name]
C = US
ST = Texas
L = Austin
O = US Department of Veterans Affairs
OU = AITC
CN = [proxy_fqdn]
emailAddress = cdcoweblogicadministrators@va.gov
[js_attributes]
challengePassword = xxxxxxxxxxx
```

Command to generate csr and private key:

```
openssl req -new -newkey rsa:2048 -keyout [proxy_fqdn].key -out [proxy_fqdn].csr -config [proxy_fqdn].cnf
```

1. As your normal Linux login account, sudo su to the weblogic account:

   ```
   $ sudo su - weblogic
   ```

2. Create a “certificates” directory to store all certificate artifacts:

   ```
   $ mkdir /u01/certificates
   $ cd /u01/certificates
   ```

3. Create the va_root_ca_cert.pem certificate in the “certificates” directory:

   ```
   $ cat > va_root_ca_cert.pem
   ```

4. Paste the va_root_ca_cert.pem content from Appendix 8.1.1.

   ```
   <ctrl>d
   ```

5. Create the va_internal_subordinate_ca_cert.pem content in the “certificates” directory:

   ```
   $ cat > va_internal_subordinate_ca_cert.pem
   ```

6. Paste the va_internal_subordinate_ca_cert.pem content from Appendix 8.1.2.

   ```
   <ctrl>d
   ```

7. Create the va_root_ca_s2_cert.pem certificate in the “certificates” directory:

   ```
   $ cat > va_root_ca_s2_cert.pem
   ```

8. Paste the va_root_ca_s2_cert.pem content from Appendix 8.1.3.

   ```
   <ctrl>d
   ```

9. Create the va_intermediate_ca1_s2_cert.pem certificate in the “certificates” directory:

   ```
   $ cat > va_intermediate_ca1_s2_cert.pem
   ```

10. Paste the va_intermediate_ca1_s2_cert.pem content from Appendix 8.1.4.

    ```
    <ctrl>d
    ```

11. Create the va_intermediate_ca2_s2_cert.pem certificate in the “certificates” directory:
12. Paste the va_intermediate_ca2_s2_cert.pem content from Appendix 8.1.5.
<ctrl>d

13. Create the betrusted_production_ssp_ca_a1_cert.pem certificate in the “certificates” directory:
$ cat > betrusted_production_ssp_ca_a1_cert.pem
<ctrl>d

14. Paste the betrusted_production_ssp_ca_a1_cert.pem content from Appendix 8.1.6.
<ctrl>d

15. Create the federal_common_policy_ca_cert.pem certificate in the “certificates” directory:
$ cat > federal_common_policy_ca_cert.pem
<ctrl>d

16. Paste federal_common_policy_ca_cert.txt content from Appendix 8.1.7.
<ctrl>d

17. Create the veterans_affairs_device_ca_b2_cert.pem certificate in the “certificates” directory:
$ cat > veterans_affairs_device_ca_b2_cert.pem
<ctrl>d

18. Paste the veterans_affairs_device_ca_b2_cert.pem content from Appendix 8.1.8.
<ctrl>d

19. Create the vaww.ersdev.aac.va.gov_cert.pem certificate in the “certificates” directory:
$ cat > vaww.ersdev.aac.va.gov_cert.pem
<ctrl>d

20. Paste the vaww.ersdev.aac.va.gov_cert.pem content from Appendix 8.1.9.
<ctrl>d

21. Create the vaww.esrstage1a.aac.va.gov.pem certificate in the “certificates” directory:
$ cat > vaww.esrstage1a.aac.va.gov.pem
<ctrl>d

22. Paste the vaww.esrstage1a.aac.va.gov.pem content from Appendix 8.1.10.
<ctrl>d

23. Create the vaww.esrstage1b.aac.va.gov.pem certificate in the “certificates” directory:
$ cat > vaww.esrstage1b.aac.va.gov.pem
<ctrl>d

24. Paste the vaww.esrstage1b.aac.va.gov.pem content from Appendix 8.1.11.
<ctrl>d

25. Create the vaww.esrpre-prod.aac.va.gov.pem certificate in the “certificates” directory:
$ cat > vaww.esrpre-prod.aac.va.gov.pem
<ctrl>d

<ctrl>d

27. Create the das-test.va.gov.pem certificate in the “certificates” directory:
$ cat > das-test.va.gov.pem
<ctrl>d

28. Paste the das-test.va.gov.pem content from Appendix 0.
<ctrl>d

29. Create the das-sqa.va.gov.pem certificate in the “certificates” directory:
$ cat > das-sqa.va.gov.pem
<ctrl>d

<ctrl>d

31. Create the das.va.gov.pem certificate in the “certificates” directory:
$ cat > das.va.gov.pem
<ctrl>d

32. Paste the das.va.gov.pem content from Appendix 8.1.15.
<ctrl>d
33. Create a certificate request configuration file:

```bash
$ cat > [proxy_fqdn]_csr_cfg.txt
[req]
default_bits=2048
prompt=no
default_md=sha256
req_extensions=req_ext
distinguished_name=dn

[ dn ]
C=US
ST=Texas
L=Austin
O=US Department of Veterans Affairs
OU=AITC
CN=[proxy_fqdn]
emailAddress=admin@va.gov

[ req_ext ]
supjectAltName=@alt_names

[ alt_names ]
DNS.1=[proxy_fqdn]
DNS.2=[vm2_fqdn]
```

34. Generate a permanent certificate signing request:

```bash
$ openssl req -out [proxy_fqdn]_csr_[yyyymmdd].txt -newkey rsa:2048 -keyout [proxy_fqdn]_key.txt -nodes -config [proxy_fqdn]_csr_cfg.txt
Generating a 2048 bit RSA private key
.........+++
writing new private key to ' [proxy_fqdn]_key.txt'
-----
```

35. Submit the certificate signing request to VA PKI to obtain a permanent certificate.

36. Save the permanent certificate in the “certificates” directory:

```bash
$ cat > /u01/certificates/[proxy_fqdn]_cert.pem
37. Paste permanent certificate content.
```

38. Generate a [proxy_fqdn] pkcs12 certificate store:

```bash
$ openssl pkcs12 -export -name [proxy_fqdn] -in [proxy_fqdn]_cert.pem -inkey [proxy_fqdn]_key.txt -out [proxy_fqdn].p12
Enter Export Password: ####
Verifying - Enter Export Password: ####
```

39. Generate [proxy_fqdn] java keystore:

```bash
```

40. Import va_root_ca_cert.pem Certificate into [proxy_fqdn] java keystore:

```bash
$ keytool -import -alias va_root_ca -file va_root_ca_cert.pem -keystore [proxy_fqdn].jks
Enter keystore password: #######
Trust this certificate? (no): yes
Certificate was added to keystore
```

41. Import va_internal_subordinate_ca_cert.pem Certificate into [proxy_fqdn] java keystore:

```bash
$ keytool -import -alias va_internal_subordinate_ca -file va_internal_subordinate_ca_cert.pem -keystore [proxy_fqdn].jks
Enter keystore password: #######
Trust this certificate? (no): yes
Certificate was added to keystore
```

42. Import va_root_ca_s2_cert.pem Certificate into [proxy_fqdn] java keystore:
$ keytool -import -alias va_root_ca_s2 -file va_root_ca_s2_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

43. Import va_intermediate_ca1_s2_cert.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias va_intermediate_ca1_s2 -file va_intermediate_ca1_s2_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

44. Import va_intermediate_ca2_s2_cert.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias va_intermediate_ca2_s2 -file va_intermediate_ca2_s2_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

45. Import veterans_affairs_device_ca_b2_cert.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias veterans_affairs_device_ca_b2 -file veterans_affairs_device_ca_b2_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

46. Import betrusted_production_ssp_ca_a1.crt.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias betrusted_production_ssp_ca_a1 -file betrusted_production_ssp_ca_a1.crt.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

47. Import federal_common_policy_ca_cert.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias federal_common_policy_ca -file federal_common_policy_ca_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

48. Import sqa.services.eauth.va.gov_cert.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias sqa.services.eauth.va.gov -file sqa.services.eauth.va.gov_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

49. Import vaww.esrdev.aac.va.gov_cert.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias vaww.esrdev.aac.va.gov -file vaww.esrdev.aac.va.gov_cert.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

50. Import vaww.esrstage1.aac.va.gov.pem Certificate into [proxy fqdn] java keystore:
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

51. Import vaww.esrstage1b.aac.va.gov.pem Certificate into [proxy fqdn] java keystore:
$ keytool -import -alias vaww.esrstage1b.aac.va.gov -file vaww.esrstage1b.aac.va.gov.pem -keystore [proxy fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

52. Import vaww.esrpre-prod.aac.va.gov.pem Certificate into [proxy_fqdn] java keystore:

$ keytool -import -alias vaww.esrpre-prod.aac.va.gov -file vaww.esrpre-
prod.aac.va.gov.pem -keystore [proxy_fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

53. Import das-test.va.gov.pem Certificate into [proxy_fqdn] java keystore:

$ keytool -import -alias das-test.va.gov -file das-test.va.gov.pem -keystore
[proxy_fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

54. Import das-sqa.va.gov.pem Certificate into [proxy_fqdn] java keystore:

$ keytool -import -alias das-sqa.va.gov -file das-sqa.va.gov.pem -keystore
[proxy_fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

55. Import das.va.gov.pem Certificate into [proxy_fqdn] java keystore:

$ keytool -import -alias das.va.gov -file das
.va.gov.pem -keystore [proxy_fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]: yes
Certificate was added to keystore

56. Copy certificate artifacts to VM2:

$ scp [proxy_fqdn].jks [vm2_fqdn]:/u01/certificates
$ scp [vm2_fqdn].p12 [vm2_fqdn]:/u01/certificates
$ scp cacerts [vm2_fqdn]:/u01/certificates
4.2.8 Create NSS certificate database on VM1

1. Create a new NSS certificate database:
   ```
   $ sudo mv /etc/httpd/alias /etc/httpd/alias_orig
   $ sudo mkdir /etc/httpd/alias
   $ sudo certutil -N -d /etc/httpd/alias
   Entering new password: ####
   Re-enter password: ####
   ```

2. Add server permanent certificate:
   ```
   $ sudo pk12util -i [proxy_fqdn].p12 -d /etc/httpd/alias -n [proxy_fqdn]
   Entering password or PIN for "NSS Certificate DB": ####
   ```

3. Add certificate chain:
   ```
   $ sudo certutil -A -d /etc/httpd/alias -i va_root_ca_s2_cert.pem -t CT,, -n va_root_ca_s2
   $ sudo certutil -A -d /etc/httpd/alias -i va_intermediate_ca1_s2_cert.pem -t CT,, -n va_intermediate_ca1_s2
   $ sudo certutil -A -d /etc/httpd/alias -i va_intermediate_ca2_s2_cert.pem -t CT,, -n va_intermediate_ca2_s2
   ```

4. Modify certificate database permissions:
   ```
   $ sudo chmod g+rx,o+rx /etc/httpd/alias
   $ sudo chmod -R g+r,o+r /etc/httpd/alias/*
   ```

5. Verify installed certificates:
   ```
   $ certutil -L -d /etc/httpd/alias
   ```

6. Create certificate database password file:
   ```
   $ cat > /etc/httpd/conf/password.conf
   internal:####
   NSS FIPS 140-2 Certificate DB:####
   <ctrl>d
   ```

7. Modify certificate database password file permissions:
   ```
   $ sudo chmod g+r,o+r /etc/httpd/conf/password.conf
   ```

8. Start HTTPD server
   ```
   $ sudo service httpd start
   ```

9. Review access_log, error_log, nss_access_log and nss_error_log to ensure TLS is functioning correctly.
4.2.9 Create NSS certificate database on VM2

1. Create a new NSS certificate database:
   $ sudo mv /etc/httpd/alias /etc/httpd/alias_orig
   $ sudo mkdir /etc/httpd/alias
   $ sudo certutil -N -d /etc/httpd/alias
   Enter new password: ####
   Re-enter password: ####

2. Add server permanent certificate:
   $ sudo pk12util -i [vm2_fqdn].p12 -d /etc/httpd/alias -n [vm2_fqdn]
   Enter Password or Pin for "NSS Certificate DB": ####
   Enter password for PKCS12 file: ####
   pk12util: PKCS12 IMPORT SUCCESSFUL

3. Add certificate chain:
   $ sudo certutil -A -d /etc/httpd/alias -i va_root_ca_s2_cert.pem -t CT,, -n va_root_ca_s2
   $ sudo certutil -A -d /etc/httpd/alias -i va_intermediate_ca1_s2_cert.pem -t CT,, -n va_intermediate_ca1_s2
   $ sudo certutil -A -d /etc/httpd/alias -i va_intermediate_ca2_s2_cert.pem -t CT,, -n va_intermediate_ca2_s2

4. Modify certificate database permissions:
   $ sudo chmod g+rx,o+rx /etc/httpd/alias
   $ sudo chmod -R g+r,o+r /etc/httpd/alias/*

5. Verify installed certificates:
   $ certutil -L -d /etc/httpd/alias

6. Create certificate database password file:
   $ cat > /etc/httpd/conf/password.conf
   internal:####
   NSS FIPS 140-2 Certificate DB:####
   <ctrl>d

7. Modify certificate database password file permissions:
   $ sudo chmod g+r,o+r /etc/httpd/conf/password.conf

8. Start HTTPD server
   $ sudo service httpd start

9. Review access_log, error_log, nss_access_log and nss_error_log to ensure TLS is functioning correctly.
4.2.10 NSS Configuration on VM1

6. cp /tmp/INB_ERX1.0/downloads/WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64/lib/mod_wl_24.so /etc/httpd/modules/ - Need Linux SA assistance.
Note: we are using mod_wl_24.so instead of mod_wl.so since Apache on this server is Apache v2.4
7. - Changed From LoadModule weblogic_module modules/mod_wl.so To LoadModule weblogic_module modules/mod_wl_24.so
   - remove "#exit"
8. Remove this step as we will run Apache commands as WebLogic.
9. Replace with
   - sudo systemctl status httpd.service
   - sudo systemctl stop httpd.service
   - sudo systemctl start httpd.service

The following steps need to be performed on VM1 and VM2:

1. Rename the RPM default ssl.conf file to ssl.conf_orig to prevent Apache from loading during startup.
   $ sudo mv ssl.conf ssl.conf_orig

2. Modify NSS configuration:
   $ sudo vi /etc/httpd/conf.d/nss.conf
   a. Modify Listen parameter:
      #Listen 8443
      Listen 443
   b. Modify NSSPassPhraseDialog parameter:
      #NSSPassPhraseDialog builtin
      NSSPassPhraseDialog file:/etc/httpd/conf/password.conf
      NSSFIPS on
   c. Modify VirtualHost tag:
      #<VirtualHost _default_:8443>
      <VirtualHost _default_:443>
   d. Modify ServerName parameter:
      #ServerName www.example.com:8443
      ServerName [proxy_fqdn]:443
   e. Modify NSS logging parameters:
      #ErrorLog /etc/httpd/logs/error_log
      ErrorLog /etc/httpd/logs/nss_error_log
      TransferLog /etc/httpd/logs/nss_access_log
   f. Modify NSSCipherSuite parameters:
      #NSSCipherSuite
      +aes_128_sha_256,+aes_256_sha_256,+ecdhe_ecdsa_aes_128_gcm_sha_256,+ecdhe_ecdsa_ae
      s_128_sha,+ecdhe_ecdsa_aes_256_sha,+ecdhe_rsa_aes_128_gcm_sha_256,+ecdhe_rsa_aes_1
      28_sha,+ecdhe_rsa_aes_256_sha,+rsa_aes_128_gcm_sha_256,+rsa_aes_128_sha,+rsa_aes_2
      56_sha
      NSSCipherSuite +rsa_aes_128_sha,+rsa_aes_256_sha
   g. Modify NSSProtocol parameters:
      #NSSProtocol SSLv3, TLSv1.0, TLSv1.1
      NSSProtocol TLSv1.1, TLSv1.2
   h. Modify NSSNickname parameter:
      #NSSNickname Server=Cert
      NSSNickname [proxy_fqdn]
      NSSEnforceValidCerts off
   i. Save the nss.conf file.

3. Start HTTPD server
   $ sudo service httpd start
4. Review access_log, error_log, nss_access_log and nss_error_log to ensure TLS is functioning correctly.

4.2.11 NSS Configuration on VM2

6. cp /tmp/INB_ERX1.0/downloads/WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64/lib/mod_wl_24.so /etc/httpd/modules/ - Need Linux SA assistance.
   Note: we are using mod_wl_24.so instead of mod_wl.so since Apache on this server is Apache v2.4
7. - Changed From LoadModule weblogic_module modules/mod_wl.so To LoadModule weblogic_module modules/mod_wl_24.so
   - remove “#exit”
8. Remove this step as we will run Apache commands as WebLogic.
9. Replace with
   - sudo systemctl status httpd.service
   - sudo systemctl stop httpd.service
   - sudo systemctl start httpd.service

The following steps need to be performed on VM1 and VM2:

1. Rename the RPM default ssl.conf file to ssl.conf.orig to prevent Apache from loading during startup.
   $ sudo mv ssl.conf ssl.conf_orig

2. Modify NSS configuration:
   $ sudo vi /etc/httpd/conf.d/nss.conf
   
   a. Modify Listen parameter:
      #Listen 8443
      Listen 443

   b. Modify NSSPassPhraseDialog parameter:
      #NSSPassPhraseDialog builtin
      NSSPassPhraseDialog file:/etc/httpd/conf/password.conf
      NSSFIPS on

   c. Modify VirtualHost tag:
      #<VirtualHost _default_:8443>
      <VirtualHost _default_:443>

   d. Modify ServerName parameter:
      #ServerName www.example.com:8443
      ServerName [vm2_fqdn]:443

   e. Modify NSS logging parameters:
      #ErrorLog /etc/httpd/logs/error_log
      ErrorLog /etc/httpd/logs/nss_error_log
      TransferLog /etc/httpd/logs/nss_access_log

   f. Modify NSSProtocol parameters:
      #NSSProtocol SSLv3,TLsv1.0,TLsv1.1
      NSSProtocol TLSv1.1,TLsv1.2

   g. Modify NSSNickname parameter:
      #NSSNickname Server-Cert
      NSSNickname [proxy_fqdn]
      NSSEnforceValidCerts off

   h. Save the nss.conf file.

3. Start HTTPD server
   $ sudo service httpd start
4. Review access_log, error_log, nss_access_log and nss_error_log to ensure TLS is functioning correctly.
Install Apache Plug-in for WebLogic on VM1 and VM2

The following steps need to be performed on VM1 and VM2:

1. As your normal Linux login account, sudo su to the weblogic account:
   
   $ sudo su - weblogic

2. Create downloads directory if it doesn’t exist:
   
   $ mkdir -p /u01/downloads

3. Download Oracle WLS Plugin 12.1.3 archive (v44415-01) to the downloads directory:
   
   Download from AITC IEP eRx Downloads directory

4. Unzip the Oracle WLS Plugin 12.1.3 archive to in the downloads directory:
   
   $ unzip fmw_12_1_3_0_wls_plugin_v44415-01.zip
   $ unzip WLSPlugins12c-12.1.3.zip WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64.zip
   $ mkdir WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64
   $ unzip WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64.zip \
   -d WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64
   $ chmod -r o+rx WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64
   $ exit

5. You should be back in your normal Linux login account.

6. Copy the Apache Plug-in for WebLogic libraries to the Linux system library directory (the following must be performed by a system administrator):
   
   $ sudo cp /u01/downloads/WLSPlugin12.1.3-Apache2.2-Apache2.4-Linux_x86_64/lib/mod_* \
   /usr/lib64/httpd/modules

### 4.2.12 Configure Apache Plug-in for WebLogic on VM1

The following steps need to be performed on VM1 and VM2:

1. As your normal Linux login account, sudo su to the root account:
   
   $ sudo su -
   
   # cat > /etc/httpd/conf.d/weblogic.conf
   
   LoadModule weblogic_module modules/mod_wl.so

   `<IfModule weblogic_module>
   WebLogicCluster [vm1_fqdn]:8001, [vm2_fqdn]:8001
   MatchExpression /*
   WLEXcludePathOrMimeType /cpanel/*
   WLIOTimeoutSecs 300
   WLPproxySSL OFF
   WebLogicSSLVersion TLSv1_1 TLSv1_2
   WLSocketTimeoutSecs 2
   DebugConfigInfo ON
   </IfModule>
   <CTRL><d>
   # exit

2. You should be back in your normal Linux login account.

3. Restart Apache
   
   $ sudo service httpd stop
   $ sudo service httpd start

4. Review access_log, error_log, nss_access_log and nss_error_log to ensure Apache is functioning correctly.
4.2.13 Configure Apache Plug-in for WebLogic on VM2

The following steps need to be performed on VM1 and VM2:

1. As your normal Linux login account, sudo su to the root account:
   $ sudo su
   # cat > /etc/httpd/conf.d/weblogic.conf
   LoadModule weblogic_module modules/mod_wl.so
   LoadModule weblogic_module modules/mod_wl_24.so

   <IfModule weblogic_module>
   WebLogicCluster [vm1_fqdn]:8001, [vm2_fqdn]:8001
   MatchExpression /*
   WLEXcludePathOrMimeType /cpanel/*
   WLEXcludePathOrMimeType /inbound/*
   WLIOTimeoutSecs 300
   WLPProxySSL OFF
   WebLogicSSLVersion TLSv1_1 TLSv1_2
   WLSocketTimeoutSecs 2
   DebugConfigInfo ON
   </IfModule>
   <CTRL><d>
   # exit

2. You should be back in your normal Linux login account.

3. Restart Apache
   $ sudo service httpd stop
   $ sudo service httpd start

4. Review access_log, error_log, nss_access_log and nss_error_log to ensure Apache is functioning correctly.

4.2.14 Create IEP CPanel on VM1 and VM2

1. As your normal Linux login account, sudo su to the weblogic account:
   $ sudo su - weblogic

2. Create downloads directory if it doesn’t exist:
   $ mkdir -p /u01/deployments

3. Download the CPanel Archive (cpanel_yyyymmdd.tgz) to the deployments directory:
   Download from AITC IEP eRx Deployments directory
   $ exit

4. You should be back in your normal Linux login account.

5. Unpack the CPanel Archive from the root (/) directory:
   $ cd /
   $ sudo tar xvf /u01/deployments/cpanel_yyyymmdd.tgz
4.2.15 Install Apache SSOi Web Agent on VM1

1. Start Xming or other X Server on your Windows Desktop/Laptop. Connect to the server using Putty. The DISPLAY environment variable should be set.

2. As your normal Linux login account, sudo su to the weblogic account:
   
   ````
   $ sudo su - weblogic
   ````

3. Create downloads directory if it doesn’t exist:
   
   ````
   $ mkdir -p /u01/downloads
   ````

4. Download CA SiteMinder Apache Web Agent (smwa-12.51-cr07-linux-x86-64.zip) to the downloads directory:
   
   Download from AITC IEP eRx Downloads directory

5. Unzip the CA SiteMinder Apache Web Agent archive to in the downloads directory:
   
   ````
   $ cd /u01/downloads
   $ unzip smwa-12.51-cr07-linux-x86-64.zip -d smwa-12.51-cr07-linux-x86-64
   $ chmod o+r smwa-12.51-cr07-linux-x86-64
   $ chmod o+r smwa-12.51-cr07-linux-x86-64/layout.properties
   $ chmod ugo+rx smwa-12.51-cr07-linux-x86-64/ca-wa-12.51-cr07-linux-x86-64.bin
   $ exit
   ````

6. You should be back in your normal Linux login account.

7. Execute the CA SiteMinder Apache Web Agent installer (the following must be performed by a system administrator):
   
   ````
   $ sudo /u01/downloads/smwa-12.51-cr07-linux-x86-64/ca-wa-12.51-cr07-linux-x86-64.bin -i console
   ````

8. Press <Enter> to continue installing in Console mode:
   
   ````
   PRESS <ENTER> TO CONTINUE: <ENTER>
   ````

9. Press <Enter> many times to scroll through license agreement:
   
   ````
   PRESS <ENTER> TO CONTINUE: <ENTER>
   ````

10. Enter “Y” to accept license agreement:
    
    ````
    DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y
    ````

11. Enter installation path:
    
    ````
    ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
    ````

12. Confirm installation path:
    
    ````
    INSTALL FOLDER IS: /u01/app/webagent
    IS THIS CORRECT? (Y/N): Y
    ````

13. Confirm installation details:
    
    ````
    Please Review the Following Before Continuing:
    Product Name: CA SiteMinder Web Agent
    Install Folder: /u01/app/webagent
    Disk Space Information (for Installation Target):
    Required: 300,510,677 Bytes
    Available: 60,435,013,632 Bytes
    ````

14. Confirm exit from installer:
    
    ````
    PRESS <ENTER> TO EXIT THE INSTALLER: <ENTER>
    ```'
### 4.2.16 Configure Apache SSOi Web Agent on VM1

1. As your normal Linux login account, `sudo su` to the root account (the following must be performed by a system administrator):
   
   ```bash
   $ sudo su -
   ```

2. Change directory to the agent home and "source" the Siteminder environment:
   
   ```bash
   # cd /u01/app/CA/webagent
   # ./.ca_wa_env.sh
   ```

3. Change to install config info directory and launch the configuration wizard:
   
   ```bash
   # cd install_config_info
   # ./wa-config.sh -i console
   ```

4. Type 1 to register the trusted host, then Press Enter
   
   ->1- Yes, I would like to do Host Registration now.
   2- No, I would like to do Host Registration later.

   ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: 1

5. In the Admin User Name prompt, type threg then press Enter
   
   Enter the name of an administrator who has the right to register trusted hosts with the Policy Server.

   This entry must match the name of an administrator defined in the Policy Server.

   Admin User Name (Default: ): threg

6. For Shared Secret Rollover, type n then press Enter
   
   Enable Shared Secret Rollover (y/n) (Default: n): n

7. Type the threg password then press Enter
   
   Enter the password of an administrator who has the right to register trusted hosts with the Policy Server. This entry must match the name of an administrator defined in the Policy Server.

   Confirm Admin Password: <va1234!

8. Type the Trusted Host Name then press Enter
   
   Specify the name of the host you want to register with the Policy Server.

   Enter the name of the host configuration object. The name must match a host configuration object name already defined on the Policy Server.

   Trusted Host Name (Default: ): [proxy_fqdn]

9. Type the Host Configuration Object then press Enter
   
   Host Configuration Object (Default: ): [iam_hco]

10. Type the Policy Server IP Address then press Enter
    
    Enter the IP Address of the Policy Server where you are registering this host.

    Policy Server IP Address (Default: ): [iam_policy]
12. Press Enter twice to accept the default file name and location of Host configuration
   Host Configuration file location
   --------------------------------
   Enter file name (Default: SmHost.conf):
   Enter location (Default: /u01/app/CA/webagent/config):

13. Select 1 for Apache Web Server, then press Enter
   Select Web Server(s)
   -------------------
   1- Apache Web Server
   2- Domino Web Server
   ->3- iPlanet or Sun ONE Web Server
   ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: 1

14. Specify the path to apache instance /home/apache/httpd
   Apache Web Server path
   ----------------------
   Enter the root path of where Apache Web server installed.
   Please enter path (Default: ): /etc/httpd

15. Select the Apache version, type 3 then press Enter
   Apache Version
   ---------------
   Please select a choice for the Apache version.
   1- Apache version 1.x
   2- Apache version 2.x
   3- Apache version 2.2.x
   4- Apache version 2.4.x
   ENTER THE NUMBER OF THE DESIRED CHOICE: 4

16. Select the Apache Type, type 6 then press Enter
   Apache Server Type
   -------------------
   Please select one of the following appropriately match your previous selection
   1- Oracle HTTP Server
   2- IBM HTTP Server
   3- HP Apache
   4- ASF/RedHat Apache
   5- RedHat JWS HTTP Server
   ENTER THE NUMBER OF THE DESIRED CHOICE: 4

17. Type 1 to confirm the Apache version
   Select Web Server(s)
Select the web server(s) you wish to preserve or configure/reconfigure as Web Agent(s). Enter a comma-separated list of numbers representing the desired choices. Already configured web servers are marked as [x] in the above list, you can un-configure or skip these web servers in next steps by not listing them in comma-separated list here.: 1

18. Type the Agent Configuration Object, then press Enter
Agent Configuration Object
--------------------------
Enter the name of an Agent Configuration Object that defines the configuration parameters which the Web Agent will use for Apache 2.2.15.
Agent Configuration Object (Default: AgentObj): PREAgentConfig

19. To select Basic over SSL Authentication, Type 1 then press Enter
SSL Authentication
------------------
The following SSL configurations are available for this web server. If the Web Agent will be providing advanced authentication, select which configuration it will use to configure Apache 2.2.15.

>1- HTTP Basic over SSL
2- X509 Client Certificate
3- X509 Client Certificate and HTTP Basic
4- X509 Client Certificate or HTTP Basic
5- X509 Client Certificate or Form
6- X509 Client Certificate and Form
7- No advanced authentication

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 1

20. Type 1 on the Webagent Enable prompt then press Enter
Webagent Enable option
-----------------------
Please select Yes to Enable the WebAgent

1- Yes

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 1

21. On the Summary Screen, Type 1 then press Enter
Web Server Configuration Summary
--------------------------------
Please confirm the configuration selection. Accept the configuration and press 'Enter' to continue. To change one or more settings, select 'Previous'. Select 'Cancel' will exit the configuration.

Configure the following webserver(s):
Apache Server:
Apache 2.2.15
Agent Configuration Object: PREAgentConfig
SSL Authentication type: HTTP Basic over SSL

IS WebAgent Enabled: YES

Please enter a choice.
->1- Continue
2- Previous
3- Cancel

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: 1

22. Continue installation if ssl.conf file doesn’t exist:
   1- Continue
   2- Exit

   Unable to process configuration. File /etc/httpd/conf.d/ssl.conf doesn't exist. Please make sure the configuration path is valid.
   Please select a choice.: 1

23. Confirm exit from installer:
   PRESS <ENTER> TO EXIT THE INSTALLER: <ENTER>

24. Enter “exit” to log out of root account:
   # exit

25. You should be back in your normal Linux login account.

4.2.17 Post Configure Edits for Apache SSOi Web Agent on VM1

1. As your normal Linux login account, sudo su to the root account:
   $ sudo su -

2. Edit /u01/app/CA/webagent/config/SmHost.conf:
   vi /u01/app/CA/webagent/config/SmHost.conf

3. Verify policyserver entries:
   # Add additional bootstrap policy servers here for fault tolerance.
   [iam_policy_servers]

4. Edit /etc/httpd/conf/WebAgent.conf:
   vi /etc/httpd/conf/WebAgent.conf

5. Enable the agent:
   EnableWebAgent="YES"

6. For an embedded Apache web server (included by default) on a RedHat Linux system, modify certain configuration files to accommodate the product first. Follow these steps:
   cp /etc/sysconfig/httpd /etc/sysconfig/httpd.orig
   vi /etc/sysconfig/httpd
   Add the following line to the end of the file:
   PATH=$PATH:web_agent_home/bin
   Save the changes and close the text editor.

7. Source ca_wa_env.sh script in the following file (instead of starting it manually each time):
   cp /etc/init.d/httpd /etc/init.d/httpd.orig
   vi /etc/init.d/httpd
   Add the following code snippet after the similar snippet for /etc/sysconfig/httpd
   # Source CA Webagent environment
   if [ -f /u01/app/CA/webagent/ca_wa_env.sh ]; then
     . /u01/app/CA/webagent/ca_wa_env.sh
   fi
8. **Modify the apachectl script to set the webagent environment variables:**

   ```
   cp /usr/sbin/apachectl /usr/sbin/apachectl.orig
   vi /usr/sbin/apachectl
   
   Locate a line resembling the following example:
   # Source /etc/sysconfig/httpd for $HTTPD setting, etc

   Add the following code snippet after the similar snippet for /etc/sysconfig/httpd:
   # Source CA Webagent environment
   if [ -r /u01/app/CA/webagent/ca_wa_env.sh ]; then
     . /u01/app/CA/webagent/ca_wa_env.sh
   fi
   ```

9. **Modify permission of CA SmHost.conf file**

   ```
   chmod 666 /u01/app/CA/webagent/config/SmConf.conf
   ```

10. **Create /opt/ca/webagent symbolic link**

    ```
    # mkdir /opt/ca
    # chmod 755 /opt/ca
    # ln -s /u01/app/CA/webagent/ /opt/ca/webagent
    ```

11. **Modify ownership and permission of CA Webagent log files**

    ```
    # chown apache:apache /u01/app/CA/webagent/log
    # chmod 777 /u01/app/CA/webagent/log
    ```

12. **Modify trace file verbosity**

    Modify SSOi WebAgent trace.conf file:
    ```
    # cd /opt/ca/webagent/config
    # vi trace.conf
    
    Modify lines near the bottom per the following:
    nete.enableConsoleLog=0
    nete.enableFileLog=0
    nete.logFile=0

    nete.conapi.logLevel=0
    nete.conapi.ipc.logLevel=0
    nete.conapi.tcpip.logLevel=0

    nete.mon.monitoringApiLogLevel=0
    ```

    Modify SSOi WebAgent WebAgentTrace.conf file:
    ```
    # vi WebAgentTrace.conf
    
    Modify lines near the bottom to be:
    components: WebAgent
    data: Date, Time, Pid, Function, TransactionID, User, Message
    ```

13. **Modify sysctl for Apache on RHEL 7.**

    **From:** Ratcliff, Mark E. (SMS)
    **Sent:** Wednesday, May 16, 2018 7:45 PM
    **To:** Combs, Marvin; OIT ITOPS SO IO EIS LT6 Linux Sys Admins
    **Cc:** Bratcher, Jay L. (SMS)
    **Subject:** RE: siteminder busted

    Hi,

    This is one fix for this (with some help from google). To keep apache updates from breaking this in the future, an override file needs to be created with a systemd command:

    ```
    dzdo systemctl edit httpd.service
    ```

    This will open a text file to edit. Drop in the following:
[Service]
ExecStart=
ExecReload=

ExecStart=/bin/bash -a -c 'source /u01/CA/webagent/ca_wa_env.sh && exec /usr/sbin/httpd $OPTIONS -DFOREGROUND'
ExecReload=/bin/bash -a -c 'source /u01/CA/webagent/ca_wa_env.sh && exec /usr/sbin/httpd $OPTIONS -k graceful'

Close and save. This will create /etc/systemd/system/httpd.service.d/override.conf.

Do a reload:
dzdo systemctl daemon-reload

httpd should come up with a normal start command. If there is a “file not found” error then “ca_wa_env.sh” may be in a different spot. These files seem to get installed in different spots across different systems. You can just run a find command to look for it, “dzdo find / -name ‘ca_wa_env.sh’”. If that one is not found it may also be named “set-apache-env.sh”. Update override.conf with the correct path then do another daemon-reload. Should be working after that.
I believe some projects used this exact approach to fix their apache installs but I was not able to recall what servers were fixed doing it this way.

Cheers!

Mark Ratcliff (Contractor)
Linux Systems Administrator – KGS
Service Operations - Infrastructure Operations
Office of Information and Technology, IT Operations and Services
Office: 512-326-6674
GFE Mobile: 512-820-7125

14. Restart Apache and check the logs for connection or errors.
   # exit
   $ sudo service httpd stop
   $ sudo service httpd start

4.3 Download and Extract Files
This section is not applicable to this guide.

4.4 Database Creation
This section is not applicable to this guide.

4.5 Installation Scripts
This section is not applicable to this guide.

4.6 Cron Scripts
This section is not applicable to this guide.
4.7 Access Requirements and Skills Needed for the Installation

This section is not applicable to this guide.

4.8 Installation Procedure

This section provides step-by-step instructions for installing all components of the Inbound eRx software on all platforms.

4.8.1 WebLogic Installation

The following subsections describe the steps to install the WebLogic application server. Most activities are to be performed by the WebLogic Administrator.

4.8.1.1 Install WebLogic

1. As your normal Linux login account, sudo su to the weblogic account:
   
   ```
   $ sudo su - weblogic
   ```

2. Modify the weblogic Linux account .bash_profile, replace the PATH= and export PATH with the following near the end of the file:
   
   ```
   export JAVA_HOME=/u01/app/java/latest
   export PATH=${JAVA_HOME}/bin:${PATH}:${HOME}/bin
   ```

3. Exit weblogic account:
   
   ```
   $ exit
   ```

4. Start Xming or other X Server on your Windows Desktop/Laptop. Connect to the server using Putty. The DISPLAY environment variable should be set.

5. As your normal Linux login account, modify your .Xauthority permissions:
   
   ```
   $ chmod 755 ~
   $ chmod 644 ~/.Xauthority
   ```

6. As your normal Linux login account, sudo su to the weblogic account:
   
   ```
   $ sudo su - weblogic
   ```

7. Copy the .Xauthority file from your normal Linux account to the current account:
   
   ```
   $ cp ~yourusername/.Xauthority .
   ```

8. Create downloads directory if it doesn’t exist:
   
   ```
   $ mkdir -p /u01/downloads
   ```

9. Download Oracle WLS 12.1.3 installer (v44413-01) to the downloads directory:
   
   ```
   Download from AITC IEP eRx Downloads directory
   ```

10. Unzip the Oracle WLS 12.1.3 installer to the downloads directory:
    
    ```
    $ unzip fmw_12.1.3.0.0_wls_v44413-01.zip
    ```

11. Run the Oracle WLS 12.1.3 installer:
    
    ```
    $ java -jar fmw_12.1.3.0.0_wls.jar
    ```

12. Enter “y” to accept prerequisite checks.
13. Enter “/u01/app/oraInventory”.
14. Click OK.
15. The Oracle Universal Installer will appear for a few moments.

**Figure 4: Install WebLogic – Oracle Universal Installer Dialog Box**
16. Once the installer is complete, click **Next**.

**Figure 5: Install WebLogic – Oracle Fusion Middleware WebLogic Server and Coherence Installer Screen**
17. Enter Oracle Home: “[ORACLE_BASE]”.
18. Click Next.

Figure 6: Install WebLogic – Installation Location
19. For *Installation Type*, select the *WebLogic Server* radio button.

20. Click **Next**.

*Figure 7: Install WebLogic – Installation Type*
21. Click Next again on the **Prerequisite Checks** screen.

**Figure 8: Install WebLogic – Prerequisite Checks**

22. On the Security Updates screen, leave the *Email* field blank.
23. Uncheck “I wish to receive security updates via My Oracle Support”.
24. Click Next.

**Figure 9: Install WebLogic – Security Updates Screen**
25. Click Yes to acknowledge not receiving critical security issues notifications.

   **Figure 10: Install WebLogic – My Oracle Support Username/Email Address Not Specified Dialog Box**

   ![My Oracle Support Username/Email Address Not Specified Dialog Box](image)


   **Figure 11: Install WebLogic – Installation Summary Screen**

   ![Installation Summary Screen](image)

27. Wait while the installation progresses.
28. Once the installation is complete, the following screen will display.
29. Click **Next**.

**Figure 12: Install WebLogic – Installation Progress Screen**

30. On the **Installation Complete** screen, leave **Automatically Launch the Configuration Wizard** checked.
31. Click **Finish**.

**Figure 13: Install WebLogic – Installation Complete**
32. The Oracle **Configuration Wizard** splash screen will appear for a few moments. 

**Figure 14: Install WebLogic – Oracle Configuration Wizard Splash Screen**

33. On the **Configuration Type** screen, select *Create a new domain.*

34. Enter the following in the **Domain Location:**

   \[
   [\text{ORACLE\_BASE}]/\text{user\_projects}/\text{domains}/[\text{domain}]
   \]

35. Click **Next.**

**Figure 15: Install WebLogic – Create New Domain**
36. On the **Templates** screen, select the **Create Domain using Product Templates** radio button.

37. Under **Available Templates**, select “Basic WebLogic Server Domain”.

38. Click **Next**.

*Figure 16: Install WebLogic – Templates Screen*
39. On the **Administrator Account** screen, enter *Name*: “weblogic”
40. Enter *Password*: “##########”
41. Enter *Confirm Password*: “##########”
42. Click **Next**.

**Figure 17: Install WebLogic – Administrator Account Screen**

43. On the **Domain Mode and JDK** screen, select the *Development* radio button for the *Domain Mode*.
44. For *JDK*, select the *Oracle HotSpot 1.8.0_xxx* radio button.
45. Click **Next**.

**Figure 18: Install WebLogic - Domain Mode and JDK**
46. On the **Advanced Configuration** screen, check *Administration Server, Node Manager, and Managed Servers, Clusters and Coherence*.

47. Click **Next**.

**Figure 19: Install WebLogic– Advanced Configuration**
48. On the **Administration Server** screen, enter *Server Name*: “AdminServer”
49. Enter *Listen Address*: “All Local Addresses”
50. Enter *Listen Port*: “7001”
51. Uncheck the check box for *Enable SSL*.
52. Leave the *SSL Listen Port* field blank.
53. Click **Next**.

**Figure 20: Install WebLogic – Administration Server Screen**
54. On the **Node Manager** screen, select the *Per Domain Default Location* radio button.
55. Enter **Username**: “weblogic”
56. Enter **Password**: “##########”
57. Enter **Confirm Password**: “##########”
58. Click Next.

**Figure 21: Install WebLogic – Node Manager**

![Node Manager Configuration Screen]

- **Node Manager Type**
  - Per Domain Default Location
  - Per Domain Custom Location
  - Manual Node Manager Setup

- **Node Manager Home**: `node_home/user_projects/domains/erdoman1/node_manager` [Browse]

- **Node Manager Credentials**
  - **Username**: weblogic
  - **Password**: *******
  - **Confirm Password**: *******

Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.
59. On the **Managed Servers** screen, click **Add**.
60. Enter the **Server Name**: “erx1”
61. Enter the **Listen Address**: \[vm1\_fqdn\]
62. Enter **Listen Port**: “8001”
63. Leave **Enable SSL** unchecked.
64. Leave **SSL Listen Port** empty (Disabled).
65. Click **Add**.
66. Enter **Server Name**: “erx2”
67. Enter **Listen Address**: \[vm2\_fqdn\]
68. Enter **Listen Port**: “8001”
69. Leave **Enable SSL** unchecked.
70. Leave **SSL Listen Port** empty (Disabled).
71. Click **Next**.

**Figure 22: Install WebLogic – Managed Servers**

![Managed Servers Screen](image-url)
72. On the **Clusters** screen, click **Add**.
73. Enter **Cluster Name**: “erx”
74. Enter **Cluster Address**: “[vm1 fqdn]:[erx_port], [vm2 fqdn]:[erx_port]”
75. Enter **Frontend Host**: “[proxy fqdn]”
76. Enter **Frontend HTTP Port**: “80”
77. Enter **Frontend HTTPS**: “443”
78. Click **Next**.

**Figure 23: Install WebLogic – Clusters**

![Clusters Configuration Wizard](image)

<table>
<thead>
<tr>
<th>Cluster Name</th>
<th>Cluster Address</th>
<th>Frontend Host</th>
<th>Frontend HTTP Port</th>
<th>Frontend HTTPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev1</td>
<td>wwwuserappdev1.</td>
<td>wwwuserappdev1.</td>
<td>80</td>
<td>443</td>
</tr>
</tbody>
</table>
79. Assign “erx1” and “erx2” servers to the “erx” cluster.

80. Click Next.

**Figure 24: Install WebLogic – Assign Servers to Clusters**

81. Click Add.

82. Enter Name: “machine1”

83. Enter Node Manager Listen Address: “[vm1_fqdn]”

84. Enter Node Manager Listen Port: “5556”

85. Enter Name: “machine2”

86. Enter Node Manager Listen Address: “[vm1_fqdn]”

87. Enter Node Manager Listen Port: “5556”

88. Click Next.

**Figure 25: Install WebLogic – Machines**
89. On the **Assign Servers to Machines** screen, add “AdminServer” on **Servers** panel to “machine1” on **Machines** panel.

90. Add “erx1” on **Servers** panel to “machine1” on **Machines** panel.

91. Add “erx2” on **Servers** panel to “machine2” on **Machines** panel.

92. Click **Next**.

**Figure 26: Install WebLogic – Assign Servers to Machines**

Select one or more servers in the left pane and one machine in the right pane. Then use the right arrow button (>) to assign the server(s) to the machine.
93. On the **Configuration Summary** screen, click **Create** to accept the options and start creating and configuring the new domain.

**Figure 27: Install WebLogic – Configuration Summary Screen**

94. Once the configuration is complete, click **Next**.
95. If the configuration is successful, the **Configuration Success** screen will display as illustrated in the figure below.

96. Click **Finish**.

**Figure 28: Install WebLogic - Configuration Success**

97. The Oracle WebLogic Server 12.1.3 installation and configuration should be complete at this time. To modify the configuration, re-run the configuration wizard:

   ```
   $ cd [ORACLE_BASE]/oracle_common/common/bin
   $ ./config.sh
   ```

98. Modify the configuration as needed.
4.8.1.2  Set Temporary Environment on VM1

On VM1, set temporary environment. Remember to amend the DOMAIN_HOME environment variable to match your domain:

$ export ORACLE_BASE=$[ORACLE_BASE]
$ export WLS_HOME=$ORACLE_BASE/wlserver
$ export DOMAIN_HOME=$ORACLE_BASE/user_projects/domains/[domain]

4.8.1.3  Create a Domain Boot Identity File on VM1

On VM1, create a boot identity file for the domain if it doesn’t exist:

$ mkdir -p $DOMAIN_HOME/servers/AdminServer/security
$ cat > $DOMAIN_HOME/servers/AdminServer/security/boot.properties
username=weblogic
password=#########
<ctrl>d

4.8.1.4  Copy Identity/Trust Store Files on VM1

Copy the server identity key store to the WebLogic domain “security” directory on VM1:

$ cp /u01/certificates/[proxy_fqdn].jks $DOMAIN_HOME/security/[proxy_fqdn].jks

4.8.1.5  Configure nodemanager Identity/Trust Store on VM1

On VM1, edit nodemanager.properties to add identity/trust store configuration:

$ cd $DOMAIN_HOME/nodemanager
$ cp nodemanager.properties nodemanager_orig.properties
$ vi nodemanager.properties

Add the following lines at the end of the file:

KeyStores=CustomIdentityAndCustomTrust
CustomIdentityAlias=[proxy_fqdn]
CustomIdentityKeyStoreFileName=$[DOMAIN_HOME]/security/[proxy_fqdn].jks
CustomIdentityKeyStorePassPhrase=[keystore_passphrase]
CustomIdentityKeyStoreType=JKS
CustomIdentityPrivateKeyPassPhrase=[privatekey_passphrase]

Enter :wq to save the file and exit vi.

4.8.1.6  Configure TLS on VM1

On VM1, edit startManagedWeblogic.sh to modify TLS configuration:

$ cd $DOMAIN_HOME/bin
$ cp startWeblogic.sh startWeblogic_orig.sh
$ vi startWeblogic.sh

Modify the the JAVA_OPTIONS as follows:

JAVA_OPTIONS="$SAVE_JAVA_OPTIONS -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.1"

Enter :wq to save the file and exit vi.

4.8.1.7  Copy Identity/Trust Store Files on VM2

Copy the server identity key store to the WebLogic domain “security” directory on VM1:

$ cp /u01/certificates/[proxy_fqdn].jks $DOMAIN_HOME/security/[proxy_fqdn].jks
4.8.1.8 Configure nodemanager Identity/Trust Store on VM2

On VM1, edit nodemanager.properties to add identity/trust store configuration:

```
$ cd $DOMAIN_HOME/nodemanager
$ cp nodemanager.properties nodemanager_orig.properties
$ vi nodemanager.properties
```

Add the following lines at the end of the file:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityAlias=[proxy_fqdn]
CustomIdentityKeyStoreFileName=[DOMAIN_HOME]/security/[proxy_fqdn].jks
CustomIdentityKeyStorePassPhrase=[keystore_passphrase]
CustomIdentityKeyType=JKS
CustomIdentityPrivateKeyPassPhrase=[privatekey_passphrase]
```

Enter :wq to save the file and exit vi.

4.8.1.9 Disable basic authentication

On VM1, edit config.xml to disable basic authentication:

```
$ cd $DOMAIN_HOME/config.xml
$ cp config.xml config_orig.xml
$ vi config.xml
```

Add the following line before the end tag </security-configuration>:

```
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
```

Enter :wq to save the file and exit vi.

4.8.1.10 Configure JPA for Domain on VM1

On VM1, edit setDomainEnv.sh script to add JPA modules via PRE_CLASSPATH:

```
$ cd $DOMAIN_HOME/bin
$ cp setDomainEnv.sh setDomainEnv_orig.sh
$ vi setDomainEnv.sh
```

Add the following two lines after the first line in the script:

```
PRE_CLASSPATH=[ORACLE_BASE]/oracle_common/modules/javax.persistence_2.1.jar:[WLS_HOME]/modules/com.oracle.weblogic.jpa21support_1.0.0.0_2-1.jar
export PRE_CLASSPATH
```

Enter :wq to save the file and exit vi.
4.8.1.11 Create Inbound eRx Datasource

This section provides step-by-step instructions for deploying VistA Link Connector.

1. Navigate to Services > Data Sources.
2. From the Data Sources page, click New.

Figure 29: Create Inbound eRx Datasource – Datasources
3. Enter **Name**: “InboundErxDataSource”
4. Enter **JNDI Name**: “jdbc/InboundErxDataSource”
5. Select **Database Type**: “Oracle”
6. Click **Next**.

**Figure 30: Create Inbound eRx Datasource – Datasource Properties**

7. Select **Database Driver**: “Oracle’s Driver (Thin XA) for Instance connections; Versions: Any”
8. Click **Next**.

**Figure 31: Create Inbound eRx Datasource – Database Driver**
9. Click Next.

**Figure 32: Create Inbound eRx Datasource – Transaction Properties**

![WebLogic Server Administration Console 12c](image)

Change Center

View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Domain Structure

- **environ1**
  - Environment
  - Deployments
  - Services
    - Messaging
      - Data Sources
        - Persistent Stores
        - Foreign JDBC Providers
      - Work Contexts
      - XML Registries
      - XML Entity Caches
      - JMS
      - JPA Sessions

Create a New JDBC Data Source

Transaction Options

You have selected an XA JDBC driver to use to create database connection in your new data source. The data source will support global transactions and use the 'Two-Phase Commit' global transaction protocol. No other transaction configuration options are available.
10. Enter Database Name: “[DB_NAME]”
11. Enter Host Name: “[DB_FQDN]”
12. Enter JNDI Name: “jdbc/InboundErxDataSource”
13. Enter Port: “[DB_PORT]”
14. Enter Password: “[DB_PASSWORD]”
15. Enter Confirm Password: “[DB_PASSWORD]”

Figure 33: Create Inbound eRx Datasource – Connection Properties
16. Click the “Test Configuration” button
17. If test is not successful, Click “Back” button and correct settings, otherwise click “Next”

Figure 34: Create Inbound eRx Datasource – Test Connection
18. Select “All servers in the cluster”
19. Click “Finish” button.

Figure 35: Create Inbound eRx Datasource – Select Targets/Finish

20. Select “InboundErxDatasource” hyperlink

Figure 36: Create Inbound eRx Datasource – Modify New Datasource
21. Select “Connection Pool” tab

**Figure 37: Inbound eRx Datasource – Connection Pool Properties**

22. Scroll to the bottom of the “Connection Pool” page

23. Select “Advanced” hyperlink to expand the advanced properties

**Figure 38: Inbound eRx Datasource – Connection Pool Advanced Properties**
24. Scroll down and uncheck the “Wrap Data Types” property

Figure 39: Inbound eRx Datasource – Wrap Data Type Property

25. Scroll to the bottom of the “Advanced Connection Pool” page

26. Click the “Save” button

Figure 40: Inbound eRx Datasource – Save Properties
4.8.1.12 Configure Identity/Trust Store File on Managed Servers

This section provides step-by-step instructions for configuring the identify/trust store file on the managed servers.

1. Under Domain Structure, navigate to Servers.
2. Click on the “erx1” link to access the server configuration page in the Administration Console.

Figure 41: Configure Identity/Trust Store File – Access Server Configuration Page
3. Under Configuration > Keystores, click Change.

   Figure 42: Configure Identity/Trust Store File – Change Keystores

4. For Keystores, select “Custom Identity and Custom Trust”.

5. Click Save.

   Figure 43: Configure Identity/Trust Store File – Keystores – Select Custom Identify and Custom Trust
6. Modify the setting under the **Keystores** tab as illustrated in the figure below. The *Custom Identity Keystore* and *Custom Trust Keystore* use the same file path to the keystore file copied to the Domain “security” directory: ([DOMIAN_HOME]/security/[proxy_fqdn].jks).

**Figure 44: Configure Identity/Trust Store File – Modify Keystore Settings**
7. Modify the setting under the **SSL** tab as illustrated in the figure below. For the *Private Key Alias*, enter “*proxy fqdn*”.

8. Enter and confirm the *Private Key Passphrase*.

9. Click **Save**.

   **Figure 45: Configure Identity/Trust Store File – Modify SSL Settings**
10. Navigate to *Servers*, and then click on the “erx2” link to access the server configuration page in the *Administration Console*.

11. Repeat the Keystore configuration steps for “erx2” as described earlier in this section for “erx1”.

   **Figure 46: Configure Identity/Trust Store File – Managed Server 2 Configuration**

![Configure Identity/Trust Store File – Managed Server 2 Configuration](image)

12. Navigate to *Servers*, and then click on the “AdminServer(admin)” hyperlink to access the server configuration page.

13. Repeat the Keystore configuration steps for “AdminServer(admin)” as described earlier in this section for “erx1”.

   **Figure 47: Configure Identity/Trust Store File – Admin Server Configuration**

![Configure Identity/Trust Store File – Admin Server Configuration](image)
14. Navigate to **Servers**, and then click on the “AdminServer(admin)” hyperlink to access the server configuration page.

**Figure 48: Configure Identity/Trust Store File – Admin Server Configuration**
15. Under “Configuration” > “general” tabs:
   Check “Listen Port Enabled”
   Enter “Listen Port”: 7001
   Check “SSL Port Enabled”
   Enter “SSL Listen Port”: 7002
   Click “Save” button.

Figure 49: Configure Identity/Trust Store File – Admin Server Configuration
4.8.1.13 Pack Domain on VM1

This section provides step-by-step instructions for packing the domain on VM1:

1. On VM1, stop the newly created domain.
2. In the session that is currently running “startWebLogic.sh”, enter <CTRL> C.
3. The log messages should indicate that the Admin Server “was shut down”.

**NOTE:** It may seem odd that we are immediately stopping the new domain, but some of the configuration is not written to the file system until the AdminServer is started for the first time.

4. We will transfer the relevant configuration using the pack and unpack utilities.
5. On VM1, pack the domain configuration using the following commands. Remember to amend the DOMAIN_HOME environment variable and the -template_name parameter to match your domain.

   ```
   $ mkdir /u01/templates
   $ chmod 777 /u01/templates
   $ $WLS_HOME/common/bin/pack.sh -managed=true -domain=$DOMAIN_HOME -template=/u01/templates/erxdomain1_template.jar -template_name=[domain] -log=/u01/templates/[domain]_template_pack.log
   ```

6. Copy the resulting jar file to VM2 under:

   ```
   /u01/templates
   ```

4.8.1.14 Unpack Domain on VM2

On VM2, set temporary environment. Remember to amend the DOMAIN_HOME environment variable to match your domain:

```
$ export ORACLE_BASE=[ORACLE_BASE]
$ export WLS_HOME=$ORACLE_BASE/wlserver
$ export DOMAIN_HOME=$ORACLE_BASE/user_projects/domains/[domain]
```

Unpack the configuration on VM2. Remember to amend the DOMAIN_HOME environment variable to match your domain.

```
$ $WLS_HOME/common/bin/unpack.sh -domain=$DOMAIN_HOME -template=/u01/templates/[domain]_template.jar -template_pack.log=/u01/templates/[domain]_template_unpack.log
```

4.8.1.15 Copy Identity/Trust Store Files on VM2

Copy the server identity key store to the WebLogic domain “security” directory on VM2:

```
$ cp /u01/certificates/[proxy_fqdn].jks $DOMAIN_HOME/security/[proxy_fqdn].jks
```

4.8.1.16 Enroll VM2

1. On VM1, restart the domain. Wait until it is fully started before continuing.

   ```
   $ nohup $DOMAIN_HOME/bin/startWebLogic.sh 2>&1 $DOMAIN_HOME.servers/AdminServer/logs/AdminServer.out &
   ```

2. On VM2, start WLST.

   ```
   $ $WLS_HOME/common/bin/wlst.sh
   ```

3. Connect to the administration server on VM1, enroll VM2, disconnect and exit WLST. Remember to amend the DOMAIN_HOME environment variable to match your domain.
4. Check the “$ORACLE_BASE/domain-registry.xml” file contains an entry like the following. If it doesn’t, add it manually.
   <domain location=""/>

5. Check the “$DOMAIN_HOME/nodemanager/nodemanager.domains” file contains an entry like the following. If it doesn’t, add it manually.
   erxdomain1=DOMAIN_HOME

6. If the node manager is not already started on this server, start it now.
   $ nohup $DOMAIN_HOME/bin/startNodeManager.sh &

4.8.1.17 Check Node Manager on Each WebLogic Machine
This section outlines the steps for checking that the node manager is reachable on each WebLogic machine.

1. Log in to the administration server (http://[vm1_fqdn]:7001/console).
2. In the Domain Structure tree, expand the Environment node and then click on the Machines node.
3. In the right-hand pane, click on the first WebLogic machine (machine1).
4. Select the Monitoring tab. Be patient. This may take some time the first time you do it.
5. If the status is “Reachable”, everything is fine.
6. Repeat for the second WebLogic machine (machine2).

4.8.1.18 Create a Boot Identity File for Managed Servers

NOTE: This is a placeholder step that may be eliminated if the boot identity file is automatically copied over during the domain clone process.

On VM2, create a boot identity file for the domain if it doesn’t exist:

   $ mkdir -p $DOMAIN_HOME/servers/AdminServer/security
   $ cat > $DOMAIN_HOME/servers/AdminServer/security/boot.properties
   username=weblogic
   password=########
   <ctrl>d

NOTE: The above username and password will be encoded/encrypted after the first shutdown/startup cycle.

4.8.1.19 Deploy Test Application
This section outlines the steps for deploying the test application.

1. Start the node manager on all servers.
2. Create the deployments directory if it doesn’t exist:
   $ mkdir -p /u01/deployments
3. Copy test application to the deployments directory:
   $ cp /u01/downloads/benefits.war /u01/deployments
4. Navigate to the Deployments page.

**Figure 50: Deploy Test Application: Deployments Page**

![Deployments Page](image)

5. From the Deployments page, click Install.

**Figure 51: Deploy Test Application – Install**

![Install Page](image)
6. Install a new deployment of the test application using the WAR file as indicated in the figure below.

7. Click Next.

   Figure 52: Deploy Test Application – WAR File

8. Accept the defaults for an application deployment. (The Install this deployment as an application radio button is marked.)

9. Click Next.

   Figure 53: Deploy Test Application – Accept Default Application Deployment
10. Select the *All servers in the cluster* option under the “erx” cluster as the target for the deployment.
11. Click Next.

![Figure 54: Deploy Test Application – Select Deployment Target](image)
12. All of the values should appear as illustrated in the figure below.

13. Click **Next**.

**Figure 55: Deploy Test Application – Verify Deployment Settings**
14. Verify that all of the values appear as illustrated in the figure below.

15. Click **Finish**.

**Figure 56: Deploy Test Application – Verify Deployment Settings (Finish)**
16. The **Overview** tab should appear as illustrated in the figure below.

**Figure 57: Deploy Test Application – Verify “benefits” Settings**
17. Navigate to the **Servers** page in the WebLogic console.
18. Select the **Control** tab.
19. Select “erx1” and “erx2” servers.
20. Click **Start**.

**Figure 58: Deploy Test Application – Summary of Servers Table**

21. After a couple minutes, the state on the servers will change to “RUNNING”.

**Figure 59: Deploy Test Application – Servers Running**
22. Open a web browser to http://[vm1_fqdn]/benefits/.
23. The Dizzyworld Benefits application will display.

**Figure 60: Deploy Test Application – Open Dizzyworld Benefits Application**

![Welcome To Dizzyworld](image)

24. Repeat Steps 22 and 23 with a Web browser pointed to http://[vm2_fqdn]/benefits/.
25. Repeat Steps 22 and 23 with a Web browser pointed to https://[proxy_fqdn]/benefits/.
26. Navigate to the **Servers** page in the WebLogic console.
27. Select the **Control** tab.
28. Select “erx1” and “erx2” servers.
29. Click **Shutdown**.

**Figure 61: Deploy Test Application – Shutdown Servers**

![Shutdown Servers](image)
4.8.1.20 Configure JPA for Domain on VM2

On VM2, edit setDomainEnv.sh script to add JPA modules via PRE_CLASSPATH:

```bash
$ cd $DOMAIN_HOME/bin
$ cp setDomainEnv.sh setDomainEnv_orig.sh
$ vi setDomainEnv.sh
```

Add the following two lines after the first line in the script:

```
PRE_CLASSPATH=[$ORACLE_BASE]/oracl
```

```
e_common/modules/javax.persistence_2.1.jar:$WLS_HOME/modules/com.oracle.weblogic.jpa21support_1.0.0.0_2-1.jar
```

export PRE_CLASSPATH

Enter :wq to save the file and exit vi.

4.8.1.21 Install VistALink on VM1

This section outlines the steps for installing VistALink on VM1:

1. As your normal Linux login account, sudo su to the weblogic account:
   ```bash
   $ sudo su -weblogic
   ```
2. Create downloads directory if it doesn’t exist:
   ```bash
   $ mkdir -p /u01/downloads
   ```
3. Download vljConnector-1.5.0.028.jar, vljFoundationsLib-1.6.0.28.jar, log4j-1.2.17.jar and COMMON_vistalink_config_YYYYMMDD.zip to the downloads directory:
   Download from AITC IEP eRx Downloads directory
4. Create Deployments/VistaLink directory if it doesn’t exist:
   ```bash
   $ mkdir -p /u01/downloads/vistalink
   ```
5. Download COMMON_vistalink_config_YYYYMMDD.zip to the Deployments/VistaLink directory:
   Download from AITC IEP eRx Deployments/VistaLink directory
6. Unpack COMMON_vistalink_config_YYYYMMDD.zip file into DOMAIN_HOME:
   ```bash
   $ cd $DOMAIN_HOME
   $ unzip /u01/deployments/vistalink/COMMON_vistalink_config_YYYYMMDD.zip
   ```
7. Modify configureVistaLink.sh (Production environment only):
   ```bash
   $ vi $DOMAIN_HOME/bin/startWeblogic.sh
   ```
   Add the following line to the bottom of the file:
   ```bash
   export JAVA_OPTIONS="${JAVA_OPTIONS} -Dgov.va.med.environment.production=true"
   ```
8. Modify the Domain Startup script (startWebLogic.sh):
   ```bash
   $ vi $DOMAIN_HOME/bin/startWeblogic.sh
   ```
9. Add call to configureVistaLink.sh after the setDomainEnv.sh call as shown:
   ```bash
   . ${DOMAIN_HOME}/bin/setDomainEnv.sh $*
   . ${DOMAIN_HOME}/bin/configureVistaLink.sh $*
   ```
10. Modify the nodemanager.properties file:
    ```bash
        $ vi $DOMAIN_HOME/nodemanager/nodemanager.properties
        StartScriptEnabled=true
    ```
4.8.1.22 Configure VistALink on VM1

1. Create Deployments/VistaLink directory if it doesn’t exist:
   
   ```
   $ mkdir -p /u01/downloads/vistalink
   ```

2. Download VistALink configuration zip file for the environment:
   
   Download from AITC IEP eRx Deployments/VistaLink directory

3. Unzip VistALink configuration files for the environment:
   
   ```
   $ cd $DOMAIN_HOME
   $ unzip /u01/deployments/vistalink/[ENV]_vistalink_config_YYYYMMDD.zip
   ```

4.8.1.23 Install VistALink on VM2

This section outlines the steps for installing VistALink on VM2:

1. As your normal Linux login account, sudo su to the weblogic account:
   
   ```
   $ sudo su - weblogic
   ```

2. Create downloads directory if it doesn’t exist:
   
   ```
   $ mkdir -p /u01/downloads
   ```

3. Download vljConnector-1.5.0.028.jar, vljFoundationsLib-1.6.0.28.jar, log4j-1.2.17.jar and COMMON_vistalink_config_YYYYMMDD.zip to the downloads directory:
   
   Download from AITC IEP eRx Downloads directory

4. Create Deployments/VistaLink directory if it doesn’t exist:
   
   ```
   $ mkdir -p /u01/downloads/vistalink
   ```

5. Download COMMON_vistalink_config_YYYYMMDD.zip to the Deployments/VistaLink directory:
   
   Download from AITC IEP eRx Deployments/VistaLink directory

6. Unpack COMMON_vistalink_config_YYYYMMDD.zip file into DOMAIN_HOME:
   
   ```
   $ cd $DOMAIN_HOME
   $ unzip /u01/deployments/vistalink/COMMON_vistalink_config_YYYYMMDD.zip
   ```

7. Modify configureVistaLink.sh (Production environment only):
   
   ```
   $ vi $DOMAIN_HOME/bin/startWeblogic.sh
   ```

   Add the following line to the bottom of the file:
   
   ```
   export JAVA_OPTIONS="${JAVA_OPTIONS} -Dgov.va.med.environment.production=true"
   ```

8. Modify the Domain Startup script (startWebLogic.sh):
   
   ```
   $ vi $DOMAIN_HOME/bin/startWeblogic.sh
   ```

9. Add call to configureVistaLink.sh after the setDomainEnv.sh call as shown:
   
   ```
   . $[DOMAIN_HOME]/bin/setDomainEnv.sh $*
   . $[DOMAIN_HOME]/bin/configureVistaLink.sh $*
   ```

10. Modify the nodemanager.properties file:
    
    ```
    $ vi $DOMAIN_HOME/nodemanager/nodemanager.properties
    ```

11. Ensure StartScriptEnabled=true:
    
    ```
    StartScriptEnabled=true
    ```
4.8.1.24 Configure VistALink on VM2

1. Create Deployments/VistaLink directory if it doesn’t exist:
   $ mkdir -p /u01/downloads/vistalink
2. Download VistALink configuration zip file for the environment:
   Download from AITC IEP eRx Deployments/VistaLink directory
3. Unzip VistALink configuration files for the environment:
   $ cd $DOMAIN_HOME
   $ unzip /u01/deployments/vistalink/[ENV]_vistalink_config_YYYYMMDD.zip

4.8.1.25 Stop and start Node Manager and Domain on VM1, VM2

This section outlines the steps for starting the node manager on the first WebLogic machine:

1. Stop the new domain on the VM1.
   $ $DOMAIN_HOME/bin/stopWebLogic.sh
2. On VM1 stop the node manager.
   $ $DOMAIN_HOME/bin/stopNodeManager.sh
3. On VM1, start the node manager.
   $ $DOMAIN_HOME/bin/stopNodeManager.sh
4. On VM2 stop the node manager.
   $ $DOMAIN_HOME/bin/stopNodeManager.sh
5. On VM2, start the node manager.
   $ $DOMAIN_HOME/bin/stopNodeManager.sh
6. Start the domain on VM1.
   $ $DOMAIN_HOME/bin/startWebLogic.sh
7. Wait for the “RUNNING” state before proceeding.
4.8.1.26 Deploy VistALink Libraries

This section provides step-by-step instructions for deploying VistA Link Connector:

1. Navigate to the Deployments page.
2. From the Deployments screen, click Install.

Figure 62: Deploy VistA Link Connector – Deployments
3. Enter *Path*: “/u01/downloads”
4. Install a new deployment of “log4j-1.2.17.jar” by selecting the jar file as indicated, and then click **Next**.

**Figure 63: Deploy VistA Link Connector – Select log4j Library to deploy**

![Deploy VistA Link Connector – Select log4j Library to deploy](image-url)
5. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

**Figure 64: Deploy VistA Link Connector – Select Deployment Targets**
6. All of the values should appear as illustrated in the figure below.
7. Click Next.

Figure 65: Deploy VistA Link Connector – Summary of Deployments Verification 1
8. Verify that all of the values appear as illustrated in the figure below.

9. Click **Finish**.

**Figure 66: Deploy VistA Link Connector – Summary of Deployments Verification 2**
10. The **Deployment Configuration** screen should appear as illustrated in the below figure.
11. Enter **Deployment Order**: “1”.
12. Click **Save**.

**Figure 67: Deploy VistA Link Connector – Deployment Configuration Screen**
13. Navigate to the *Deployments* page.
14. From the *Deployments* screen, click **Install**.

**Figure 68: Deploy VistA Link Connector – Deployments**
15. Enter *Path*: “/u01/downloads”

16. Install a new deployment of “vljConnector-1.6.0.028.jar” by selecting the jar file as indicated, and then click *Next*.

**Figure 69: Deploy VistA Link Connector – Select vljConnector-1.6.0.028.jar Library to deploy**
17. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

**Figure 70: Deploy VistA Link Connector – Select Deployment Targets**
18. All of the values should appear as illustrated in the figure below.
19. Click Next.

**Figure 71: Deploy VistA Link Connector – Summary of Deployments Verification 1**
20. Verify that all of the values appear as illustrated in the figure below.
21. Click **Finish**.

**Figure 72: Deploy VistA Link Connector – Summary of Deployments Verification 2**
22. The **Deployment Configuration** screen should appear as illustrated in the below figure.
23. Enter *Deployment Order*: “1”.
24. Click Save.

**Figure 73: Deploy VistA Link Connector – Deployment Configuration Screen**
25. Navigate to the *Deployments* page.
26. From the *Deployments* screen, click **Install**.

*Figure 74: Deploy VistA Link Connector – Deployments*
27. Enter Path: “/u01/downloads”
28. Install a new deployment of “log4j-1.2.17.jar” by selecting the jar file as indicated, and then click Next.

Figure 75: Deploy VistA Link Connector – Select log4j Library to deploy
29. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

**Figure 76: Deploy VistA Link Connector – Select Deployment Targets**
30. All of the values should appear as illustrated in the figure below.
31. Click Next.

**Figure 77: Deploy VistA Link Connector – Summary of Deployments Verification 1**
32. Verify that all of the values appear as illustrated in the figure below.

33. Click **Finish**.

---

**Figure 78: Deploy VistA Link Connector – Summary of Deployments Verification 2**
34. The **Deployment Configuration** screen should appear as illustrated in the below figure.

35. Enter *Deployment Order*: “1”.

36. Click *Save*.

Figure 79: Deploy VistA Link Connector – Deployment Configuration Screen
37. Navigate to the Deployments page.
38. From the Deployments screen, click Install.

**Figure 80: Deploy VistA Link Connector – Deployments**
39. Enter *Path*: “/u01/downloads”
40. Install a new deployment of “VistaLinkConsole-1.6.0.0.28.ear” by selecting the jar file as indicated, and then click **Next**.

**Figure 81: Deploy VistA Link Connector – Select log4j Library to deploy**
41. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

**Figure 82: Deploy VistA Link Connector – Select Deployment Targets**

![Deploy VistA Link Connector - Select Deployment Targets](image-url)
42. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.
43. All of the values should appear as illustrated in the figure below.
44. Click Next.

**Figure 84: Deploy VistA Link Connector – Summary of Deployments Verification 1**
45. Verify that all of the values appear as illustrated in the figure below.
46. Click **Finish**.

**Figure 85: Deploy VistA Link Connector – Summary of Deployments Verification 2**
47. The **Deployment Configuration** screen should appear as illustrated in the below figure.
48. Enter *Deployment Order:* “1”.
49. Click *Save.*

**Figure 86: Deploy VistA Link Connector – Deployment Configuration Screen**
4.8.1.27  Deploy VistALink Adapters

This section provides step-by-step instructions for deploying VistA Link Connector.

50. Navigate to the Deployments page.
51. From the Deployments screen, click Install.

Figure 87: Deploy VistA Link Connector – Deployments
52. Enter Path: “/u01/downloads”

53. Install a new deployment of “log4j-1.2.17.jar” by selecting the jar file as indicated, and then click Next.

Figure 88: Deploy VistA Link Connector – Select log4j Library to deploy
54. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.
55. All of the values should appear as illustrated in the figure below.

56. Click Next.

Figure 90: Deploy VistA Link Connector – Summary of Deployments Verification 1
57. Verify that all of the values appear as illustrated in the figure below.

58. Click **Finish**.

**Figure 91: Deploy VistA Link Connector – Summary of Deployments Verification 2**
59. The **Deployment Configuration** screen should appear as illustrated in the below figure.
60. Enter *Deployment Order*: “1”.
61. Click **Save**.

**Figure 92: Deploy VistA Link Connector – Deployment Configuration Screen**
4.8.2 Inbound eRx Application Installation

The following sections describe the steps to install and configure the Inbound eRx application. Most activities are to be performed by the WebLogic Administrator.

4.8.2.1 Install Inbound eRx Application

1. Shut down WebLogic (refer to Sections 4.8.2.3 and 4.8.2.4).
2. As your normal Linux login account, sudo su to the weblogic account:
   ```
   $ sudo su - weblogic
   ```
3. Create the downloads directory if it doesn’t exist:
   ```
   $ mkdir -p /u01/downloads
   ```
4. Download Inbound eRx application to the downloads directory.
   Download from AITC IEP eRx Downloads directory
5. Create the deployments directory if it doesn’t exist:
   ```
   $ mkdir -p /u01/deployments
   ```
6. Copy the application EAR to the deployments directory:
   Download from AITC IEP eRx Downloads directory
7. Access the WebLogic Admin Console by directing a browser to:
   https://[vm1_fqdn]:7002/console/ and log in with the “weblogic” account.
8. Navigate to the Servers page.
9. From the Administration Console > Servers page, click the “erx1” link to configure the server.

Figure 93: Install Inbound eRx Application – Configure Servers
10. The server configuration screen should appear as shown in the figure below.

11. Inspect the settings under the **General** tab. The **Listen Address** should be \[vm1\_fqdn\]. The non-secure listening port (**Listen Port Enabled**) should be enabled and set to port “8001” (**Listen Port**). The secure listening port should be disabled (**SSL Listen Port Enabled**). These ports need to be consistent with the Apache Load Balancer/Proxy and local firewall settings.

**Figure 94: Install Inbound eRx Application – Verify Server Settings**
12. Review the setting under the **Keystores** tab as illustrated in the figure below. Verify the **Keystores** option is set to “Custom Identity and Custom Trust”, and that the fields under the **Identity** and **Trust** sections are filled with the same corresponding values.

**Figure 95: Install Inbound eRx Application – Verify General & Keystore Settings**
13. Verify the settings under the **SSL** tab. The *Private Key Alias* should be the Fully Qualified Domain Name of the server, and the *Passphrase* is """".

**Figure 96: Install Inbound eRx Application – Verify SSL Settings**

14. Repeat the previous three steps for the “erx2” managed server to verify the *General Configuration*, *Keystores*, and *SSL* settings.
15. Navigate to the **Deployments** page.
16. From the **Deployments** page, click **Install**.

**Figure 97: Install Inbound eRx Application – Summary of Deployments**

17. Install a new deployment of INB_-ERX-3.1.0.004.ear using the WAR file as indicated in the figure below.
18. Click **Next**.

**Figure 98: Install Inbound eRx Application – Install New Deployment of INB_ERX**
19. Accept the defaults for an application deployment.
20. Click **Next**.
21. Select the cluster and “All servers in the cluster” as the target for the deployment.
22. Click **Next**.

**Figure 99: Install Inbound eRx Application – Select INB_ERX Deployment Targets**
23. All of the values should appear as illustrated in the figure below.
24. Click Next.

Figure 100: Install Inbound eRx Application – Verify INB_ERX Deployment Settings
25. All of the values should appear as illustrated in the figure below.

26. Click **Finish**.

**Figure 101: Install Inbound eRx Application – Verify INB_ERX Deployment Settings (Finish)**
27. The **Overview** tab should appear as illustrated in the figure below.
28. Navigate to the **Deployments** page.

29. From the **Deployments** page, click **Install**.

30. Install a new deployment of INB_ERX_UI-3.1.0.004.ear, select the appropriate EAR file.

31. Click **Next**.

**Figure 103: Install Inbound eRx Application – Install New Deployment of INB_ERX_UI**
32. Accept the defaults for an application deployment.
33. Click **Next**.
34. Select the cluster and “All servers in the cluster” as the target for the deployment.
35. Click **Next**.

**Figure 104: Install Inbound eRx Application – Select INB_ERX_UI Deployment Targets**
36. All of the values should appear as illustrated in the figure below.

37. Click Next.

**Figure 105: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings**

![Install Application Assistant](image)

- Optional Settings
  - You can modify these settings or accept the defaults. *Indicates required fields.
  - General
    - What do you want to name this deployment?
    - Name: `INB_ERX_UI-1.0.2.015_20161219`
  - Security
    - What security model do you want to use with this application?
    - ODD Only: Use only roles and policies that are defined in the deployment descriptors.
    - Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
  - Advanced
    - Source Accessibility
      - How should the source files be made accessible?
    - Use the defaults defined by the deployment's targets
      - Recommended selection.
    - Copy this application onto every target for me
      - During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted.
    - I will make the deployment accessible from the following location
      - Location: `u01/deployments/INB_ERX_UI-1.0.2.015_20161219`
        - Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.
  - Plan Source Accessibility
    - How should the plan source files be made accessible?
    - Use the same accessibility as the application
      - Recommended selection.
    - Copy this plan onto every target for me
      - During deployment, the plan files will be copied automatically to the Managed Servers to which the application is targeted.
    - Do not copy this plan to targets
      - You must ensure the plan files exist in this shared location and that each target can reach the location.
38. All of the values should appear as illustrated in the figure below.

39. Click **Finish**.

**Figure 106: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings (Finish)**

![Image of Oracle WebLogic Console showing the deployment assistant with configuration settings and options for deployment completion.](image_url)
40. The **Overview** tab should appear as illustrated in the figure below.

**Figure 107: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Configuration Settings**
41. Navigate to the **Servers** page in the WebLogic console.
42. Select the **Control** tab.
43. Select “erx1” and “erx2”, and then click **Start**.

**Figure 108: Install Inbound eRx Application – Start erx Servers**
4.8.2.2 Create Startup/Shutdown Scripts

This section outlines the steps for creating startup/shutdown scripts:

1. As your normal Linux login account, sudo su to the weblogic account:
   
   ```
   $ sudo su - weblogic
   ```

2. Create startup scripts with the following commands:
   
   ```
   $ cat > startNodemanager_[domain].sh
   tmp_domain_home="[DOMAIN_HOME]"
   cp $tmp_domain_home/nodemanager/nodemanager.log
   $tmp_domain_home/nodemanager/nodemanager_old.log
   cat /dev/null > $tmp_domain_home/nodemanager/nodemanager.log
   nohup $tmp_domain_home/bin/startNodeManager.sh 2>&1 > $tmp_domain_home/nodemanager/nm.out &
   `<ctrl>d`
   
   $ cat > startWebLogic_[domain].sh
   tmp_domain_home="[DOMAIN_HOME]"
   cp $tmp_domain_home/servers/AdminServer/logs/AdminServer.log
   $tmp_domain_home/servers/AdminServer/logs/AdminServer_old.log
   cat /dev/null > $tmp_domain_home/servers/AdminServer/logs/AdminServer.log
   ```
nohup ${tmp_domain_home}/bin/startWebLogic.sh 2>&1>
$(tmp_domain_home)/servers/AdminServer/logs/AdminServer.out &
<ctrl>d

$ cat > stopNodemanager_[domain].sh
tmp_domain_home="[DOMAIN_HOME]"
$(tmp_domain_home)/bin/stopNodeManager.sh
<ctrl>d

$ cat > stopWebLogic_[domain].sh
tmp_domain_home="[DOMAIN_HOME]"
$(tmp_domain_home)/bin/stopWebLogic.sh
<ctrl>d

4.8.2.3 Shut Down Domain
The section provides the steps for shutting down the domain:

1. On VM1, as your normal Linux login account, sudo su to the weblogic account:
   $ sudo su - weblogic
2. Shut down the Administration Console with the following command:
   $ ./stopWebLogic_[domain].sh

4.8.2.4 Shut Down Nodemangers
This sections outlines the steps for shutting down the nodemanagers:

1. On VM1, as your normal Linux login account, sudo su to the weblogic account:
   $ sudo su - weblogic
2. Shut down Nodemanager with the following command:
   $ ./stopNodeManager_[domain].sh
3. On VM2, as your normal Linux login account, sudo su to the weblogic account:
   $ sudo su - weblogic
4. Shut down Nodemanager with the following command:
   $ ./stopNodeManager_[domain].sh
4.8.3 Pentaho Installation

The following sections describe the steps to install the WebLogic application server. Most activities are to be performed by the WebLogic Administrator.

4.8.3.1 Pentaho Software Installation

The section provides step-by-step guidance on the installing the Pentaho software:

1. As your normal Linux login account, sudo su to the kettle account:
   
   ```bash
   $ sudo su - kettle
   ```

2. Create downloads directory if it doesn’t exist:
   
   ```bash
   $ mkdir -p /u01/downloads
   ```

3. Download Pentaho Data Integration Community Edition 6.1 archive (pdi-ce-6.1.0.1-196.zip) to the downloads directory.
   
   Download from AITC IEP eRx Downloads directory

4. Download INB_ERX Pentaho configuration zip archive for [ENV].
   
   Download pdi-[env]_cfg_[yyyyMMdd].zip from AITC IEP eRx Deployments directory

5. Create a pentaho directory if it doesn’t exist:
   
   ```bash
   $ mkdir -p /u01/app/pentaho
   ```

6. On VM1, unzip the Pentaho Data Integration Community Edition 6.1 archive to the pentaho master1 installation directory:
   
   ```bash
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-6.1.0.1-196.zip
   $ mv data-integration pdi-[env]master1
   ```

7. On VM1, unzip the Pentaho Data Integration Community Edition 6.1 archive to the pentaho slave1 installation directory:
   
   ```bash
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-6.1.0.1-196.zip
   $ mv data-integration pdi-[env]slave1
   ```

8. On VM1, unzip the Pentaho Data Integration Community Edition 6.1 archive to the pentaho slave2 installation directory:
   
   ```bash
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-6.1.0.1-196.zip
   $ mv data-integration pdi-[env]slave2
   ```

9. On VM2, unzip the Pentaho Data Integration Community Edition 6.1 archive to the pentaho slave3 installation directory:
   
   ```bash
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-6.1.0.1-196.zip
   $ mv data-integration pdi-[env]slave3
   ```

10. On VM2, unzip the Pentaho Data Integration Community Edition 6.1 archive to the pentaho slave4 installation directory:
    
    ```bash
    $ cd /u01/app/pentaho
    $ unzip /u01/downloads/pdi-ce-6.1.0.1-196.zip
    $ mv data-integration pdi-[env]slave4
    ```

11. On VM1, unzip the environment specific configuration archive to the pentaho master1 installation directory:
    
    ```bash
    $ cd /u01/app/pentaho/pdi-[env]master1
    $ unzip /u01/downloads/pdi-[env]_cfg_[yyyyMMdd].zip
    ```
12. On VM1, unzip the environment specific configuration archive to the pentaho slave1 installation directory:

```
$ cd /u01/app/pentaho/pdi-[env]slave1
$ unzip /u01/downloads/pdi-[env]_cfg_[yyyymmdd].zip
```

13. On VM1, unzip the environment specific configuration archive to the pentaho slave2 installation directory:

```
$ cd /u01/app/pentaho/pdi-[env]slave2
$ unzip /u01/downloads/pdi-[env]_cfg_[yyyymmdd].zip
```

14. On VM2, unzip the environment specific configuration archive to the pentaho slave3 installation directory:

```
$ cd /u01/app/pentaho/pdi-[env]slave3
$ unzip /u01/downloads/pdi-[env]_cfg_[yyyymmdd].zip
```

15. On VM2, unzip the environment specific configuration archive to the pentaho slave4 installation directory:

```
$ cd /u01/app/pentaho/pdi-[env]slave4
$ unzip /u01/downloads/pdi-[env]_cfg_[yyyymmdd].zip
```

16. On the Master VM, create master1, slave1 and slave2 startup scripts in the ~kettle directory:

```
$ cd ~
$ cat > ~/startCarte[Env]Master1.sh
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi-[env]master1
datestamp=`date +%Y%m%d_%H%M%S`
export PENTAHO_DI_JAVA_OPTIONS="-Xms1024m -Xmx2048m -XX:MaxPermSize=256m"
${KETTLE_HOME}/carte.sh ${KETTLE_HOME}/pwd/[env]master1-8080.xml >
${KETTLE_HOME}/logs/[env]master1-8080_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Master1.sh

$ cat > ~/startCarte[Env]Slave1.sh
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi-[env]slave1
datestamp=`date +%Y%m%d_%H%M%S`
export PENTAHO_DI_JAVA_OPTIONS="-Xms1024m -Xmx3072m -XX:MaxPermSize=256m"
${KETTLE_HOME}/carte.sh ${KETTLE_HOME}/pwd/[env]slave1-8081.xml >
${KETTLE_HOME}/logs/[env]slave1-8081_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Slave1.sh

$ cat > ~/startCarte[Env]Slave2.sh
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi-[env]slave1
datestamp=`date +%Y%m%d_%H%M%S`
export PENTAHO_DI_JAVA_OPTIONS="-Xms1024m -Xmx3072m -XX:MaxPermSize=256m"
${KETTLE_HOME}/carte.sh ${KETTLE_HOME}/pwd/[env]slave2-8082.xml >
${KETTLE_HOME}/logs/[env]slave2-8082_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Slave2.sh
```

17. On the Master VM, create slave3 and slave4 startup script in the ~kettle directory:

```
$ cd ~
$ cat > ~/startCarte[Env]Slave3.sh
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi-[env]slave3
datestamp=`date +%Y%m%d_%H%M%S`
export PENTAHO_DI_JAVA_OPTIONS="-Xms1024m -Xmx3072m -XX:MaxPermSize=256m"
${KETTLE_HOME}/carte.sh ${KETTLE_HOME}/pwd/[env]slave3-8083.xml >
${KETTLE_HOME}/logs/[env]slave3-8083_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Slave3.sh

$ cat > ~/startCarte[Env]Slave4.sh
unset DISPLAY
```
export KETTLE_HOME=/u01/app/pentaho/pdi

datestamp=`date +%Y%m%d_%H%M%S`

export PENTATHO_DJ_JAVA_OPTIONS="-Xms1024m -Xmx3072m -XX:MaxPermSize=256m"

$(KETTLE_HOME)/carte.sh $(KETTLE_HOME)/pwd/[env]slave4-8084.xml >

${KETTLE_HOME}/logs/[env]slave4-8084_${datestamp}.out 2>&1 &

<ctlr>d

$ chmod 755 ~/startCarte[Env]Slave4.sh

18. On the Master VM, create repository update script in the ~kettle directory:

$ cd ~
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi

datestamp=`date +%Y%m%d_%H%M%S`

$(KETTLE_HOME)/import.sh -rep="[ENV] Repo" -user=admin -pass=admin -dir=/ -replace=Y -norules=Y -file=${KETTLE_HOME}/erx_repo/inbound_main.xml | tee

$(KETTLE_HOME)/import.sh -rep="[ENV] Repo" -user=admin -pass=admin -dir=/ -replace=Y -norules=Y -file=${KETTLE_HOME}/erx_repo/inbound_vista_delivery.xml | tee -a

$(KETTLE_HOME)/import.sh -rep="[ENV] Repo" -user=admin -pass=admin -dir=/ -replace=Y -norules=Y -file=${KETTLE_HOME}/erx_repo/outbound_main.xml | tee -a
<ctlr>d

$ chmod 755 ~/updateRepo[Env].sh

4.8.3.2 Pentaho Repository Definition Import

The section provides step-by-step guidance to import the Pentaho repository:

1. As your normal Linux login account, sudo su to the kettle account:

   $ sudo su - kettle

2. Create downloads directory if it doesn’t exist:

   $ mkdir -p /u01/downloads

3. Download INB_ERX Pentaho Repository Definition zip archive for [ENV].

   Download PS_INB_ERX_Pentaho_[n.n.n.nnn].zip from AITC IEP eRx Deployments directory

4. Unpack repository definition in Master1 instance:

   $ cd /u01/app/pentaho/pdi-[env]master1
   $ unzip /u01/app/downloads/PS_INB_ERX_Pentaho_[n.n.n.nnn].zip erx_repo/*

5. Update Pentaho repository:

   $ cd ~
   $ ~/updateRepo[Env].sh
4.8.4 Nexus Repository Installation (DEV2 VM1 Only)

The following sections describe the steps to install the SonaType Nexus OSS repository server. All activities are to be performed by a Systems Administrator.

4.8.4.1 SonaType Nexus Software Installation

The section provides step-by-step guidance on the installing the SonaType Nexus repository software:

1. As your normal Linux login account, sudo su to the weblogic account:
   $ sudo su - weblogic
2. Create downloads directory if it doesn’t exist:
   $ mkdir -p /u01/downloads
3. Download SonaType Nexus OSS repository software archive (nexus-3.5.2-01-unix.tar.gz) to the downloads directory.
   Download from AITC IEP eRx Downloads directory
4. Return back in your normal Linux login account.
   $ exit
5. Create the nexus software directory if it doesn’t exist:
   $ sudo mkdir -p /u01/app/nexus
   $ sudo chown nexusloc:weblogic /u01/app/nexus
   $ sudo chmod 755 /u01/app/nexus
6. Unpack Nexus repository software:
   $ cd /u01/app/nexus
   $ sudo -u nexusloc tar xvzf /u01/downloads/nexus-3.5.2-01-unix.tar.gz
   $ sudo ln -s nexus-3.5.2-01 latest
7. Modify /u01/app/nexus/latest/bin/nexus.rc:
   $sudo vi /u01/app/nexus/latest/bin/nexus.rc
8. Modify service user account:
   run_as_user="nexusloc"
9. Modify /u01/app/nexus/sonatype-work/nexus3/etc/nexus.properties:
   $sudo vi /u01/app/nexus/sonatype-work/nexus3/etc/nexus.properties
10. Modify as follows:
    application-port=8061
    application-host=vauserxappdev2.aac.va.gov
    nexus-context-path=/nexus/
11. Modify ~nexusloc/.bashrc:
    $ sudo vi ~nexusloc/.bashrc
12. Add NEXUS_HOME near the end of the file:
    export NEXUS_HOME=/u01/app/nexus/latest
13. Modify /u01/app/nexus/latest/bin/nexus
    $sudo vi /u01/app/nexus/latest/bin/nexus
14. Enable the INSTALL4_JAVA_HOME_OVERRIDE variable:
    INSTALL4_JAVA_HOME_OVERRIDE=/u01/app/java/latest
15. Modify HTTPD configuration:
    $ sudo vi /etc/httpd/conf/httpd.conf
16. Add the following for Nexus reverse proxy:
Reverse proxy to Nexus


17. Create symbolic link for /etc/init.d/nexus:
   
   ```
   $ sudo ln -s /u01/app/nexus/latest/bin/nexus /etc/init.d/nexus
   ```

18. Enable the Nexus OSS repository service:

   ```
   $ cd /etc/init.d
   $ sudo chkconfig --add nexus
   $ sudo chkconfig --levels 345 nexus on
   ```

4.8.5 VistA Patch Installation

Steps for installing the VistA patch for Inbound eRx reference PSO*7.0*551 Patch Description (PD) in Forum and pso_7_0_p551_ig detailing Deployment, Installation, Back-Out, and Rollback for PD PSO*7.0*551.

4.9 Installation Verification Procedure

Please refer to the installation steps in the previous sections, which outline the installation verification procedures within each step.

4.10 System Configuration

This section is not applicable to the Inbound eRx project.

4.11 Database Tuning

This section will be added in future versions of this document.

5. Back-Out Procedure

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

The Inbound eRx 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 recover point objective). This section outlines the backout strategy, considerations, testing, criteria for backout, risks, authority to approve and the procedures to perform a backout for Inbound eRx.

5.1 Back-Out Strategy

The back-out strategy will follow VA guidelines and best practices as referenced in the Enterprise Operations (EO) National Data Center Hosting Services document.

5.2 Back-Out Considerations

Back-out considerations will follow VA guidelines and best practices as referenced in the EO National Data Center Hosting Services document.
5.2.1 Load Testing
This section is not applicable to the Inbound eRx project.

5.2.2 User Acceptance Testing
The results of User Acceptance Testing (UAT) will be added to this document in a future version, following the completion of UAT.

5.3 Back-Out Criteria
Back-out criteria will follow VA guidelines and best practices as referenced in the EO National Data Center Hosting Services document.

5.4 Back-Out Risks
There are no known risks related to a back-out.

5.5 Authority for Back-Out
The POCs with the authority to order the back-out is the Inbound eRx IPT, the VA PM, and other relevant stakeholders, where applicable.

5.6 Back-Out Procedure
This section outlines the backout procedure for the following:

- VistA Patch PSO*7.0*551
- WebLogic

5.6.1 Back-Out of VistA Patch
Prior to installing a patch, the site/region should have saved a backup of the routines in a mail message using the Backup a Transport Global [XPD BACKUP] menu option (this is done at time of install). The message containing the backed up routines can be loaded with the "Xtract PackMan" function at the Message Action prompt. The PackMan function "INSTALL/CHECK MESSAGE" is then used to install the backed up routines onto the VistA System.

Steps for back out of the VistA patch for Inbound eRx one can reference PSO*7.0*551 Patch Description in Forum and pso_7_0_p551_ig detailing Deployment, Installation, Back-Out, and Rollback for PD PSO*7.0*551.

If the decision is made to back-out the PSO*7.0*551 patch, users should be off of the system and option ‘Finish Orders from eRx’ [PSO ERX FINISH] should be placed out of order. Due to the complexity and inclusion of support for new message types, there are two options for back-out procedures.

1. Re-install patches PSO*7.0*467, PSO*7.0*506, PSO*7.0*520, and PSO*7.0*527.
a. This approach will revert the system to inbound eRx version 2.0 functionality, and does not contain support for the new refill and cancel message types. These records can still be viewed, but are incomplete due to the lack of supporting logic.

b. This approach also causes all message types to be treated as ‘newrx’ message types, and will require a follow-on patch to lock down all actions that are not applicable to Cancel and Refill message types (i.e. Validate Patient, Validate Drug, Validate Provider, Accept eRx).

2. Leave PSO*7.0*550 in place and disable all new actions.

c. Taking this approach will ensure supporting logic related to the display of refill and cancel message types is still available, ensuring the user can still view the records in their entirety.

d. A follow-on patch will be required to disable all new functionality related to refill and cancel message types.

### 5.6.2 Back-Out of Database

This section outlines the steps for backing out Database changes on local database server. These steps should be performed under strict guidance of the PRE Inbound eRx PM team.

#### 5.6.2.1 Restore backup files from tape

Recover data per procedures in the EO National Data Center Hosting Services document.

#### 5.6.2.2 Mount the instance

1. Set ORACLE_SID=IEPP
2. rman TARGET SYS/Password NOCATALOG
3. RMAN:> shutdown immediate;
   RMAN:> startup mount;

#### 5.6.2.3 Restore and recover the datafiles

1. RMAN> run
   {
   allocate channel dev1 type disk;
   set until time "to_date('2011-12-30:00:00:00', 'yyyy-mm-dd:hh24:mi:ss')";
   restore database;
   recover database;
   }

#### 5.6.2.4 Open the database and reset logs

1. RMAN> alter database open resetlogs;

### 5.6.3 Back-Out of WebLogic

This section outlines the steps for backing out a new version of the PRE Inbound eRx application deployed on a local WebLogic (application) server. This is a two-step process: first, remove the new release, and then deploy the rolled-back release. These steps should be performed under strict guidance of the PRE Inbound eRx PM team.
5.6.3.1 Remove New Release

1. Open and log into the WebLogic console. Use WebLogic username and password.
2. Within the Domain Structure panel in the left column of the WebLogic console, click the Deployments node.
3. Within the Change Center panel in the left column of the WebLogic console, click Lock & Edit.
4. WebLogic will now display the panel Summary of Deployments in the right column of the console, where all deployments for the WebLogic domain are listed.
5. Select the previously deployed Inbound eRx deployment, click Stop, and then select “Force Stop Now” from the drop-down list box.
6. WebLogic will now display the panel Force Stop Application Assistant in the right column of the console for confirmation to start servicing requests.
7. Click Yes in the Force Stop Application Assistant panel in the right column of the WebLogic console.
8. WebLogic now returns to the Summary of Deployments panel in the right column of the console.
9. Verify that the State of the Inbound eRx deployment is “Prepared”.
10. Select the previously deployed Inbound eRx deployment, and then click Delete.
11. WebLogic will now display the panel Delete Application Assistant in the right column of the console for confirmation to start servicing requests.
12. Click Yes in the Delete Application Assistant panel in the right column of the WebLogic console.
13. WebLogic now returns to the Summary of Deployments panel in the right column of the console.
14. Verify that the Inbound eRx deployment is deleted and no longer present.

5.6.3.2 Deploy Back-out Release

The following steps detail the deployment of the rolled-back Inbound eRx application.

1. Use the WebLogic console that was started at the beginning of the roll-back process.
2. Within the Domain Structure panel in the left column of the WebLogic console, click the Deployments node.
3. Verify that application is in Lock & Edit mode. Lock & Edit mode is indicated by the “greyed-out” Lock & Edit selection button.
4. Click the Install button in the Deployments panel in the right column of the WebLogic console.
5. WebLogic will now display the panel Install Application Assistant in the right column of the console, where the location of the Inbound eRx deployment will be found.
   a. If the rolled-back Inbound eRx deployment has already been transferred to the Deployment Machine, navigate to the deployment file location using the links and file structure displayed within the Location panel within the Install Application Assistant in the right column of the console. Choose the ear file associated with the rolled-back release.
b. If the rolled-back Inbound eRx deployment has not been transferred to the Deployment Machine:
   i. Click on the upload your file(s) link in the Install Application Assistant panel in the right section of the console.
   ii. Click the Deployment Archive Browse to see the Choose file dialogue used to select the Deployment Archive.
   iii. Click Next in the Upload a Deployment to the admin server panel in the right column of the WebLogic console to return to the Locate deployment to install and prepare for deployment panel within the Install Application Assistant.

6. Once the rolled-back Inbound eRx deployment is located and selected, click Next.
7. WebLogic will now display the panel Choose targeting style within the Install Application Assistant in the right column of the console. Leave the default value selected, install this deployment as an application, and click Next.
8. Within the Install Application Assistant in the right column of the console, WebLogic will now display the panel Select deployment targets, where the Deployment Server will be selected as the target in the next step.
9. For the Target, select the Deployment Server.
10. Click Next.
11. Within the Install Application Assistant, WebLogic will now display the panel Optional Settings in the right column of the console, where the name of the deployment and the copy behavior are chosen.
12. Enter the Name for the deployment. Use: : INB_ERX-3.5.0.008
13. Verify that the following default option for Security is selected: DD Only: Use only roles and policies that are defined in the deployment descriptors.
14. Verify that the following default option for Source accessibility is selected:
    Use the defaults defined by the deployment's targets.
15. Click Next.
16. Within the Install Application Assistant, in the right column of the console WebLogic, will now display the panel Review your choices and click Finish, which summarizes the steps completed above.
17. Verify that the values match those entered in Steps 6 through 17 and click Finish.
18. WebLogic will now display the panel Settings for Inbound eRx, in the right column of the console, where the values previously entered are available as well as a setting to change the deployment order.
19. Leave all the values as defaulted by WebLogic and click Save.
20. Within the Change Center panel in the left column of the WebLogic console, click Activate Changes.
21. Within the Domain Structure panel in the left column of the WebLogic console, click the Deployments node.
22. WebLogic will now display the panel **Summary of Deployments** in the right column of the console, where all deployments for the WebLogic domain are listed.

23. Select the previously deployed INB_ERX-3.0.5.008 deployment, click **Start**, and then select **Servicing all requests** from the drop-down list box.

24. WebLogic will now display the panel **Start Application Assistant** in the right column of the console for confirmation to start servicing requests.

25. Click **Yes** in the **Start Application Assistant** panel in the right column of the WebLogic console.

26. WebLogic now returns to the **Summary of Deployments** panel in the right column of the console.

27. Verify that the State of the INB_ERX-3.0.5.008 deployment is “Active”.

### 5.7 Back-out Verification Procedure

Steps for verifying the VistA patch backout for Inbound eRx reference PSO*7.0*551 Patch Description in Forum and pso_7_0_p551_ig detailing Deployment, Installation, Back-Out, and Rollback for PD PSO*7.0*551.

Depending on the approach taken for the back-out the verification steps will differ. Please contact the Inbound eRx development/maintenance team for verification instructions.

### 6. Rollback Procedure

This section outlines the procedures for rolling back to a previous state of the data.

#### 6.1 Rollback Considerations

Back-out considerations will follow VA guidelines and best practices as referenced in the EO National Data Center Hosting Services document.

#### 6.2 Rollback Criteria

Roleback criteria will follow VA guidelines and best practices as referenced in the EO National Data Center Hosting Services document.

#### 6.3 Rollback Risks

There are no known risks related to a Roleback.

#### 6.4 Authority for Rollback

The POCs with the authority to order the Roleback is the Inbound eRx IPT, the VA PM, and other relevant stakeholders, where applicable.
6.5 Rollback Procedure

6.5.1 Rollback of Database

This section outlines the steps for rollback of Database changes on local database server. These steps should be performed under strict guidance of the PRE Inbound eRx PM team.

6.5.1.1 Restore backup files from tape

Recover data per procedures in the EO National Data Center Hosting Services document.

6.5.1.2 Mount the instance

28. Set ORACLE_SID=IEPP
29. rman TARGET SYS/Password NOCATALOG
30. RMAN:> shutdown immediate;
     RMAN:> startup mount;

6.5.1.3 Restore and recover the datafiles

31. RMAN> run
    { 
    allocate channel dev1 type disk;
    set until time "to_date('2011-12-30:00:00:00', 'yyyy-mm-dd:hh24:mi:ss')";
    restore database;
    recover database; }

6.5.1.4 Open the database and reset logs

32. RMAN> alter database open resetlogs;

6.5.2 Rollback WebLogic

This section outlines the steps for rolling back to a previous version of the PRE Inbound eRx application deployed on a local WebLogic (application) server. This is a two-step process: first, remove the old release, and then deploy the rolled-back release. These steps should be performed under strict guidance of the PRE Inbound eRx PM team.

6.5.2.1 Remove New Release

1. Open and log into the WebLogic console; This is located at: \vaauspecdbs801.aac.dva.va.gov\erx\install\ Use WebLogic username and password.
2. Within the Domain Structure panel in the left column of the WebLogic console, click the Deployments node.
3. Within the Change Center panel in the left column of the WebLogic console, click Lock & Edit.
4. WebLogic will now display the panel Summary of Deployments in the right column of the console, where all deployments for the WebLogic domain are listed.
5. Select the previously deployed Inbound eRx deployment, click **Stop**, and then select “Force Stop Now” from the drop-down list box.

6. WebLogic will now display the panel Force Stop Application Assistant in the right column of the console for confirmation to start servicing requests.

7. Click **Yes** in the **Force Stop Application Assistant** panel in the right column of the WebLogic console.

8. WebLogic now returns to the **Summary of Deployments** panel in the right column of the console.

9. Verify that the State of the Inbound eRx deployment is “Prepared”.

10. Select the previously deployed Inbound eRx deployment, and then click **Delete**.

11. WebLogic will now display the panel **Delete Application Assistant** in the right column of the console for confirmation to start servicing requests.

12. Click **Yes** in the **Delete Application Assistant** panel in the right column of the WebLogic console.

13. WebLogic now returns to the Summary of Deployments panel in the right column of the console.

14. Verify that the Inbound eRx deployment is deleted and no longer present.

### 6.5.2.2 Deploy Rolled-Back Release

The following steps detail the deployment of the rolled-back Inbound eRx application.

1. Use the WebLogic console that was started at the beginning of the roll-back process.

2. Within the **Domain Structure** panel in the left column of the WebLogic console, click the Deployments node.

3. Verify that application is in **Lock & Edit** mode. **Lock & Edit** mode is indicated by the “greyed-out” Lock & Edit selection button.

4. Click the **Install** button in the **Deployments** panel in the right column of the WebLogic console.

5. WebLogic will now display the panel **Install Application Assistant** in the right column of the console, where the location of the Inbound eRx deployment will be found.
   
   c. If the rolled-back Inbound eRx deployment has already been transferred to the Deployment Machine, navigate to the deployment file location using the links and file structure displayed within the **Location** panel within the Install Application Assistant in the right column of the console. Choose the ear file associated with the rolled-back release.
   
   d. If the rolled-back Inbound eRx deployment has not been transferred to the Deployment Machine:
      
      iv. Click on the upload your file(s) link in the **Install Application Assistant** panel in the right section of the console.
      
      v. Click the **Deployment Archive Browse** to see the Choose file dialogue used to select the Deployment Archive.
vi. Click **Next** in the Upload a Deployment to the admin server panel in the right column of the WebLogic console to return to the Locate deployment to install and prepare for deployment panel within the Install Application Assistant.

6. Once the rolled-back Inbound eRx deployment is located and selected, click **Next**.

7. WebLogic will now display the panel Choose targeting style within the Install Application Assistant in the right column of the console. Leave the default value selected, install this deployment as an application, and click **Next**.

8. Within the **Install Application Assistant** in the right column of the console, WebLogic will now display the panel Select deployment targets, where the Deployment Server will be selected as the target in the next step.

9. For the **Target**, select the **Deployment Server**.

10. Click **Next**.

11. Within the **Install Application Assistant**, WebLogic will now display the panel **Optional Settings** in the right column of the console, where the name of the deployment and the copy behavior are chosen.

12. Enter the **Name** for the deployment. Use: **INB_ERX-3.1.0.003**

13. Verify that the following default option for Security is selected:
   - DD Only: Use only roles and policies that are defined in the deployment descriptors.

14. Verify that the following default option for Source accessibility is selected:
   - Use the defaults defined by the deployment's targets.

15. Click **Next**.

16. Within the **Install Application Assistant**, in the right column of the console WebLogic, will now display the panel **Review your choices and click Finish**, which summarizes the steps completed above.

17. Verify that the values match those entered in Steps 6 through 17 and click **Finish**.

18. WebLogic will now display the panel **Settings for Inbound eRx**, in the right column of the console, where the values previously entered are available as well as a setting to change the deployment order.

19. Leave all the values as defaulted by WebLogic and click **Save**.

20. Within the **Change Center** panel in the left column of the WebLogic console, click **Activate Changes**.

21. Within the **Domain Structure** panel in the left column of the WebLogic console, click the Deployments node.

22. WebLogic will now display the panel **Summary of Deployments** in the right column of the console, where all deployments for the WebLogic domain are listed.

23. Select the previously deployed INB_ERX-3.1.0.003 deployment, click **Start**, and then select **Servicing all requests** from the drop-down list box.

24. WebLogic will now display the panel **Start Application Assistant** in the right column of the console for confirmation to start servicing requests.
25. Click **Yes** in the **Start Application Assistant** panel in the right column of the WebLogic console.

26. WebLogic now returns to the **Summary of Deployments** panel in the right column of the console.

27. Verify that the State of the INB_ERX-3.1.0.003 deployment is “Active”.

### 6.5.3 Rollback VistA Patch

Due to the fact that the data involved with inbound eRx is prescription related, data dictionary changes and existing data will not be rolled back. The system should maintain the new fields and records. The back-out procedure will dictate the usage/view of the new data. Any new message type will still be available to the user, and will be impacted only by the back-out procedure. Message linking between NewRx message types and cancel/refill message types will be established. The rolling back of the data would sever this linkage, potentially causing major problems.

### 6.6 Rollback Verification Procedure

#### 6.6.1.1 Validation of Roll Back Procedure

The user will be able to view the cancel and refill message types. All actions besides print will be locked so the user cannot take action on the record. This will create a view only scenario for cancel and refill message types.

### 7. Operational Procedures

This section outlines server startup and shutdown procedures.

#### 7.1 Startup Procedures

##### 7.1.1 Start Weblogic Node Managers and Admin Console

1. At your normal Linux login account, sudo su to the weblogic account:

   ```
   $ sudo su - weblogic
   ```

2. On VM1, start node managers:

   ```
   $ ./startNodemanager_[domain].sh
   ```

3. On VM2, start node managers:

   ```
   $ ./startNodemanager_[domain].sh
   ```

4. On VM1, wait for node manager startups to complete:

   ```
   $ tail -f [DOMAIN_HOME]/nodemanager/nodemanager.log
   ```

5. On VM1, watch for the following log messages to indicate the node managers are up:

   ```
   <INFO> <Secure socket listener started on port 5556, host [vm1_fqdn]>
   ```

6. On VM2, wait for node manager startups to complete:

   ```
   $ tail -f [DOMAIN_HOME]/nodemanager/nodemanager.log
   ```

7. On VM2, watch for the following log messages to indicate the node managers are up:

   ```
   <INFO> <Secure socket listener started on port 5556, host [vm2_fqdn]>
   ```

8. On VM1, start AdminServer:
9. On VM1, wait for the AdminServer startup to complete:

   $ tail -f [DOMAIN_HOME]/servers/AdminServer/logs/AdminServer.out

10. On VM1, watch for the following log messages to indicate the AdminServer is up:

   <Notice> <WebLogicServer> <BEA-000365> <Server state changed to RUNNING.>

### 7.1.2 Managed Servers

1. Log into the [domain] Admin Console, start “erx1” and “erx2” managed servers

2. Verify landing pages are responding:

   https://[proxy_fqdn]/INB-ERX/
   https://[proxy_fqdn]/inbound/

### 7.1.3 Pentaho Services Startup

1. As your normal Linux login account, sudo su to the kettle account:

   $ sudo su - kettle

2. On VM1, start [ENV] Master Slave:

   $ ./startCarte [Env]Master1.sh

3. From the CPanel (https://[proxy_fqdn]/cpanel), wait for the [ENV] Master Slave to start up by watching: https://[proxy_fqdn]/master1/kettle/status/

4. On VM 1, start [ENV] Dynamic Slave1:

   $ ./startCarte [Env]Slave1.sh

5. On VM 1, start [ENV] Dynamic Slave2:

   $ ./startCarte [Env]Slave2.sh

6. On VM 2, start [ENV] Dynamic Slave3:

   $ ./startCarte [Env]Slave3.sh

7. On VM 2, start [ENV] Dynamic Slave4:

   $ ./startCarte [Env]Slave4.sh

8. From the CPanel (https://[proxy_fqdn]/cpanel), wait for the [ENV] Slave1 to start up by watching: https://[proxy_fqdn]/slave1/kettle/status/

9. From the CPanel (https://[proxy_fqdn]/cpanel), wait for the [ENV] Slave2 to start up by watching: https://[proxy_fqdn]/slave2/kettle/status/

10. From the CPanel (https://[proxy_fqdn]/cpanel), wait for the [ENV] Slave3 to start up by watching: https://[proxy_fqdn]/slave3/kettle/status/

11. From the CPanel (https://[proxy_fqdn]/cpanel), wait for the [ENV] Slave4 to start up by watching: https://[proxy_fqdn]/slave4/kettle/status/

12. From the CPanel (https://[proxy_fqdn]/cpanel), check that all 4 dynamic slaves have registered with the master: https://[proxy_fqdn]/slave1/kettle/getSlaves/

13. From the CPanel (https://[proxy_fqdn]/cpanel), start the message processing jobs:

    https://[proxy_fqdn]/slave1/kettle/runJob/?job=inbound_main/InboundMessageProcessing_JOB

    https://[proxy_fqdn]/slave2/kettle/runJob/?job=inbound_main/InboundMessageProcessingRetry_JOB

    https://[proxy_fqdn]/slave3/kettle/runJob/?job=inbound_vista_delivery/InboundDeliverToVista_JOB
https://[proxy_fqdn]/slave4/kettle/runJob/?job=outbound_main/OutboundMessageProcessing_JOB

14. From the CPanel (https://[proxy_fqdn]/cpanel), check the InboundMessageProcessing_JOB status: https://[proxy_fqdn]/slave1/kettle/status, click on the InboundMessageProcessing_JOB hyperlink and check the job status page.

15. From the CPanel (https://[proxy_fqdn]/cpanel), check the InboundMessageProcessingRetry_JOB status: https://[proxy_fqdn]/slave2/kettle/status, click on the InboundMessageProcessingRetry_JOB hyperlink and check the job status page.

16. From the CPanel (https://[proxy_fqdn]/cpanel), check the InboundDeliverToVista_JOB status: https://[proxy_fqdn]/slave3/kettle/status, click on the InboundDeliverToVista_JOB hyperlink and check the job status page.

17. From the CPanel (https://[proxy_fqdn]/cpanel), check the OutboundMessageProcessing_JOB status: https://[proxy_fqdn]/slave4/kettle/status, click on the OutboundMessageProcessing_hyperlink and check the job status page.

### 7.2 Shut Down Procedures

#### 7.2.1 Pentaho Services Shutdown

1. As your normal Linux login account, sudo su to the kettle account:
   
   ```bash
   $ sudo su - kettle
   ```

2. As kettle on VM2:
   
   ```bash
   $ /u01/app/pentaho/pdi-{env}slave3/carte.sh [vm2_fqdn] 8083 -s -u cluster -p cluster
   $ /u01/app/pentaho/pdi-{env}slave4/carte.sh [vm2_fqdn] 8084 -s -u cluster -p cluster
   ```

3. As kettle on VM1:
   
   ```bash
   $ /u01/app/pentaho/pdi-{env}slave1/carte.sh [vm1_fqdn] 8081 -s -u cluster -p cluster
   $ /u01/app/pentaho/pdi-{env}slave2/carte.sh [vm1_fqdn] 8082 -s -u cluster -p cluster
   $ /u01/app/pentaho/pdi-{env}master1/carte.sh [vm1_fqdn] 8080 -s -u cluster -p cluster
   ```

#### 7.2.2 WebLogic Application Server Shutdown

1. As your normal Linux login account, sudo su to the weblogic account:
   
   ```bash
   $ sudo su - weblogic
   ```

2. Log into erxdomain1 Admin Console as weblogic
   
   ```
   Stop erx1 and erx2 managed servers
   Stop Admin console
   ```

3. On VM1, as weblogic:
   
   ```bash
   $ ./stopWebLogic_[domain].sh
   ```

4. On VM1, as weblogic:
   
   ```bash
   $ ./stopNodemanager_[domain].sh
   ```

5. On VM2, as weblogic:

6. $ ./stopNodemanager_[domain].sh
8. Appendices

This section provides additional reference information to use for the installation of various components.

8.1 Certificate Contents

Use the text in this section for the certificate configuration steps in Section 4.2.7.

8.1.1 va_root_ca_cert.txt

-----BEGIN CERTIFICATE-----
MIIDfjCCAmagAwIBAgIQA399zv0pkaxAy6VO4im+hDANBgkqhkiG9w0BAQUFADBH
MRMwEQYKCIIm1IzPyLGQBGRYDZ292MRIwEAYKCIIm1IzPyLGQBGRYCdmeEHDAAAgNV
BAMTEIBIEluGdVybEmFaIFjFv39gQ0EwWhcNMUwMjtyMTY0NDM1WhcNMUwMjty
MTY1MIe5WJHRMwEQYKCIIm1IzPyLGQBGRYDZ292MRIwEAYKCIIm1IzPyLGQBGRYCd
meEHDAAAgNVBAMTEIBIEluGdVybEmFaIFjFv39gQ0EwWhcNMUwMjtyMTY0NDM1WhcNMUwMjty

-----BEGIN CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfjCCAmagAwIBAgIQA399zv0pkaxAy6VO4im+hDANBgkqhkiG9w0BAQUFADBH
MRMwEQYKCIIm1IzPyLGQBGRYDZ292MRIwEAYKCIIm1IzPyLGQBGRYCdmeEHDAAAgNV
BAMTEIBIEluGdVybEmFaIFjFv39gQ0EwWhcNMUwMjtyMTY0NDM1WhcNMUwMjty
MTY1MIe5WJHRMwEQYKCIIm1IzPyLGQBGRYDZ292MRIwEAYKCIIm1IzPyLGQBGRYCd
meEHDAAAgNVBAMTEIBIEluGdVybEmFaIFjFv39gQ0EwWhcNMUwMjtyMTY0NDM1WhcNMUwMjty

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
-----BEGIN CERTIFICATE-----
8.1.2 va_internal_subordinate_ca_cert.txt

-----BEGIN CERTIFICATE-----
MIIF2zCCBMIgAwIBAgIQFQAAAA4TANBgkqhkiG9w0BQFADHMWhMQxGCAQYMQw
-----END CERTIFICATE-----

8.1.3 va_root_ca_s2_cert.pem

-----BEGIN CERTIFICATE-----
MIIDzCAgIBAgIQXfKzloNpHhQXaa9uJ9mzO+1sdGREaSfDP46je2m7Nelz2CD
d7/goRS5q1+uxQpaUvH08Lxw9N6Chs018LkuHMYJFybfim50R
XK7H7Zn1enxRfCtCpAqAgMBAA5jtb

-----END CERTIFICATE-----

PRE Inbound eRx Deployment, Installation, Roll Back & Back-Out Guide 157 May 2019
8.1.4 va_internal_ca1_s2_cert

-----BEGIN CERTIFICATE-----
MIIBDoCCAgIwAwIBAgITFFAADAAADaAB4AQAAAABANbkxhkiG9w0BAQFs
ADBMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN

8.1.5 va_internal_ca2_s2_cert

-----BEGIN CERTIFICATE-----
MIIEoDCCA4igAwIBAgITFFAADDAAADaAB4AQAAAABANbkxhkiG9w0BAQFs
ADBMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN
MJyW10DI1M0YMTA3WjRMrwMDQGQYDROZ29HIWEAYCKZlI2My1PGQ8RCDemHsAAd
BogQVBMATF1ZBLU1udGybmFSeLMyLJQDTrtdjEWhhcNMTYXeMDITYMT5A3WhcN

-----END CERTIFICATE-----
8.1.10 vaww.esrstage1.aac.va.gov

-----BEGIN CERTIFICATE-----
MIIFDCCBChgAwIBAgIHAQAAAAC3jANBgkqhkiG9w0BAQEFAAOCAQ8wgg5EMBQGCCsGAQUFBzAChGEBQAQEEbQgAQL2k0eFzN+n+iaQbS2uYxhFt6/Cd2U/w5iidw1OjVx55hZ292Mi1JQzIoei9m8Nv5是我国的根CA，颁发的证书是安全的。
...
-----END CERTIFICATE-----

8.1.11 vaww.esrstage1.aac.va.gov

-----BEGIN CERTIFICATE-----
MIIFDCCBChgAwIBAgIHAQAAAAC3jANBgkqhkiG9w0BAQEFAAOCAQ8wgg5EMBQGCCsGAQUFBzAChGEBQAQEEbQgAQL2k0eFzN+n+iaQbS2uYxhFt6/Cd2U/w5iidw1OjVx55hZ292Mi1JQzIoei9m8Nv5是我国的根CA，颁发的证书是安全的。
...
-----END CERTIFICATE-----
8.1.12 vaww.esrpre-prod.aac.va.gov.pem

-----BEGIN CERTIFICATE-----
MIIFoJCCBQgAwIBAgIHMFQQAAAADC65jANBgkqhkiG9w0BAQsFADBKNMwEQYGZI...

-----END CERTIFICATE-----
---BEGIN CERTIFICATE-----
-----END CERTIFICATE-----